Security AppScan Enterprise v9.0.3 Planning & Installation Guide

GC14-7268-19

Contents

Chapter 1. Product overview

Application security management

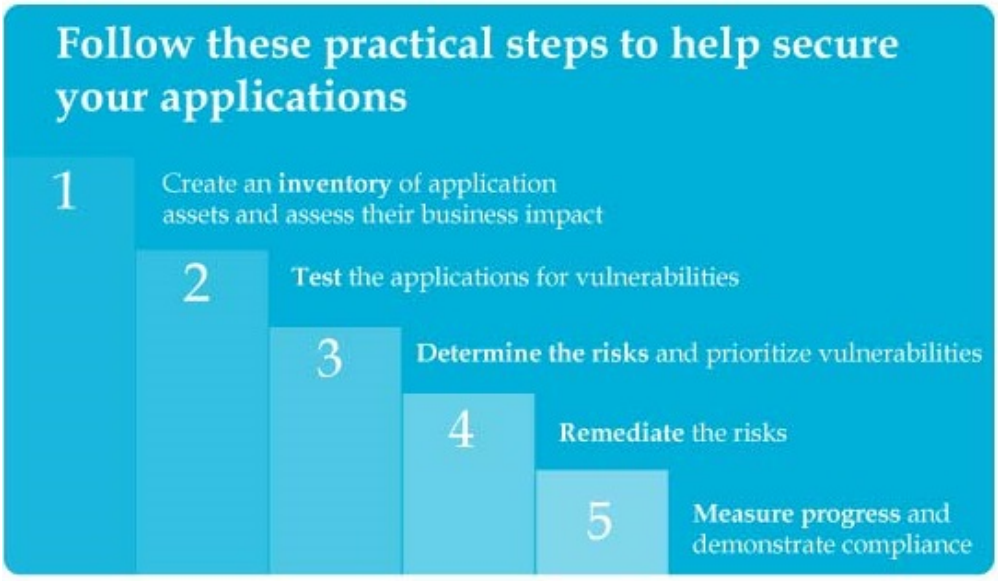
Security is about protecting your valuable assets. Some of the most important assets your organization owns are in the form of information, such as intellectual property, strategic plans, and customer data. Protecting this information is critical for your organization to continue to operate, be competitive, and meet regulatory requirements.

One of main weaknesses in the IT infrastructure of organizations is where most people do not expect – in the application layer. Many applications are not built with security in mind and they become the weakest link that attackers use to carry out a data breach.

What are some of the challenges your organization might be facing when it comes to application security?

- Compliance: External regulations and internal policy requirements
  - How do you set internal policy requirements for application security?
  - Is your private/sensitive data exposed by apps?
  - How do you check for, and demonstrate, application compliance?
- Pace: Rapid growth in the number of applications and releases to meet business requirements
  - Which applications pose the biggest business risk?
  - How do you test apps for security in rapid DevOps/Agile shops, without slowing down the process?
  - How do you reduce costs and catch security problems earlier in the lifecycle before they get into production?
- Resources: Resource and awareness challenges
  - Where do you start? How do you prioritize the work?
  - What do you test, and how do you test it?
  - How do you staff and improve skills and awareness?

To manage the challenge of addressing application security at the enterprise level, security teams must take a risk-based approach. This risk-based approach means that the team must prioritize assets, focus on identifying areas of highest risk, and then mitigate the risk. Addressing application security at an enterprise level goes beyond scanning applications for vulnerabilities. Large organizations might have thousands of applications that serve various purposes. The responsibility to assess and address application security typically belongs to a small security team.

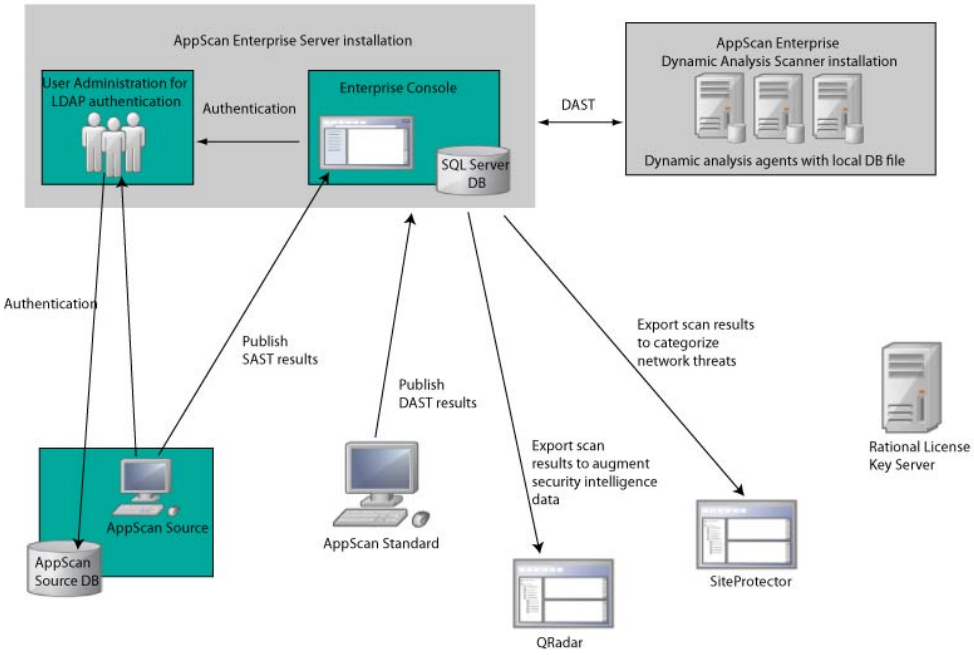


Using AppScan Enterprise, security teams can build an inventory of their application assets, classify, and prioritize their assets by business impact before they even start any security testing. This is important because organizations have limited resources and need to focus on the areas of highest risk. After applications are assessed for security vulnerabilities, they can be ranked by a security risk score. This enables Security teams to prioritize vulnerabilities in the context of the applications in which they exist, and focus on remediation activities that have the biggest impact when it comes to mitigating security risk for the organization.

AppScan Enterprise components

IBM® Security AppScan® Enterprise enables organizations to mitigate application security risk, strengthen application security program management initiatives and achieve regulatory compliance. Security and development teams can collaborate, establish policies and scale testing throughout the application lifecycle. Enterprise dashboards classify and prioritize application assets based on business impact and identify high-risk areas, permitting you to maximize your remediation efforts. Performance metrics are provided that help you monitor the progress of your application security programs.

This diagram depicts the AppScan Enterprise ecosystem, including integrations.



The SQL Server Database

The SQL Server database is the central repository for the following information gathered during a job: statistics, scan logs, polling for activity events, and is the means of communication between the Enterprise Console and the testing agents on the Dynamic Analysis Scanner. Regardless if you install the Server or Scanner, you create a database on a SQL Server you have installed in your environment. It should be configured first so that key information that AppScan Enterprise Server requires during configuration is ready and available. The database contains the following data:

- All data gathered by the agents
- Information about the scope applied to report data
- Summarized historical reporting data
- Agent configuration, scheduling, status, and alerting information
- User configuration and permission information

AppScan Enterprise Server

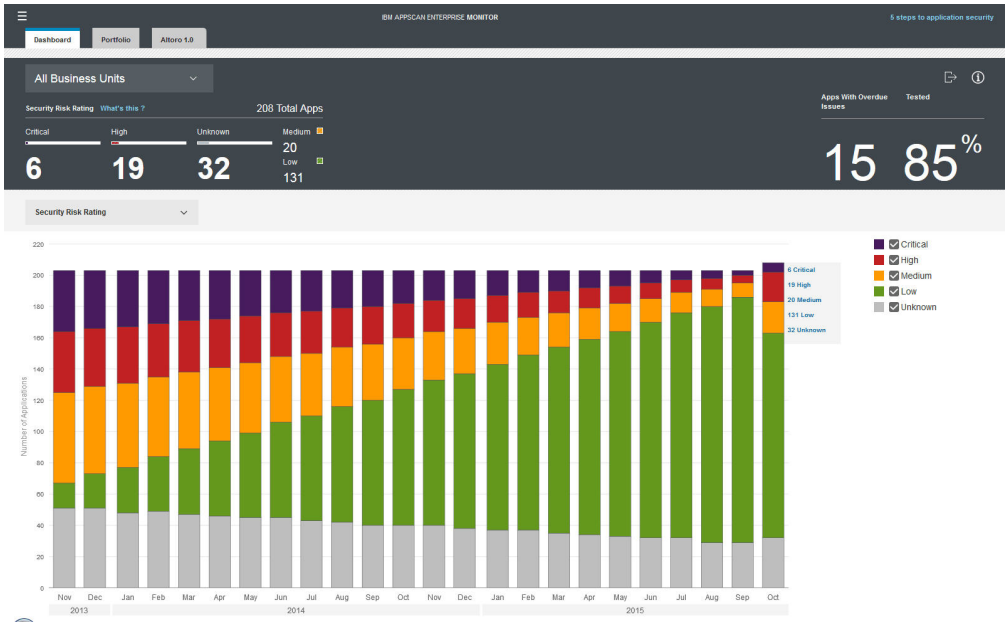
This component comprises:

- **User Administration:** The User Administration component of the Enterprise Server is used for LDAP user authentication.

  Note: If you are an AppScan Source user, this is all you need to install, unless you want to see correlated reports from results you publish to the Enterprise Server. Then you need to install the Enterprise Console as well.
- **Enterprise Console:** The Enterprise Console provides the user interface and reports through a web browser. It is the main user interface and supports

administration, scan configuration, and reporting. Depending on your requirements, you can install one or several instances of the Enterprise Console on a single server.

The Monitor view displays only the applications that you have permission to access. The dashboard charts track various metrics and trends of the web applications that compose your portfolio.



The Dashboard tab provides a holistic view of your business portfolio. In the lower section of the dashboard, select a chart to further investigate:

- **Security Risk Rating** (trend): Track application risk over time. Select the category check boxes to display the content you want to see. Hover over chart sections for details.
- **Security Risk Rating by Business Unit**: Prioritize application risk management by business unit. Hover over chart sections for details. Click through to the Portfolio tab to continue your triage process.
- **Testing Status** (trend): Track testing status. Select the category check boxes to display the content you want to see. Hover over chart sections for details.
- **Open Issues** (trend): Shows the number of open issues. Hover over chart sections for details.
- **Applications with Open Issues** (trend): Track the number of applications with open issues. Hover over chart sections for details.
- **Top Issue Types**: Shows the top issue types across all of your applications in the portfolio. For example, if there are many SQL injection issues, you can plan training for your developers. Hover over chart sections for details.
- **Issue Severity (Max)**: Identifies applications by their highest level of issue severity. Hover over chart sections for details. Click through to the Portfolio tab to continue your triage process.
- **Issue Severity (Max) by Business Unit**: Identifies applications by business unit, by their highest level of issue severity. Hover over chart sections for details. Click through to the Portfolio tab to continue your triage process.

Dynamic Analysis Scanner

A local database file is created at the beginning of each scan. Having a local database improves performance and scalability because it frees up the resource load on the central SQL database. The local database holds the information for each job the Scanner runs and sends the data to the main SQL Server database when the scan is completed.

The Scanner comprises two services:

- **Agent service and agents:** The agent service monitors the SQL Server database for jobs to perform. An agent is a Windows process that is created by an agent service when there is a job to be performed. While a scan job is in progress, the agent records the scan information in the database. If alerts have been configured, the alerting service informs the relevant users when specific events occur during the job.

  Note:

  1. Content and infrastructure agents can perform only one job at a time; however, a single Scanner can run more than one agent simultaneously. More than one job of the same type can be executed simultaneously on a given computer, with each job being run in its own agent process.
  2. The number of jobs running can exceed the maximum number of agents assigned to the Scanner because the number of jobs running includes jobs that are now in postprocessing or report generation. These jobs are no longer using an agent on the Scanner.
  3. If the number of blackout period suspended jobs exceeds the available number of available agents on the Scanner, the blackout period suspended job is given priority when it is time to run the next job.
- **Alerting service:** The alerting service is responsible for sending alerts to the appropriate notification devices. Although you can have as many agents and agent services as you need, only one alerting service can be installed for each database.

What's new

Features and enhancements new to AppScan Enterprise.

New in 9.0.3

- Reporting: From the Monitor view, export issues to reports in PDF or HTML formats.
- Issue import:
  - Ability to create custom scanner profiles to import issues in XML format, in addition to these IBM Security Cloud offerings: AppScan Mobile Analyzer, AppScan Dynamic Analyzer, and AppScan Static Analyzer
  - Ability to import issues exported from a report in XML format from AppScan Standard v9.0.3
- New and updated dashboard charts:
  - **OWASP Top Ten 2013**: Identifies applications that contain issues that match the 10 most critical web application security risks.
  - **CWE/SANS Top 25 Most Dangerous Software Errors**: Identifies applications that contain issues that match the CWE/SANS Top 25 Most Dangerous Software Errors.

  - **Top Issue Types (App)**: Updated to reflect the number of apps that are affected by the top issues that are discovered in your portfolio
- Issue management:
  - Track overdue issues. From the Portfolio view, track the number of applications with overdue issues. At the application level, track the overdue status for each individual issue.
  - New issue attributes:
    - Fixed Date: The date and time stamp when an issue was fixed.
    - Overdue: An issue that is not fixed by a predetermined date.
    - Customize the issue list view so that issues with a particular status are hidden from view: noise, passed, or fixed. From an application, go to **List menu** > **Customize View** to make your selections. As you classify issues with one of these statuses, they disappear from the list so that you can continue focusing on the issues that need attention.
  - Edit multiple applications simultaneously
- Portfolio triage:
  - Advanced filtering
  - Filter applications by issue attributes.
- New and updated REST APIs

New in 9.0.2.1 iFix1

- Support for Mozilla Firefox 38 (ESR) was added
- Changes in scan management APIs
- Ability to import issues in XML format from IBM Security Cloud offerings: AppScan Mobile Analyzer, AppScan Dynamic Analyzer, and AppScan Static Analyzer

New in 9.0.2.1

- Editing multiple issues simultaneously
- New dashboard trend chart: Open Issues by Severity
- Support was added for Microsoft SQL Server 2014
- Support for Liberty was upgraded from v8.5.5.4 to v8.5.5.6
- Standard Users can edit Basic and Additional options in the AppScan Dynamic Analysis Client. This capability can be given to other users as a custom user permission.
- Changes in the AppScan Dynamic Analysis Client:
  - New Proxy pane. If AppScan Enterprise uses a proxy server during the scan, you can use your Internet Explorer proxy settings (if configured), or enter custom settings.
  - Ability to log in to the Client from the desktop by using LDAP authentication.
- New and updated REST APIs
- Changes in content and layout of the About this Issue dialog

New in 9.0.2 iFix1

- Integration with JIRA for defect tracking.
- New REST APIs for Defect Tracking System integration.
- The search and filter fields in the Portfolio and Application tabs are combined into one field for simplicity and improved usability.

New in 9.0.2

- A new Dashboard tab displays the charts that were previously displayed in the Portfolio tab, and adds more metrics to assess the current status and progress of an application security initiative. This includes
  - trend of portfolio risk status
  - the number of applications with open security issues
  - trend of overall open issues
  - trend of applications test status
- A new approach to create scans consistent with AppScan Standard, for both the security team who creates the templates and for the developers who create the scans. See "Overview of scan configuration differences in v9.0.2 and previous versions" on page 143.
- New built-in formulas include new issues, open issues, fixed issues, and total issues.
- Enhancements to issue management:
  - A 'new' classification has been added for issue management. All issues that are scanned or imported from 3rd party scanners and that have not been triaged before are now classified as 'new' in both the Monitor and the Scans views.
  - Group issues by Status in an application tab.
- New and updated Application Security Management REST APIs.

For further details on what's new and changed since v9.0.1.1, read this whitepaper.

New in 9.0.1.1

- Security rules can be updated from Fix Central. See Deprecated features.
- When a scan is associated with an application, the Status and Severity Value for any issues that are triaged from the Monitor view are propagated in the reports in the Scans view. Reports do not need to be rerun to see the changes.
- Added support for Windows Server 2012 R2.
- Improved the way that CVSS scores are calculated for Static Analysis (SAST) issues that are imported from AppScan Source.
- Added a horizontal scroll bar for easier viewing in both the Applications and Issues tabs.
- Added a new compliance report: DISA's Application Security and Development STIG Category 1, V3R9.

New in 9.0.1

- Redesigned Application Security Management user interface for easier navigation and access to information.
- Capability to import application security vulnerabilities discovered using manual pen-testing or third-party tools.
- Scoring and ranking vulnerabilities in application context using Common Vulnerability Scoring System (CVSS). See Determining issue severity.
- Architecture redesign to reduce installation footprint and replacement of IBM Rational® Jazz™ user authentication component with IBM WebSphere® Liberty. See "Replacing Jazz Team Server with WebSphere Liberty - Frequently asked questions" on page 108 before upgrading.
- A built-in REST API interface provides you with a way to visualize RESTful web services that are used for creating and updating applications, setting up

application access for users, and adding or updating issues. Use the framework to interact with the API and get clear insight into how the API responds to parameters and options. See Enabling the Application Security Management REST API interactive framework.

- Glass box .NET agent now supports invisible parameters This enables AppScan to identify HTTP parameters that are not visible to black box scanners, improving scan coverage. No special configuration is needed. Until now, invisible parameters were supported only for Java™ platforms.

AppScan Enterprise Legal Notices

This information was developed for products and services offered in the US. This material might be available from IBM in other languages. However, you may be required to own a copy of the product or product version in that language in order to access it.

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-IBMproducts. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

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

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

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.

© (your company name) (year).
Portions of this code are derived from IBM Corp. Sample Programs.
© Copyright IBM Corp. _insert years here_.

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 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.

Depending upon the configurations deployed, this Software Offering may use session and persistent cookies that collect each user name for purposes of authentication and enhanced user usability. These cookies cannot be disabled.

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/us/en sections entitled “Cookies, Web Beacons and Other Technologies” and “Software Products and Software-as-a Service”.

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 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.

Accessibility features

Accessibility features help a user who has a physical disability, such as limited vision or hearing, to use software products successfully.

These accessibility features are offered:

- User interface keyboard navigation
- Screen reader navigation
- Tooltip help for links, buttons, messages, and other selections
- Non-text content that is presented to the user has a text alternative that serves the equivalent purpose
- Methods are provided for skipping over navigation links to get to main content of the page
- Captions are provided for prerecorded audio content in synchronized media
- Visual focus indicators by way of cursors in editable objects and highlighted buttons, menu items, and other selections
- Content can be displayed in high contrast and large font mode
- Landmarks are used on the page to identify commonly found sections of web page content, such as banners, breadcrumbs, and tabs
- Input errors that are automatically detected are identified and described in text
- Web pages do not contain content that flashes more than three seconds
- Color is not used as the only visual means of conveying information
- Documentation that includes hover-over image descriptions

Note:

1. During manual explore or recorded login, use the Tab key to navigate the links you want to explore and record. Use ALT+F4 to exit the recording browser window. Pausing or resuming the recording session is not available using keyboard shortcuts.
2. Input errors detected provide the user with text descriptions: for required fields not completed (upon submit), when a user input falls outside the required values, and when input data is not in the list of allowed values. Required fields may not always have indicators.
3. The DOM (Document Object Model) has been tagged with WAI-ARIA (Web Accessibility Initiative - Accessible Rich Internet Applications) landmarks which vastly improves keyboard navigation for the following: Data grouping, Accordion twisty, Regular twisty, breadcrumbs, navigational buttons, Quick scan Tabs, Help Tabs, ViewHTTPRequest tabs, Report Grid Tabs, About this Document tabs, About this Form tabs, About this Issue tabs, About this Page tabs, Dashboard tabs, Trend tabs, Report pack Summary layout tabs, and Security Dashboard tabs.

The IBM Knowledge Center is accessibility-enabled. The accessibility features are described at http://www-01.ibm.com/support/knowledgecenter/doc/kc_help.html#accessibility.

Keyboard shortcuts for the help system

The following table lists the shortcuts that you can use to control the help system through the keyboard.

Key combination	Context	Function
Right Arrow or Left Arrow	Navigation tree	Expand or collapse
Down Arrow or Tab	Navigation tree	Move to next topic node
Up Arrow or Shift+Tab	Navigation tree	Move to previous topic node
Tab	Content frame	Next link or toolbar button
Home or End	Content frame	Move to top or bottom
Alt+Left Arrow	Content frame	Back
Alt+Right Arrow	Content frame	Forward
Ctrl+P	Content frame	Print
Ctrl+Tab	Anywhere in the help browser	Put focus in the next frame
Ctrl+Shift+Tab	Anywhere in the help browser	Put focus in the previous frame

IBM and accessibility

See the IBM Human Ability and Accessibility Center for more information about the commitment that IBM has to accessibility:

Chapter 2. Installing

Planning the deployment and installation

The configuration you use depends on a number of factors: what you plan to do with the software, how your organization and website or applications are structured, and how the information is to be distributed. Before you install the current release, review the information about hardware and software requirements, licensing, and other deployment considerations.

Planning checklist

Before you install IBM Security AppScan Enterprise, review and complete all of the necessary tasks on the planning checklist.

Table 1. Planning checklist

Task	Check when complete
Get an inventory of your existing applications and identify the networks where they exist.	☐
Determine how many users will require access to AppScan Enterprise.	☐
Figure out how many applications you will scan. Are they in testing or production environments?	☐
Review your existing environment.	☐
Check the hardware and software requirements for SQL Server database. Are you going to use the Standard or Enterprise version of SQL Server?	☐
Review the hardware and software requirements of the hosting servers you need.	☐
What type of authentication are you using: Windows or LDAP?	☐
Identify the people in your organization who will help you get things done: • user accounts • licensing issues • setting up the SQL Server • LDAP administrator (if you use LDAP) They will need to: • Verify product and user license requirements. • Review the required user account information.	☐
Find out if you already have Rational License Key Server in your organization. If you do not, you can use the one that gets installed with AppScan Enterprise.	☐
Determine which components of AppScan Enterprise you need to install.	☐

Installation requirements

The Installation of AppScan Enterprise requires the correct hardware, software, operating system, and other factors.

Hardware and software requirements

The following tables provide a summary of the hardware and software required to run the software.

Average size deployment requirements

Attention: Hardware and software requirements that apply to an AppScan Source deployment that only uses the User Administration component of AppScan Enterprise Server are highlighted like this: **Applicable for an AppScan Source deployment**.

This configuration supports an average size deployment: 3-4 Dynamic Analysis Scanners (4 concurrent scan jobs per scanner). Larger deployments or loads might require more resources.

Note: If you install on a virtual machine (VM), make sure that you use these settings during the VM configuration:

- Number of virtual sockets: 4
- Number of cores per socket: 1

	Machine that hosts the SQL Server Database	**Machine that hosts the AppScan Enterprise Server** **Also applicable for an AppScan Source deployment**	**Machine that hosts the Dynamic Analysis Scanner**
Operating System	• 64-bit Windows Server 2008 R2 SP1 (64-bit) • Windows 2012 Server • Windows 2012 Server R2 (DataCenter) • Windows 2012 Server R2 (Standard) **Note:** See the Database section for details on supported SQL Server versions.	• 64-bit Windows Server 2008 R2 SP1 (64-bit) • Windows 2012 Server • Windows 2012 Server R2 (DataCenter) • Windows 2012 Server R2 (Standard) **Note:** The following environmental components are automatically installed during installation: • .NET 4.5.2 framework • IIS 7.5 and its dependencies • Rational License Server	• 64-bit Windows Server 2008 R2 SP1 (64-bit) • Windows 2012 Server • Windows 2012 Server R2 (DataCenter) • Windows 2012 Server R2 (Standard)
Processor	4 separate CPUs	2 separate CPUs	4 separate CPUs
RAM	16 GB	8 GB	16 GB
Hard disk specific	Fast input/output *		Fast input/output *
Hard disk drive size	1 TB	200 GB	500 GB

	Machine that hosts the SQL Server Database	Machine that hosts the AppScan Enterprise Server Also applicable for an AppScan Source deployment	Machine that hosts the Dynamic Analysis Scanner
C drive space		minimum 10 GB	minimum 10 GB
Required user accounts	Service account	• Service account • Local system user account	• Service account • Local system user account

* Fast input/output refers to the fast network and disk access, for example, use of Gigabit networking and use of a fast hard-drive such as SCSI or SSD for running the database. The requirement for "Fast input/output" depends on usage. Both the Dynamic Analysis Scanner server and the AppScan Enterprise Console server directly depend on a good connection to the SQL Server Database server and a good performing SQL Server database server. The faster the SQL Server Database server can handle requests, the more the system will be able to handle simultaneous scans and the faster the whole system will be in terms of UI responsiveness, report generation, etc.

Software requirement options

Software	Requirement
Operating System **Also applicable for an AppScan Source deployment**	• Windows 2008 Server SP1 / SP2 (Standard) x86-32 (**Limitation**: See Note 1 below) • Windows 2008 Server SP1 / SP2 (Enterprise) x86-32 (**Limitation**: See Note 1 below) • Windows 2008 Server SP1 / SP2 (Standard) x64 (**Limitation**: See Note 1 below) • Windows 2008 Server SP1 / SP2 (Enterprise) x64 (**Limitation**: See Note 1 below) • Windows 2008 Server R2 (Standard) x64 • Windows 2008 Server R2 (Enterprise) x64 • Windows 2008 Server R2 SP1 (Standard, Enterprise) x64 • Windows 2012 Server (DataCenter) • Windows 2012 Server (Standard) • Windows 2012 Server R2 (DataCenter) • Windows 2012 Server R2 (Standard) • Red Hat Enterprise Linux Version 6.0, 6.2, 6.3, and 6.4 (AppScan Enterprise Server, User Administration component only. Does not apply to the Dynamic Analysis Scanner) **Attention:** AppScan Enterprise is a 32-bit product. Run the *glibc.i686* and *libgcc.i686* packages to enable 32-bit compatibility on a 64-bit Linux machine. • The Windows 7 Enterprise, Professional, and Ultimate operating systems are only for the client-side components of AppScan Enterprise: – Browser – Manual Explore plugins – Manual Explorer stand-alone tool – Web Services Explorer – AppScan Dynamic Analysis Client **Note:** 1. Windows 2008 Server only supports TLSv1.0. Scanning sites that require TLSv1.1 or TLSv1.2 will not work. Enterprise Console will not have TLSv1.1 or TLSv1.2 protocols available for the IIS hosted part of the application. 2. The installer for the Dynamic Analysis Scanner and AppScan Enterprise Server checks for the .Net 4.5.2 framework, and installs it if it does not exist. 3. For best results, install all critical Microsoft software updates. 4. If the website being scanned uses technologies such as Flash, Windows Media, and additional character sets, these technologies must also be installed on the agent server machines.

Software	Requirement
Web Server	• IIS7 (Windows 2008 Server) **Note:** IIS7 must be enabled on the Windows 2008 Server so that AppScan Enterprise Server properly installs (not required for servers running Scanning Agents only): – Common HTTP features (all components except HTTP Redirection) – Application development (ASP.NET, ISAPI Extensions, ISAPI Filters) – Health and diagnostics (HTTP Logging, Request Monitor) – Security (Basic and Windows Authentication) – Performance (Static Content Compression) – Management tools (IIS Management console) – IIS 6 Management Compatibility (All) • IIS8.0 (Windows 2012 Server) **Note:** IIS8.0 must be enabled on the Windows 2012 Server so that AppScan Enterprise Server properly installs (not required for servers running Scanning Agents only): – Common HTTP features (all components except HTTP Redirection) – Application development (ASP.NET, ISAPI Extensions, ISAPI Filters) – Health and diagnostics (HTTP Logging, Request Monitor) – Security (Basic and Windows Authentication) – Performance (Static Content Compression) – Management tools (IIS Management console) – IIS 6 Management Compatibility (All)

Software	Requirement
Database	**Note:** 1. While Enterprise and Standard editions are supported for the following SQL Server versions, the Enterprise edition has superior scalability and security-enabling capabilities, such as built-in support for Transparent Data Encryption (TDE). Standard Edition can be secured through MS Windows Encrypting File System (EFS) or other third party encryption methods. 2. While both 64 and 32 bit versions of SQL Server are supported, using the 64-bit version of SQL Server can result in better performance. The 32-bit version works best for evaluation and small deployments. 3. If your environment uses a named SQL Server for the AppScan Enterprise database or SQL Server Express®, make sure that TCP/IP is enabled in the SQL Server configuration manager, and restart the SQL services for SQL Server and SQL Server browser. • Microsoft SQL Server 2008 SP3 • Microsoft SQL Server 2008 R2 SP2 • Microsoft SQL Server SQL Server 2012 • Microsoft SQL Server SQL Server 2014 • Microsoft SQL Server system requirements available from Microsoft (http://www.microsoft.com/sqlserver/2005/en/us/system-requirements.aspx).
Other Prerequisites	• Ensure that ASP.Net is installed and enabled in IIS.
Supported Browsers Minimum resolution: 1024x768. Higher resolution recommended.	• Microsoft Internet Explorer 8.0 (with Silverlight), 9.0, 10.0, 11.0 **Note:** 1. When using IE 8.0, you must install Microsoft Silverlight to view the charts in the Monitor view. • Mozilla Firefox 38.0 (ESR) • Google Chrome (only for Manual Explore Desktop tool)
Rational License Key Server	Version 8.1.1, 8.1.2, 8.1.3, 8.1.4
Defect Tracking Systems	• Rational Team Concert 3.0, 3.0.1, 4.0, 4.0.1, 4.0.3 • Rational Quality Manager 2.0, 2.0.1

Software	Requirement
Supported Integrations	• AppScan Source 9.0.2 (versions 7.0 - 9.0.1 are supported for importing of security results only) • AppScan Standard V7.7 - V9.0.2 inclusive (previous versions are supported for importing of security results only) • IBM Security SiteProtector™ 3.0, 3.0.0.1, 3.1 • IBM Security QRadar® SIEM 7.0 MR5, 7.1 MR2, 7.2, 7.2.1, 7.2.2, 7.2.3, 7.2.4, 7.2.5 • WebSphere Portal 6.0.1.4 and higher
VM	VMware ESXi v4.0, 4.1, 5.0
Application Server	WebSphere Application Server Liberty Core 8.5.5.6

Additional software requirements for the Dynamic Analysis Scanner

If you are executing Adobe Flash, the Flash Player plugin for Internet Explorer browser must be installed on the machine where the Dynamic Analysis Scanner runs. The supported versions of Adobe Flash can be downloaded from http://get.adobe.com/flashplayer/. Version 8 and higher are supported, but only versions 9 and higher have ActionScript 3 capabilities.

Glass box security testing requirements

The Glass box software must be installed on the same server as the application you want to test, not on the local machine where AppScan Enterprise itself is installed.

Table 2. Java platform requirements

Software	Requirement
Java EE containers	JBoss AS 6, 7; JBoss EAP 6.1; Tomcat 6.0, 7.0; WebLogic 11; WebSphere 7.0, 8.0, 8.5, 8.5.5
Operating Systems	Windows: • Windows Server 2008 R2 with and without SP1 (both 32 and 64-bit supported) Linux: • Linux RHEL 5, 6, 6.1, 6.2, 6.3 • Linux SLES 10 SP4, 11 SP2 UNIX: • AIX®, 6.1 • Solaris 10 (SPARC) • Solaris 11 Express

Table 3. .NET platform requirements

Software	Requirement
Operating System	32–bit and 64–bit editions: • Microsoft Windows Server 2008 • Microsoft Windows Server 2008 R2 • Microsoft Windows Server 2012 • Microsoft Windows Server 2012 R2
Other	Microsoft IIS version 7.0 or later Microsoft .NET4 Framework must be installed, and IIS must be configured at the root level to work with this version of ASP.net

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

Translated languages

The AppScan Enterprise user interfaces are available in these languages:

- English
- French
- German
- Italian
- Japanese
- Korean
- Brazil Portuguese
- Russian
- Spanish
- Simplified Chinese
- Traditional Chinese

Required user account information during installation and configuration

During installation and configuration, various user accounts are used, each with specific permissions. The Service Account and the Local System User account can be a single account, with the same user name and password. However, if your organization requires a separation of duties, use the Local System User Account during installation and configuration, and then use the Service Account for maintaining SQL Server database access.

Using the service account during installation and configuration

Table 4. Using the service account as the installation account.

Permissions	Descriptions
Make the service account a local administrator. Log in as this account when you are installing or maintaining the software. The service account must have the following permissions in the local security policy for the computer: • Access this computer from the network • Log on as a service (this permission is granted by the Server Configuration wizard, which is being run by a local Product Administrator) With a SQL Server database, you can use a single service account or multiple service accounts, depending on how you decide to install.	If there is some type of group policy that is deployed on the server that alters the local security policy of the computer and revokes any of these rights after installation and configuration, AppScan Enterprise will not work.
During the configuration of the components you install, you must enter service account information. This service account allows the agents to access the database server. Individual users do not require any form of database permissions. The service accounts used for the agents and the database should have passwords that do not expire. If, however, the passwords must change at regular intervals, you can rerun the Configuration wizard on all the AppScan Enterprise Server and Dynamic Analysis Scanner computers and enter the new password.	
The service account is granted db_owner rights to the database and must have permissions that allow it to create a database and tables, add users, run stored procedures, and grant rights.	If granting db_owner rights to the service account contravenes your organization's security policies, you can create a role to run stored procedures. See “Creating a wizard user account to run stored procedures” on page 138.

Table 4. Using the service account as the installation account (continued).

Permissions	Descriptions
File and folder permissions	The service account must have the following permissions on `Drive:\\YourInstallFolder\IBM\product name\` and all of its subfolders: • Read and Execute • Write • Delete • Delete files and subfolders • Create files and subfolders **Note:** These permissions enable the service account to write to the log files. They also enable the scan agents to write temp files, without which the scans would not function. The Configuration wizard creates these permissions for you - do not change them.
Local security policies	The service account must have permission to log on locally on the target machine so that it can impersonate the user's logon credentials. It also must have permission to log on as a service.
Registry permissions	The service account must have the following permissions: • Read and Execute • Write • Delete

Using the local system user account during installation and configuration

The Local System User Account must be a local Product Administrator on the machine (does not have to be the service account). In the local security policy for that machine, this user must have the following permissions:

- Access this computer from the network
- Allow logon locally

During installation and configuration, the Local System User Account requires db_owner permissions on the SQL Server database to create a database and tables, add users, run stored procedures, and grant rights. After installation and configuration are completed, remove the database permissions from the Local System User Account and assign them to the Service Account to handle all interaction between AppScan Enterprise and the database.

Tip: If you upgrade AppScan Enterprise or rerun the configuration wizard (which changes the database), give the Local System User Account the appropriate database privileges.

1. The Local System User Account creates and structures the AppScan database on the MS SQL Server.
2. The Local System User Account adds the database service to the database as db_owner.
3. The Local System User Account initializes the database with necessary data.

Table 5. Using the Local System User Account as the installation account.

Permissions	Descriptions
Make the local system user account a local administrator. Log in as this account when you are installing or maintaining the software. The local system user account must have the following permissions in the local security policy for the computer: • Access this computer from the network • Log on as a service (this permission is granted by the Server Configuration wizard, which is being run by a local Product Administrator) With a SQL Server database, you can use a single account or multiple accounts, depending on how you decide to install.	If there is some type of group policy that is deployed on the server that alters the local security policy of the computer and revokes any of these rights after installation and configuration, AppScan Enterprise will not work.
The local system user account allows the agents to access the database server. Individual users do not require any form of database permissions. The local system user accounts used for the agents and the database should have passwords that do not expire. If, however, the passwords must change at regular intervals, you can rerun the Configuration wizard on all the AppScan Enterprise Server and Dynamic Analysis Scanner computers and enter the new password.	After installation and configuration are completed, remove the database permissions from the Local System User Account and assign them to the Service Account to handle all interaction between AppScan Enterprise and the database.
The local system user account is granted db_owner rights to the database and must have permissions that allow it to create a database and tables, add users, run stored procedures, and grant rights.	If granting db_owner rights to the local system user account contravenes your organization's security policies, you can create a role to run stored procedures. See “Creating a wizard user account to run stored procedures” on page 138.

Table 5. Using the Local System User Account as the installation account (continued).

Permissions	Descriptions
File and folder permissions	The local system user account must have the following permissions on `Drive:\\YourInstallFolder\IBM\product name\` and all of its subfolders: • Read and Execute • Write • Delete • Delete files and subfolders • Create files and subfolders **Note:** These permissions enable the local system user account to write to the log files. They also enable the scan agents to write temp files, without which the scans would not function. The Configuration wizard creates these permissions for you -- do not change them.
Local security policies	The local system user account must have permission to log on locally on the target machine so that it can impersonate the user's logon credentials. It also must have permission to log on as a service.
Registry permissions	The local system user account must have the following permissions: • Read and Execute • Write • Delete

Other user accounts

Table 6. Other user accounts.

Account	Description
ASPNET account	The ASPNET account must have the following permissions on Drive:\\YourInstallFolder\IBM\ product name\ and all of its subfolders: • Read and Execute • Write • Delete • Impersonate a client after authentication
Internet Guest account	The Internet Guest account must have the following permissions on Drive:\\YourInstallFolder\IBM\ product name\ and all of its subfolders: • Read and Execute • Write

Related information:

Troubleshooting: Viewing a report in AppScan Enterprise results in error

Ports used by AppScan Enterprise

Deployment of AppScan® Enterprise requires that certain ports be open on the computers where those components are installed.

Table 7. Ports used by AppScan Enterprise

Port	Component	Protocol
80	Dynamic Analysis Scanner	HTTP
443	Dynamic Analysis Scanner	HTTPS
40001-40500	Manual Explore to communicate with the Enterprise Console	
40501-50000	Manual Explore to communicate with the Enterprise Console (multiple instances)	
27000-27009	Rational License Server **Note:** 1. The Rational License Key Server is used for serving floating licenses to AppScan Enterprise. To make use of AppScan Enterprise floating licenses through a firewall, refer to this technote: What ports to open when License Key Server is behind a firewall. 2. To operate in a port forwarding environment, you must make configuration changes to the AppScan® Enterprise system properties. For detailed instructions for changing the appropriate settings, contact your IBM® support representative.	TCP/IP

Table 7. Ports used by AppScan Enterprise (continued)

Port	Component	Protocol
1443	AppScan Enterprise uses the standard OLE drivers and standard ports to communicate with the database. To see the ports used, review Microsoft SQL Server documentation specific for the version of SQL Server you are running. For SQL Server 2008 (and other close versions) review this Microsoft article, How to: Configure a Windows Firewall for Database Engine Access. For an overview for the ports used by Microsoft SQL Server 6.5, 7.0, and 2000, review this Microsoft article, TCP Ports Needed for Communication to SQL Server Through a Firewall. By default, the configuration wizard uses port 1443 to connect to SQL Server database. In the Database Connection window of the wizard, enter the SQL Server name, port number and the name of the database you are connecting to.	HTTPS
9443	Liberty server in AppScan Enterprise v9.0.1 and later (note that this port is configurable in the Configuration Wizard). User Authentication in Jazz Team Server, if using Jazz for user authentication, in AppScan Enterprise v8.5 - 9.0.0.1.	HTTPS
25	Alerting service on the Dynamic Analysis Scanner	SMTP
444	Alerting service on the Dynamic Analysis Scanner	SNPP

Product and user licenses

This topic on AppScan Enterprise licenses opens a technote in a separate browser.

Read this technote: Licensing for AppScan Enterprise.

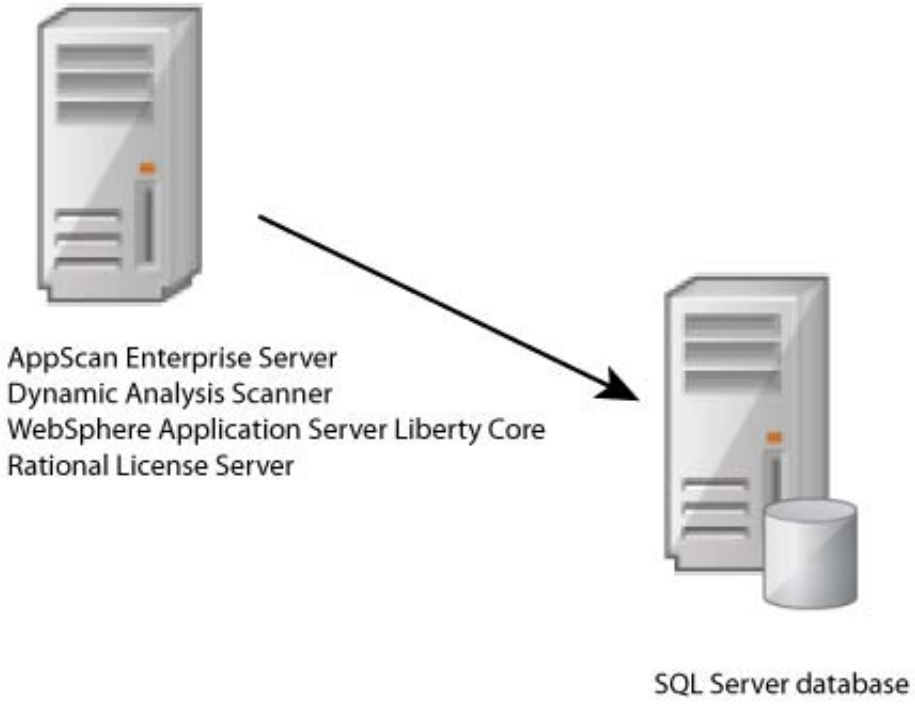
Installation topology examples

These examples illustrate installation topologies that are commonly used for deployment. Use the example that closely matches your situation. Each topology provides more information about when and how to use it.

Evaluation topology example

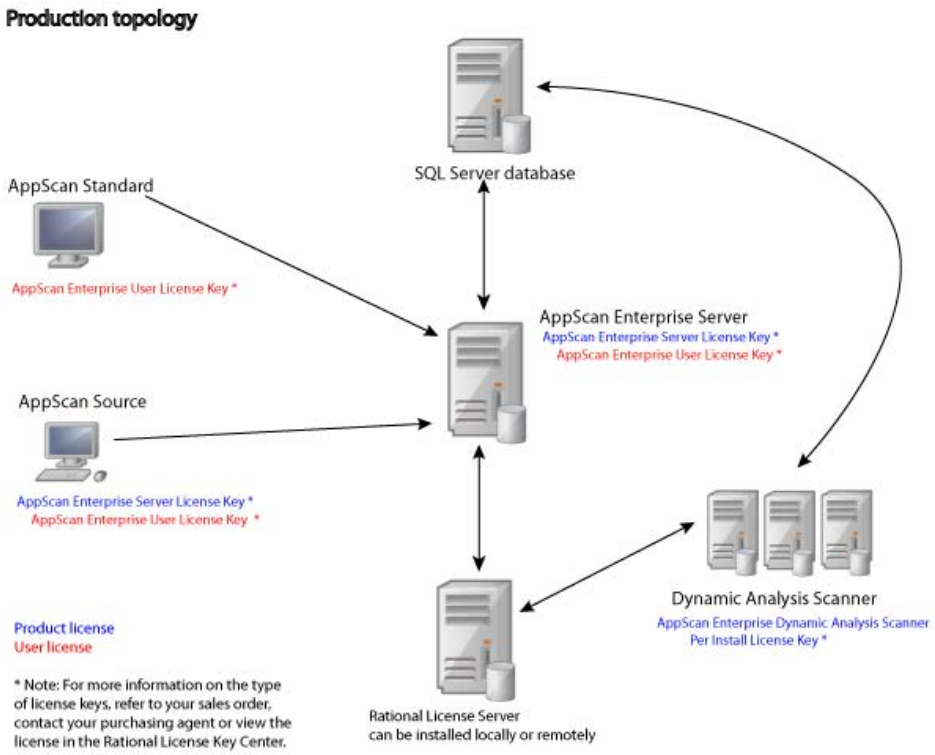
Evaluation installations are useful for demonstration or training deployments.

The following topology is a general representation of an evaluation installation. In this type of installation, the application software and the Rational License Key Server is installed on the same server. The SQL Server database is installed on a separate server.



Production topology example

This enterprise topology example is useful for production or medium-sized teams and multiple server deployments. In this type of installation, databases are installed on a single database server and each application is installed on a dedicated application server. You can install multiple instances of an application on separate application servers.



Improved traffic performance for DAST scanning

Architecture changes made in AppScan Enterprise 8.7 to enhance scalability and performance decreased the traffic between the Dynamic Analysis Scanner (DAST scan server) and the SQL Server database, and increased the amount of data stored locally on the scan server.

In earlier versions of AppScan Enterprise, the DAST scan server wrote data into the central database throughout the entire duration of the scan. This consumed a lot of resources on the database server, which affected the Web UI performance and greatly limited the number of scans that could run simultaneously on a scan server. There were also latency concerns depending on where the scan server was located in relation to the database server.

As of AppScan Enterprise version 8.7, scan data is now written into a local built-in database on the DAST scan server. At the end of the scan, data is transferred to the central SQL Server database which resides on the AppScan Enterprise Server. The increase in network traffic between the scan server and the target application reduces the network bandwidth between the scan server and the database. This improves the performance of the Web UI, enables organizations to run more simultaneous scans on a single scan server, and addresses the latency concerns when the scan server is located far from the database server.

Network traffic benchmarks for AppScan Enterprise DAST scanning

The following benchmarks are based on a dynamic analysis scan of a test website 'Altoro Mutual' (demo.testfire.net). The web application is hosted in Texas, USA; the DAST scan server and the SQL Server database are hosted in Ottawa, Canada. The test scan was completed by AppScan Enterprise 8.7 in 41 minutes, covered 688 pages, and included 21,068 unique security tests.

The specifications of the computer that hosted AppScan Enterprise Sever and the SQL Server database are:

- Windows 2008 R2 SP1
- 4 CPU 16G RAM
- Microsoft SQL Server 2008 R2 (SP2), 10.50.4000.0 (x64)

The specifications of the computer that hosted the DAST scanner are:

- Windows 2008 R2 SP1
- 2 CPU 4G RAM

Table 8. Network traffic data

Server	Total bytes	Bytes sent	KB/second sent	Bytes received	KB/second received
SQL Database Server	167,471,086	81,546,724	258.6	85,924,362	272.5
DAST Scan Server	329,359,220	112,187,145	355.8	217,172,075	688.8
Web Server	161,890,890	135,628,107	472.5	26,262,783	91.5

The total traffic usage between the SQL Database Server and the DAST scan server is 81,546,724 (Bytes sent) +85,924,362 (Bytes received) =167,471,086 bytes.

The total traffic usage between the DAST scan server and the Web Server is 135,628,107 (Bytes sent) +26,262,783 (Bytes received) =161,890,890 bytes.

Preinstallation tasks

Before you install AppScan Enterprise, you will need to prepare and configure your system.

Preinstallation checklist

You must take certain steps before you install AppScan Enterprise.

Table 9. Preinstallation checklist

Task	Check when complete
Install and configure your SQL Server database.	☐
Create a “Service Account” on page 149. Make sure the service account works on each machine where the Scanner and Server are going to be installed. See “Required user account information during installation and configuration” on page 22.	☐
Attach the service account with appropriate privileges to access the SQL Server database.	☐
Log in to the Rational License Key Center to get your license keys for AppScan Enterprise.	☐
Find out the MAC id and disk id of the server where the Rational License Server is installed.	☐
Import licenses into the Rational License Server.	☐
Set up your LDAP accounts. Identify your users and groups.	☐

Table 9. Preinstallation checklist (continued)

Task	Check when complete
If you are upgrading to v9.0.1, read "Replacing Jazz Team Server with WebSphere Liberty - Frequently asked questions" on page 108 before you begin upgrading.	☐
If you are upgrading to v9.0.1 and need to migrate Jazz Team Server users to use the Liberty authentication method, export a .csv file of users by using the **cd <install-dir>\Appscan Enterpise\ JazzTeamServer\server\ repotools-jts.bat -exportUsers toFile=C:\users.csv repositoryURL=https://<hostname>:9443/jts** before you begin upgrading to v9.0.1. Then follow the steps that are documented in Configuring a basic user registry for the Liberty profile to import the users into Liberty.	☐
If you don't have a server certificate, create one from your certificate authority to use with Liberty. See "Using a certificate in your certificate store with Liberty" on page 34.	☐
Set up security on SQL Server. On the Enterprise edition, enable Transparent Data Encryption (TDE). On the Standard version, use Encrypting File System (EFS).	☐
Export your server certificate from IIS as a .pfx file, and give it a password. It contains information that you need to use during configuration to ensure AppScan Enterprise works with WebSphere Application Server Liberty Core. If you don't have a server certificate, create one from your certificate authority.	☐
If you plan to import scan templates from AppScan Standard, disable Enhanced Security on Windows Server 2008, 2008 R2, and 2012 so that AppScan Enterprise can log in to applications. See "Disabling Internet Explorer Enhanced Security Configuration on Windows Server 2008, 2008 R2, and 2012" on page 33.	☐
Download the installation media from PassPort Advantage.	☐

Configuring the SQL Server database for AppScan Enterprise

The AppScan Enterprise Server configuration needs information about SQL Server. Configure the SQL Server first to save time during the AppScan configuration. If you upgrade SQL Server to a newer version, follow these instructions as well.

SQL Server properties

To define server properties:

1. Right-click the server name and select **Properties** > **Security**.
2. In the Server Authentication section, choose *Windows Authentication mode* and click **OK**.

Note: If your environment uses a named SQL Server instance for the AppScan Enterprise database or SQL Server Express, make sure that TCP/IP is enabled in the SQL Server configuration manager, and restart the SQL services for SQL Server and SQL Server browser. For example, if you specify the instance name as:`SQL Server or Server\Instance name: <sql_server_host>\<sql_server_instance>` instead of `SQL Server or Server\Instance name: <sql_server_host>`.

Encrypting a SQL Server database with EFS

If your configuration uses Microsoft SQL Server Standard Edition, and you plan to encrypt your AppScan Enterprise databases, then this procedure needs to be performed before you install AppScan Enterprise.

Related information:

 Building Secure ASP.NET Applications: Authentication, Authorization, and Secure Communication

Enabling IIS6 compatability with IIS7 on Windows 2008 Server

IIS7 must be enabled on the Windows 2008 Server so that installation is successful. This task guides your through the correct configuration.

About this task

The following procedure assumes that IIS7 is already installed on the server. See a list of prerequisite IIS features in the system requirements.

Procedure

1. On the Windows 2008 Server, go to **Start** > **Control Panel** > **Programs and Features**.
2. Click **Turn Windows features on or off** in the **Tasks** panel.
3. In the Contents view, click **Roles**.
4. Click **Add Role Services** in the **Role Services** section.
5. Select the **Static Content** role service.
6. Expand **Management Tools (Installed)**, select the **IIS6 Management Compatibility** check box, and click **Install**.

What to do next

Install a valid security certificate into IIS.

- For IIS6: See Install a Server Certificate (IIS 6.0)
- For IIS7: See Configuring Server Certificates in IIS 7

Disabling Internet Explorer Enhanced Security Configuration on Windows Server 2008, 2008 R2, and 2012

This Windows security feature prevents Internet Explorer from navigating to sites that are not listed in the browser's 'trusted sites'. How does it affect you? If you plan to import scan configuration templates from AppScan Standard, the scan might not be able to log in to the sites you want to test. Use these instructions to disable the feature on the servers where the Dynamic Analysis Scanner is installed.

Procedure

1. On Windows Server 2008 or 2008 R2:
   a. Open the Server Manager (**Start** > **Server Manager**).
   b. In the Security Information section, click **Configure IE ESC**.
   c. In the Internet Explorer Enhanced Security Configuration window, disable the IE ESC for Administrators and Users, and click **OK**.
2. On Windows Server 2012:
   a. Start the Server Manager (**Server Manager** > **Local Server**).

b. In the Properties section, scroll to the right until you see this option: **IE Enhanced Security Configuration**, and toggle the setting to **Off**.
c. In the Internet Explorer Enhanced Security Configuration window, disable the IE ESC for Administrators and Users, and click **OK**.

Note: In the Server Manager, you will notice that the setting has not changed. Press F5 to refresh the screen to see that the setting has turned off.

Configuring Flash to work on Windows Server 2012

Installing Adobe Flash on Windows Server 2012 can be complicated; certain filters must be disabled before it can be used properly by AppScan Enterprise.

Procedure

1. Add the Desktop Experience feature:
   a. On the Windows Server 2012 computer, open Server Manager from the taskbar or from the **Start** menu.
   b. In the Dashboard section, click **Add roles and features**.
   c. In the Add Roles and Features wizard, select **Server Selection** > **Features**.
   d. In the Features list, select **User Interfaces and Infrastructure** > **Desktop Experience**.
   e. Click **Next**, and then click **Install** and respond to the wizard prompts to complete the wizard.
2. Enable the Flash Player in Microsoft Internet Explorer. Follow the instructions at http://forums.adobe.com/thread/885448.
3. Disable the ActiveX filtering in Internet Explorer. Follow the instructions at http://forums.adobe.com/thread/867968.

Downloading and extracting the electronic images

If you download the installation files from Passport Advantage®, you must correctly extract the contents of the compressed files before you can install AppScan Enterprise.

Procedure

1. Go to Passport Advantage and sign in using your IBM ID and password.
2. In the **Find by search text** field, enter `AppScan Enterprise Server <version>` and download this eAssembly for your particular operating system: **IBM Security AppScan Enterprise Server <version> Multiplatform, Multilingual**.
3. Go back to the search page, and in the **Find by search text** field, enter `AppScan Enterprise Dynamic Analysis Scanner <version>` and download this eAssembly for your particular operating system: **IBM Security AppScan Enterprise Dynamic Analysis Scanner <version> Windows Multilingual**.

Using a certificate in your certificate store with Liberty

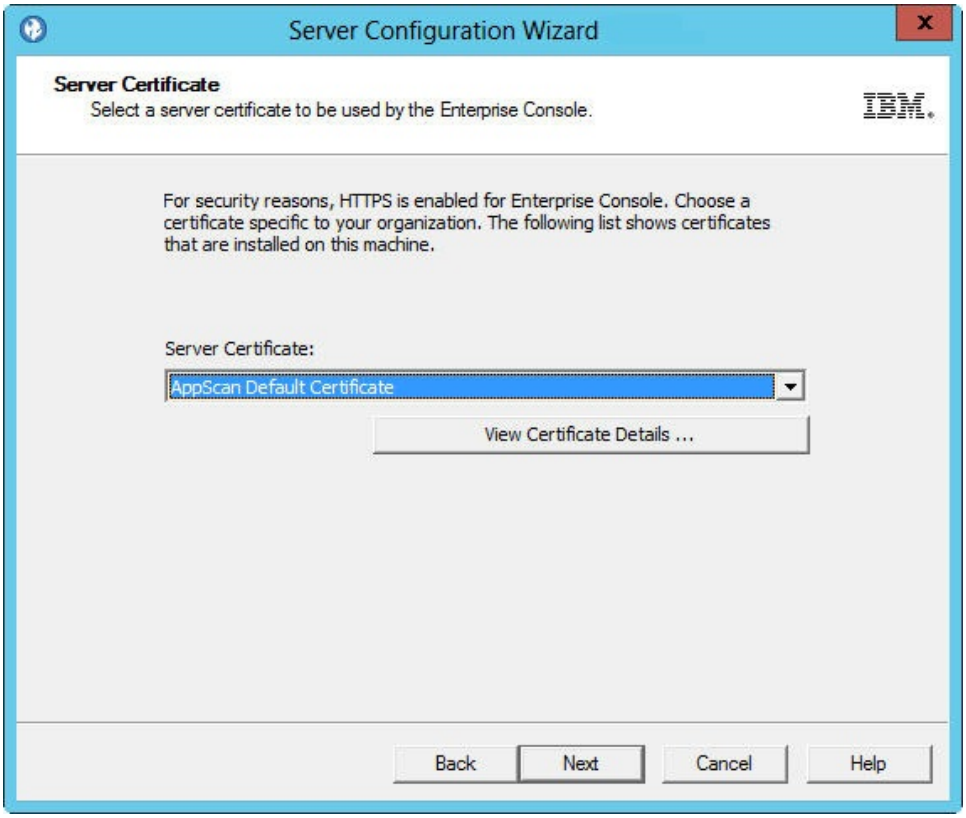
This procedure describes how to use Liberty certificates to secure IIS.

Procedure

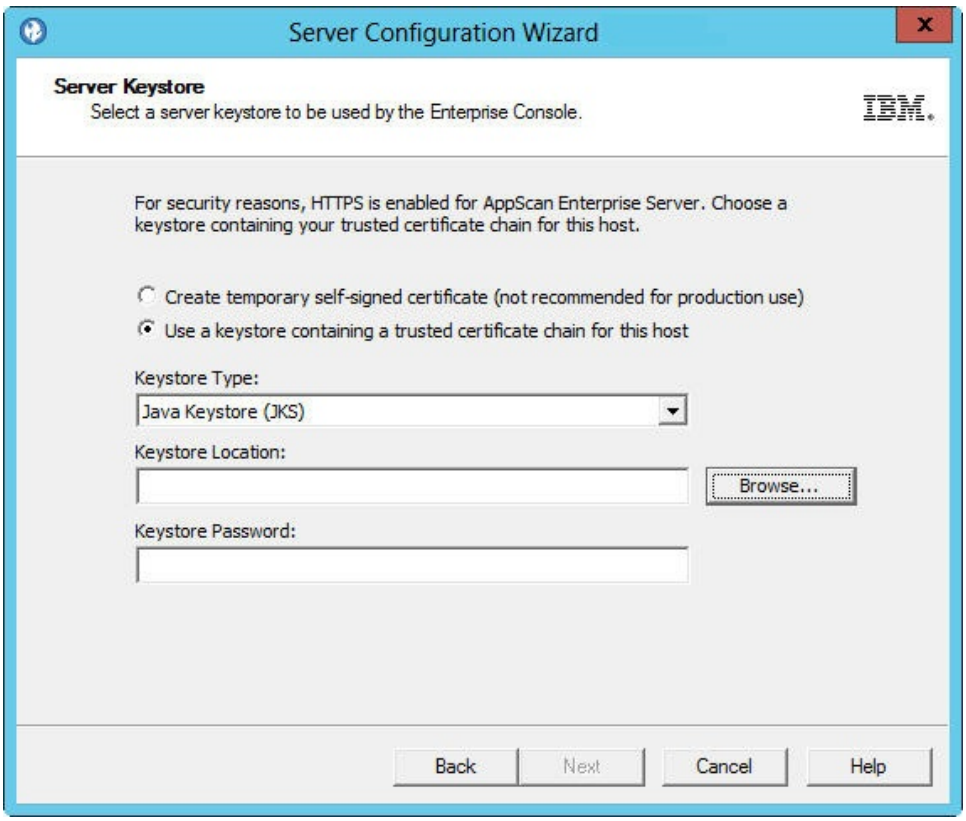
1. Optional: If you don't have a server certificate, create one from your certificate authority.
   a. Generate a certificate request to send to your external certificate authority.
   b. Send the certificate request to the certificate authority using a method that the certificate authority accepts.

c. When you receive the certificate, complete the certificate request.

2. Install AppScan Enterprise Server.
3. Run the configuration wizard.
4. In the Server Certificate window, choose a certificate specific to your organization. This step helps you deploy a secure AppScan Enterprise in your environment. See “Server Certificate” on page 150.



5. In the **Server Keystore** screen, select a server keystore to be used by the Enterprise Console. If you exported a .pfx file, select **Public key cryptography standards #12 (PKCS #12)**. Browse to the location where you saved the .pfx file, import it and enter the password you created when you exported the file. See “Server Keystore” on page 150.



6. Finish the configuration wizard.

Installation tasks

This section provides the instructions for installing AppScan Enterprise.

Installation checklist

As you install AppScan Enterprise, review and complete all of the necessary tasks on the installation checklist.

Table 10. Installation checklist

Task	Check when complete
Install AppScan Enterprise Server (User Administration and Enterprise Console components).	☐
Run the Configuration Wizard.	☐
Verify the installation (Log in to the Enterprise Console).	☐
Run default settings wizard on console server.	☐
(If using distributed topology) Install Dynamic Analysis Scanner on the required number of machines.	☐
Run the Configuration Wizard.	☐
Verify the installation.	☐

Sample installation scenarios

These installation deployment scenarios are example installation topologies that are commonly used for the deployment of AppScan Enterprise. Use the example that most closely matches your situation. When installing AppScan® Enterprise, it is important that the correct installation workflow be followed. These topics guide you through the workflow involved in some sample installation scenarios.

Installing all required components on one computer

In this scenario, all components are installed on one computer. This type of deployment is best suited for demonstration or training deployments, not full production environments.

About this task

This scenario is divided into several sections:

- "Installing IBM Rational License Key Server"
- "Installing IBM Security AppScan Enterprise Server" on page 39
- "Running the Configuration wizard" on page 41
- "Running the Default Settings wizard" on page 51
- "Installing IBM Security Dynamic Analysis Scanner" on page 52
- "Running the Configuration wizard" on page 54
- "Verifying the installation of the Enterprise Console" on page 58
- Verifying the scanner installation

Note:

1. This scenario assumes that the SQL Server database is installed and configured so that key information is available during configuration of AppScan Enterprise Server.
2. If you already have a Rational License Key Server that is deployed on your network, skip to the "Installing IBM Security AppScan Enterprise Server" on page 39 task.
3. If you are upgrading from a previous version of AppScan Enterprise, read "Replacing Jazz Team Server with WebSphere Liberty - Frequently asked questions" on page 108 before you begin upgrading.
4. To migrate Jazz Team Users users to this new authentication method, export a .csv file of users by using the **cd <install-dir>\Appscan Enterprise\ JazzTeamServer\server\ repotools-jts.bat -exportUsers toFile=C:\users.csv repositoryURL=https://<hostname>:9443/jts** before you begin upgrading to v9.0.1. Then follow the steps in this topic: Configuring a basic user registry for the Liberty profile to import the users into Liberty.

Installing IBM Rational License Key Server:

The Rational License Key Server is used for hosting your AppScan Enterprise Server license. If you do not have a Rational License Key Server on your network, you can install it locally when you install AppScan Enterprise Server.

About this task

If you already have a supported version of Rational License Server that is installed, you can skip the portion of these instructions that cover Rational License Server installation - and proceed to the portion of the instructions that covers starting License Key Administrator and importing your license.)

Procedure

1. Go to the directory where you downloaded the executable file (`AppScanEnterpriseServerSetup_<version>.exe`) and double-click the file. (The Rational License Key Server is bundled in this .exe file.)

   Note: It might take a while for the next screen to display.
2. Click **Yes** when you are asked to install Rational License Key Server.
3. In the Rational License Server installer, click **Install or Update IBM Rational License Key Server**.
4. If IBM Installation Manager is not already installed on your system, it launches for installation purposes. Click **Install**.
5. On the first page of the Install Packages wizard, ensure that the **IBM Rational License Key Server** check box, and check boxes for all entries beneath it, are selected. Click **Next**.
6. In the Prerequisites page, you are instructed to close all applications and disable anti-virus software. Complete these precautionary tasks and then click **Next**.
7. On the Licenses page, read the license agreement. If you agree to the terms of the license agreement, click **I accept the terms in the license agreement** and then click **Next**.
8. In the Location page, specify the installation directory and then click **Next**.
9. Complete the Package Group page according to your needs (for example, if you are using Installation Manager for the first time and have no existing package group, leave the default settings as-is). Click **Next**.
10. In the Translation Selection page, select the national languages that you want to install. Click **Next**.
11. On the Features page, ensure that all features are selected and then click **Next**.
12. A summary of what is installed is shown on the Summary page. If you want to change your selections, click **Back** to return to the previous pages. When you are satisfied with your installation choices, click **Install**.
13. When the installation is complete, click **Finish** and close IBM Installation Manager.
14. Start the IBM Rational License Key Administrator from the **Windows Start** menu (in the **Programs** menu, launch **IBM Rational** > **License Key Administrator**).
15. When the IBM Rational License Key Administrator starts, you are prompted with the License Key Administrator wizard (if the wizard does not open automatically, select **License Keys** > **License Key Wizard** from the main menu). In this wizard, select **Import a Rational License File** and then click **Next**.
16. In the Import a License File panel, click **Browse** and then browse to your AppScan Enterprise Server license file. Open the file with the browse dialog box and then click **Import**. This table maps the license names in LKAD to the license types in AppScan Enterprise.

Table 11. AppScan Enterprise licenses

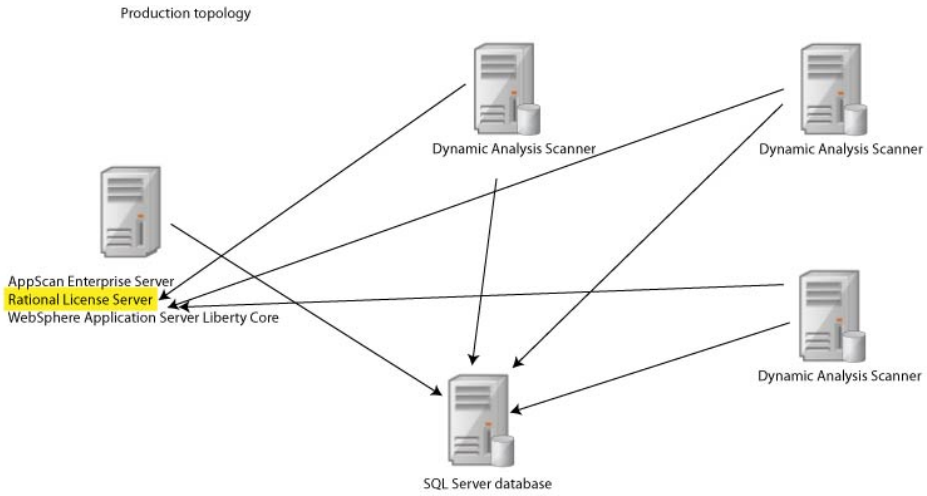
License	What it is for
AppScan Enterprise Dynamic Analysis Scanner Per Install License Key	Dynamic Analysis Scanner
AppScan Enterprise Dynamic Analysis User Authorized User Single Install License Key	Authorized Scanning

Table 11. AppScan Enterprise licenses (continued)

License	What it is for
AppScan Enterprise Dynamic Analysis User Floating User Single Install License Key	Floating Scanning
AppScan Enterprise Server Basic Per Install License Key	Enterprise Server Basic
AppScan Enterprise Server Per Install License Key	Enterprise Server Premium
Appscan Enterprise Edition Reporting Only User Authorized User Single Install License Key	Authorized Reporting
Appscan Enterprise Edition Reporting Only User Floating User Single Install License Key	Floating Reporting

17. After you confirm the license or licenses to import, the Restart License Server dialog box will open. Click **Yes** to restart the license server. If the License Server service fails to start, open the Windows Services administrative tool. In the tool, locate **FLEXlm License Manager** and start it.

Results



Installing IBM Security AppScan Enterprise Server:

Use this procedure to install the User Administration component and Enterprise Console for reporting and user administration tasks.

Before you begin

Make sure you read "Required user account information during installation and configuration" on page 22 so that you know which user account to use during installation.

About this task

If you have a Rational License Key Server that is already deployed elsewhere on your network, start at Step 1; otherwise start at Step 2.

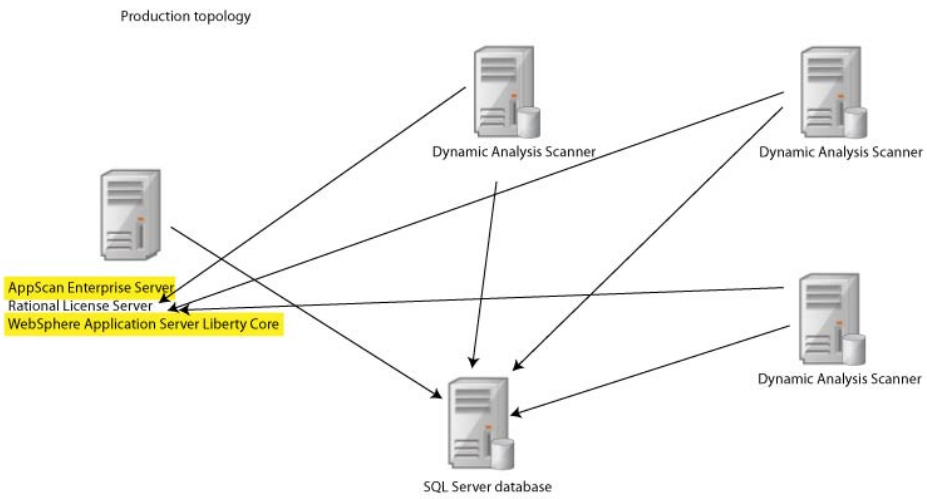
Procedure

1. Go to the directory where you downloaded the compressed file (`AppScanEnterpriseServerSetup_<version>.zip`), extract the files, and double-click the `AppScanEnterpriseServerSetup_<version>.exe` file.

   Note: It might take a while for the next screen to display. The compressed file includes these files:

   - `AppScanEnterpriseServerSetup_<version>.exe`
   - `IBM Security AppScan Enterprise Server.msi` - **do not run this file**
   - `Data1.cab`
2. If you do not already have Rational License Key Server that is installed on your network, install it when prompted, and follow the procedure in the **Installing Rational License Key Server** task. Otherwise, click **No**.
3. In the Setup wizard Welcome screen, click **Next**.
4. In the License Agreement window, select the **I accept the terms in the license agreement** option, and click **Next**.
5. In the Destination Folder window, do one of the following actions and click **Next**:
   a. Click **Next** to accept the default installation location.
   b. Click **Change** to select a different installation location.
6. In the Ready to Install the Program window, click **Install** to proceed with the installation.
7. On the Setup Wizard Completed screen, click **Finish** to launch the Configuration Wizard.

Results



Running the Configuration wizard:

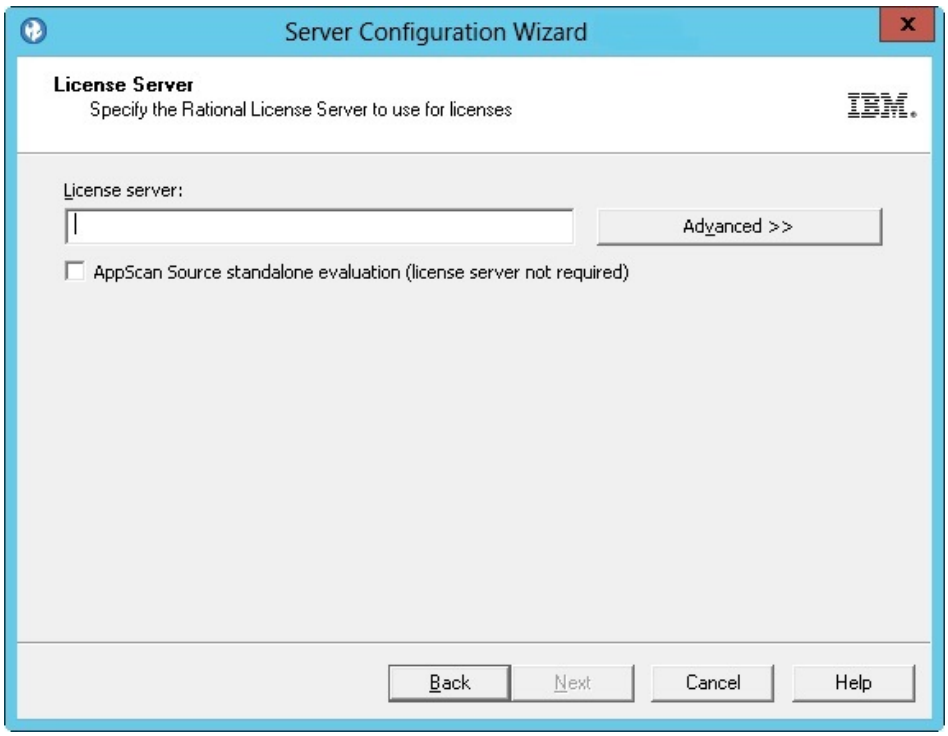
After you install or upgrade the Server or Scanner, you must configure each installed component and run the Configuration wizard on all instances and on all servers.

Before you begin

1. During configuration, you define the name and location of the SQL Server database to be used, and the service account name and password. The user who runs the configuration wizard must be able to create a database and grant rights.
2. If you encounter an error "**WARNING** Unable to configure virtual directory "ase" for local directory "C:\Program Files (x86)\IBM\AppScan Enterprise\WebApp". Ensure IIS is configured properly and try again. ", consider disabling your antivirus software while you are running the configuration wizard. If you do not want to disable the antivirus software, you can exclude the AppScan Enterprise folder from the antivirus configuration, and run the configuration wizard again.

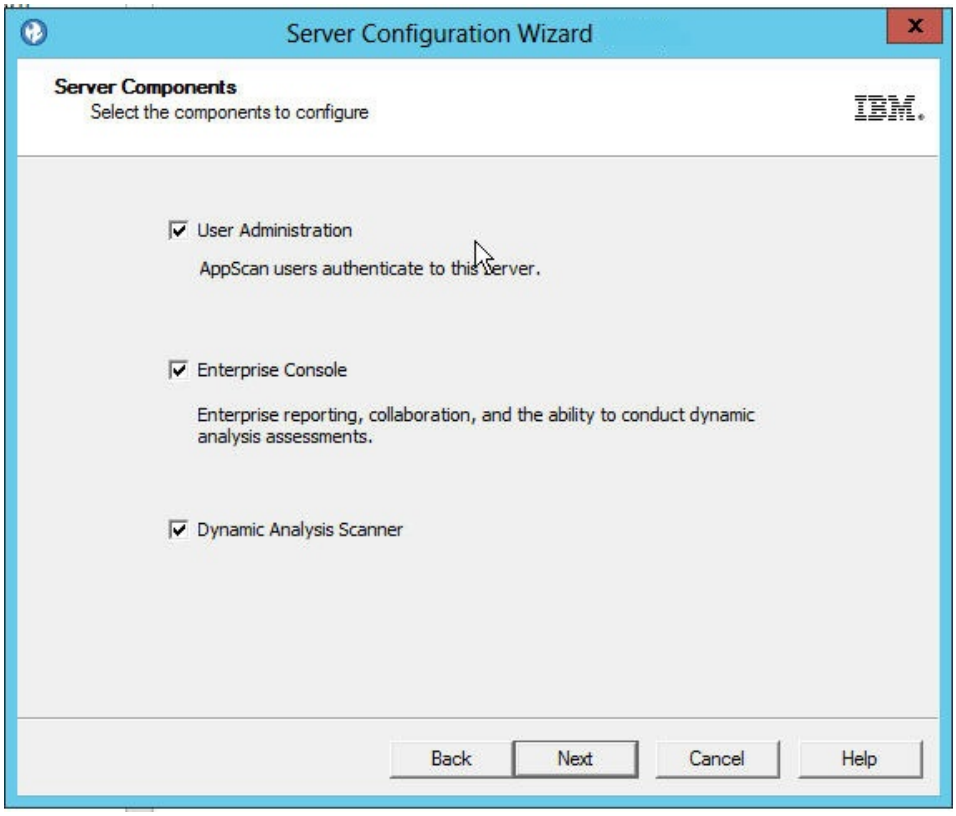
Procedure

1. When the installation is complete, the Configuration wizard launches automatically. You can also start it by selecting **Configuration Wizard** from the Windows **Start** menu.
2. In the Welcome screen, click **Next**.
3. In the License Server window, specify the Rational License Server to use for licenses. See “License Server” on page 147.

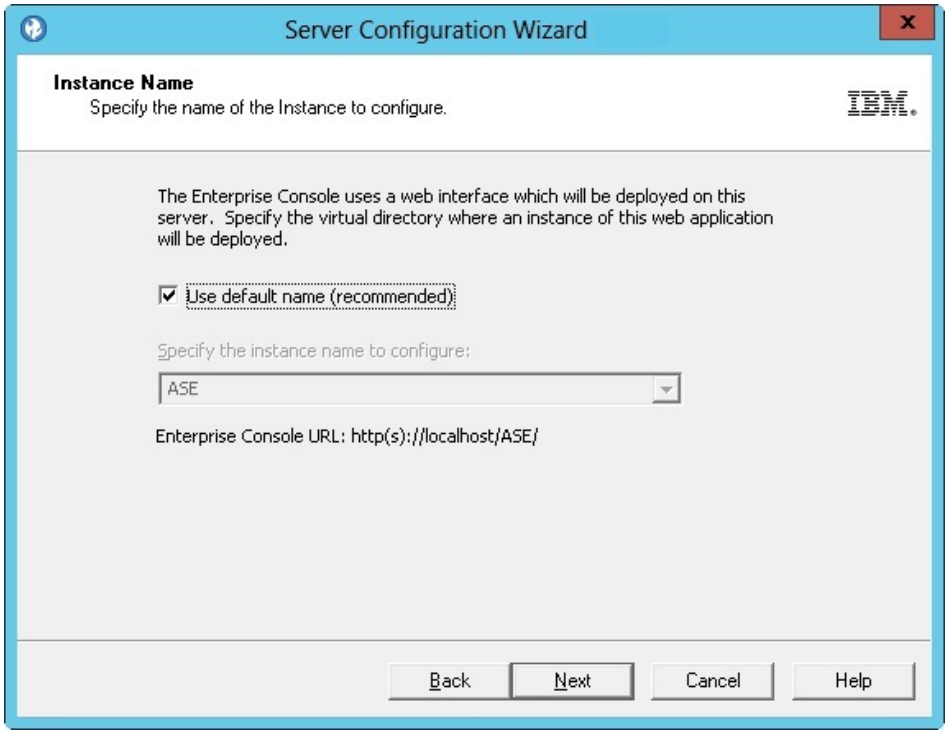


Do not check the **AppScan Source standalone evaluation** check box.

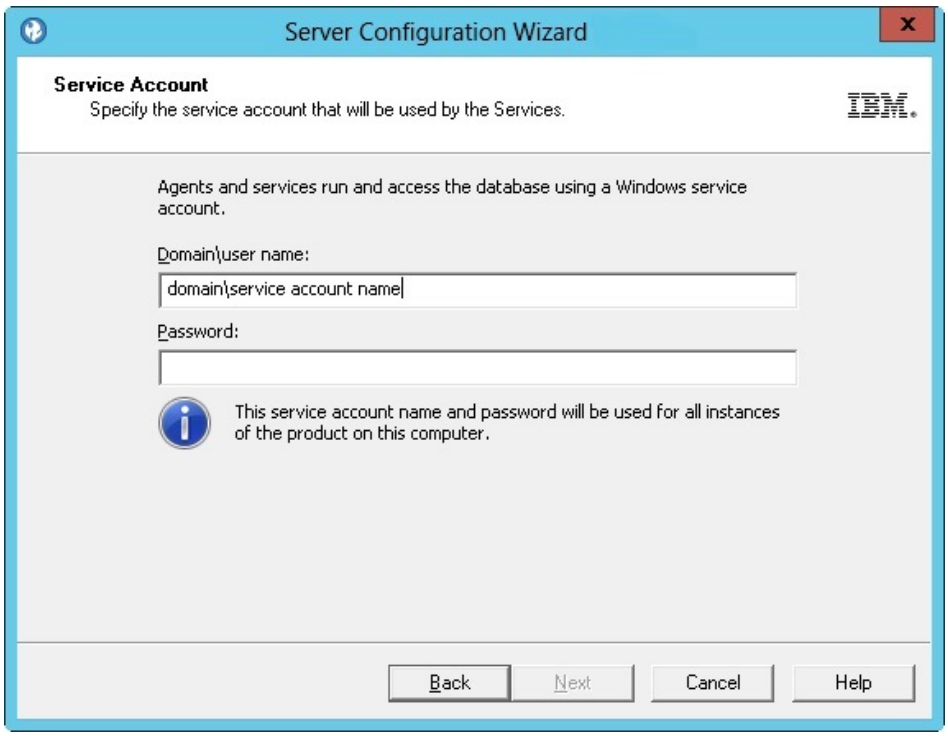
4. In the Server Components window, select the components that you want to configure. The components available to you depend on your license. See "Server Components" on page 147. **If you are installing the components on one machine, select all the check boxes, even if you have installed one of the components previously.**



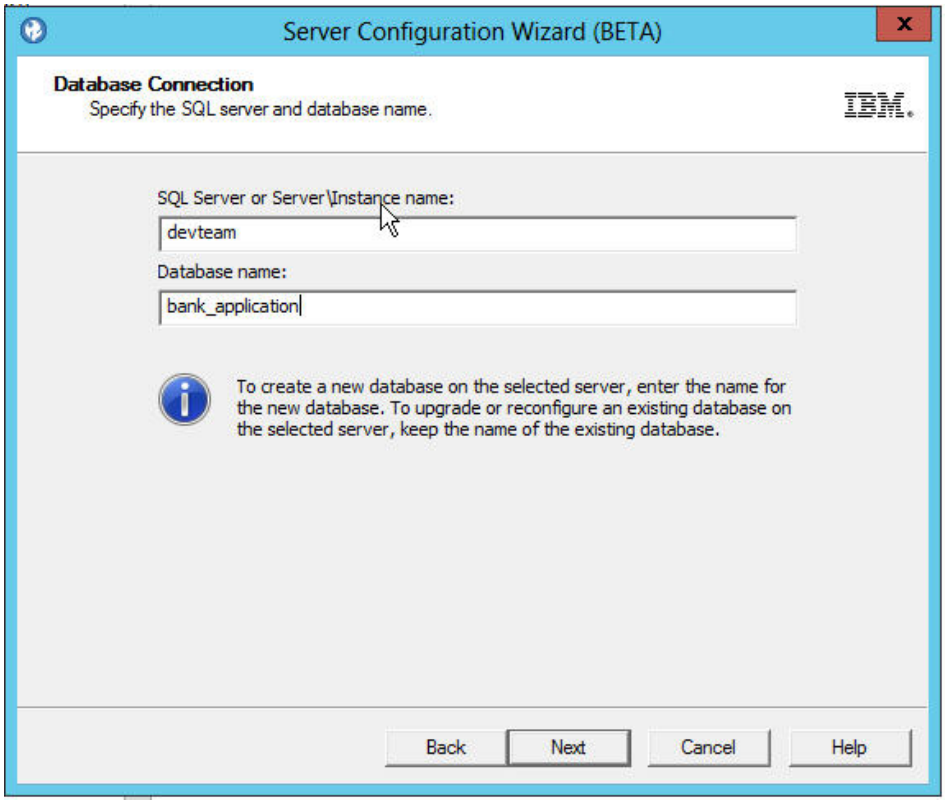
5. In the Instance Name window, specify the name of the instance you want to configure. See "Instance Name" on page 148.



6. In the Service Account window, enter the **Domain/Username Service Account** and password, and click **Next**. See "Service Account" on page 149.



7. In the Database Connection window, enter the SQL Server name, port number, and the name of the database you are connecting to. You can click **Test Connection** to make sure you can connect to the SQL Server. The configuration wizard does not proceed until the connection is successful. When AppScan Enterprise Server creates the database in SQL Server, it automatically configures the collation for it.



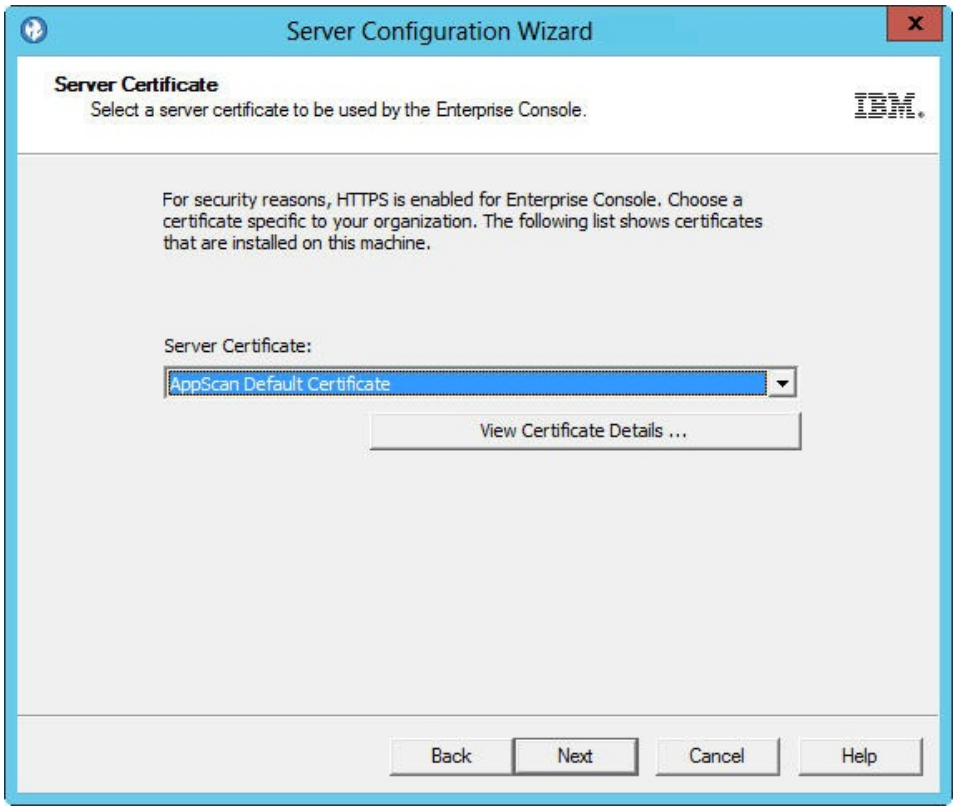
Note:

a. The syntax for the SQL Server name has changed with the introduction of Liberty support. *".\SQL_SERVER_NAME"* no longer works. Use *"HOSTNAME\SQL_SERVER_NAME"* instead.

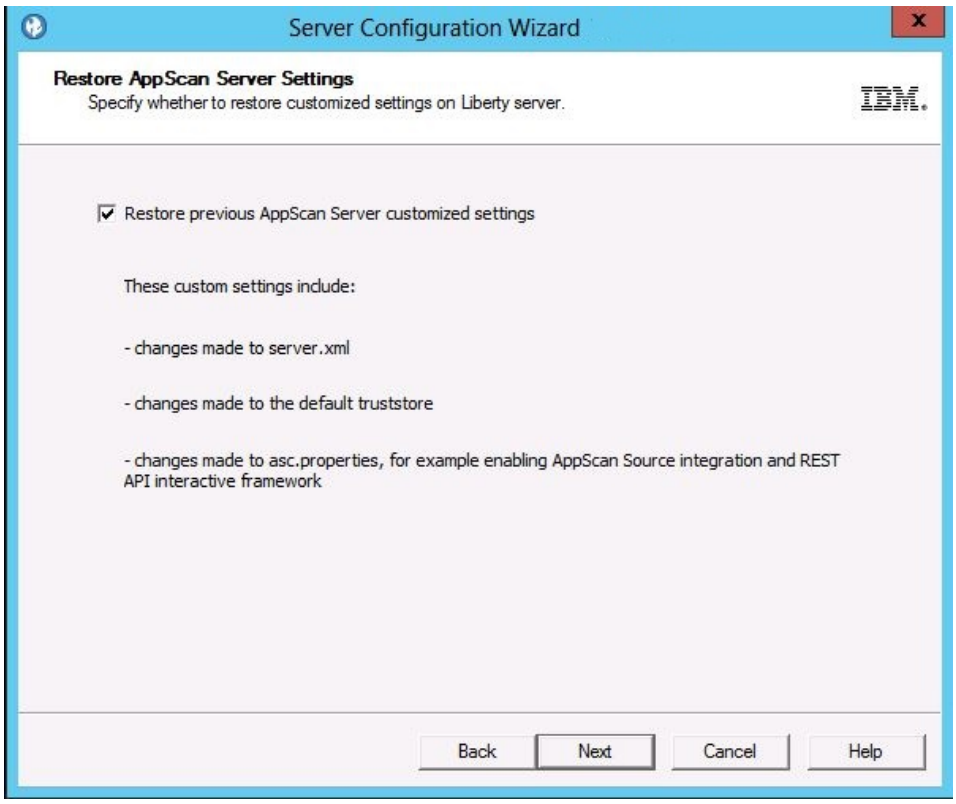
b. If you are upgrading an existing database from v8.6 or earlier, enter the **Database Master Key Password** on the next screen to access it. Keep this password in a secure location.

c. If your environment uses a named SQL Server instance for the AppScan Enterprise database or SQL Server Express, make sure that TCP/IP is enabled in the SQL Server configuration manager, and restart the SQL services for SQL Server. Use the port number of the named SQL Server instance instead of the default port number (1443).

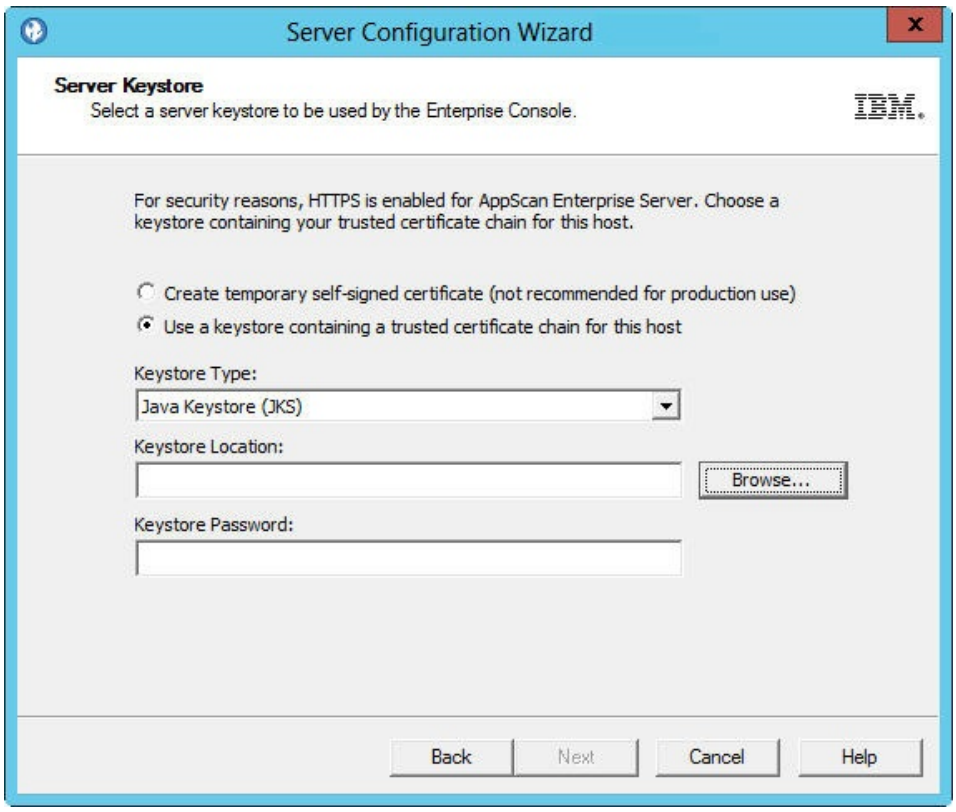
8. In the Server Certificate window, choose a certificate specific to your organization. This step helps you deploy a secure AppScan Enterprise in your environment. See “Server Certificate” on page 150.



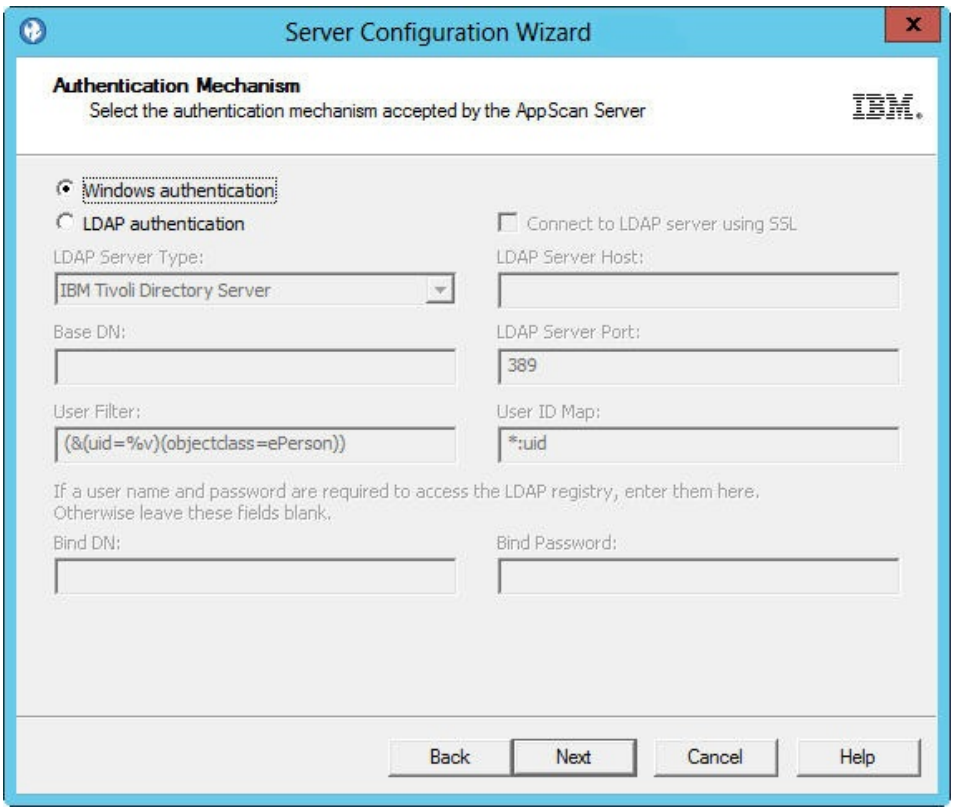
9. (Upgrade only). In the **Restore AppScan Server Settings** screen, you can choose to restore previous AppScan Server customized settings on the Liberty Server (default). This screen appears once upon upgrade; if you run the configuration wizard later, this screen won't appear. See Restore AppScan Server settings.



10. In the **Server Keystore** screen, select a server keystore to be used by the Enterprise Console. If you exported a .pfx file, select **Public key cryptography standards #12 (PKCS #12)**. Browse to the location where you saved the .pfx file, import it and enter the password you created when you exported the file. See "Server Keystore" on page 150.

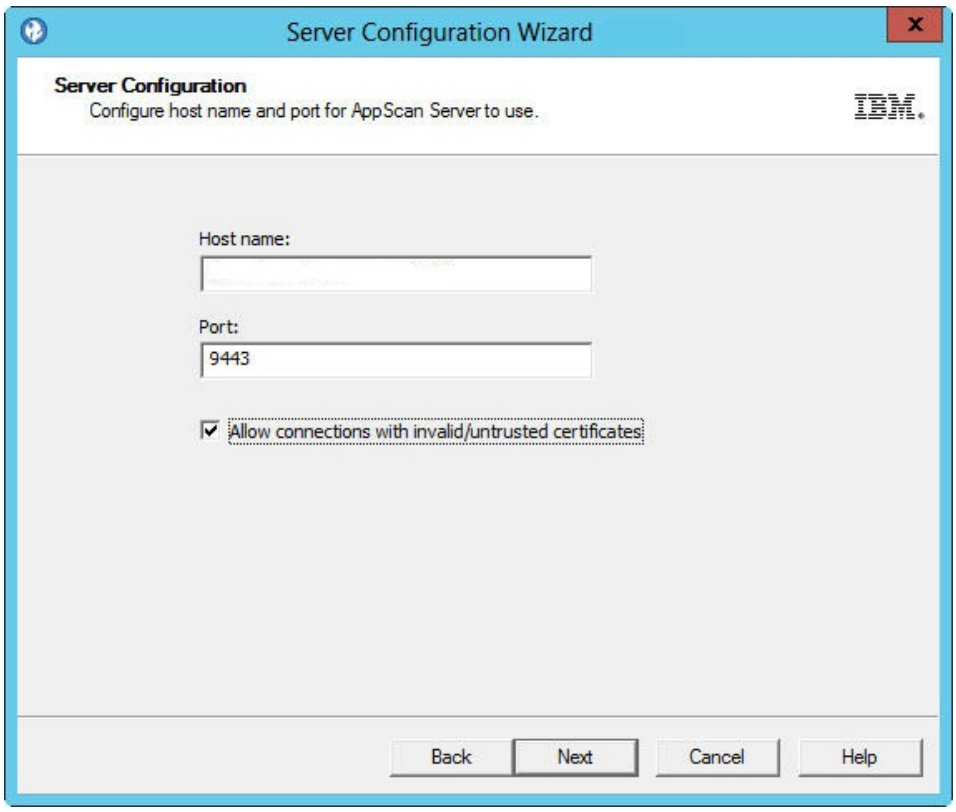


11. In the Authentication Mechanism window, select an **Authentication Mechanism** to use to log in to the Enterprise Console. The default is to authenticate via Windows. To use LDAP, see "Authentication Mechanism" on page 150.



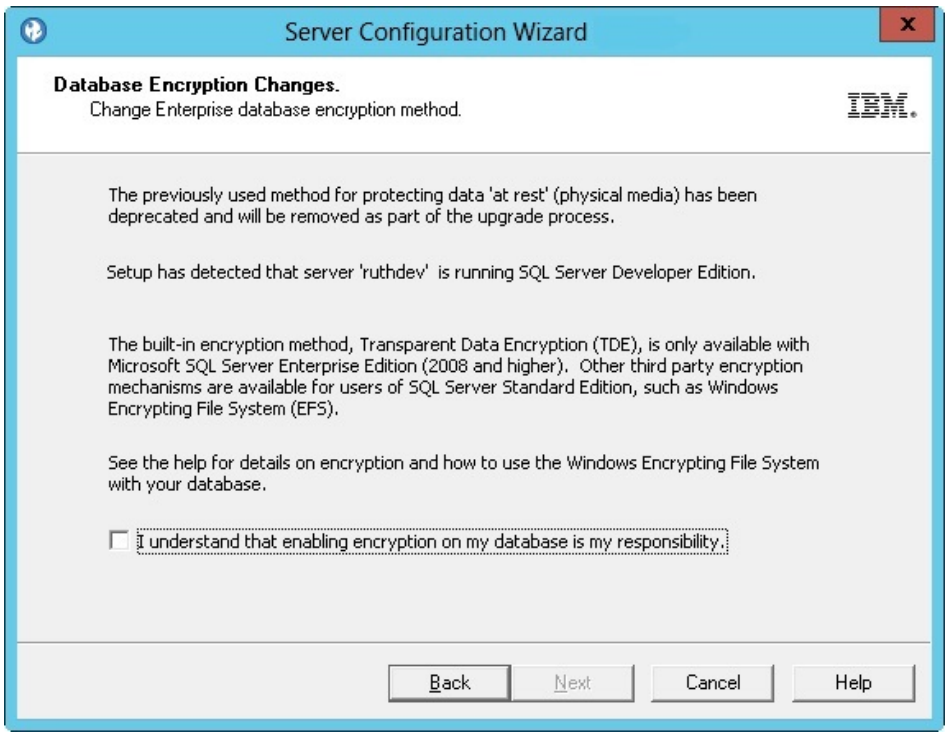
Note: If you need to authenticate with the Common Access Card (CAC), make sure you choose LDAP as your authentication mechanism. Once AppScan Enterprise is configured, follow the instructions in "Authenticating with the Common Access Card (CAC)" on page 95 to authenticate with CAC.

12. In the Server Configuration window, configure the host name and port of the Liberty server for AppScan Server to use. If you are using Windows authentication, prefix the host name with your domain name.



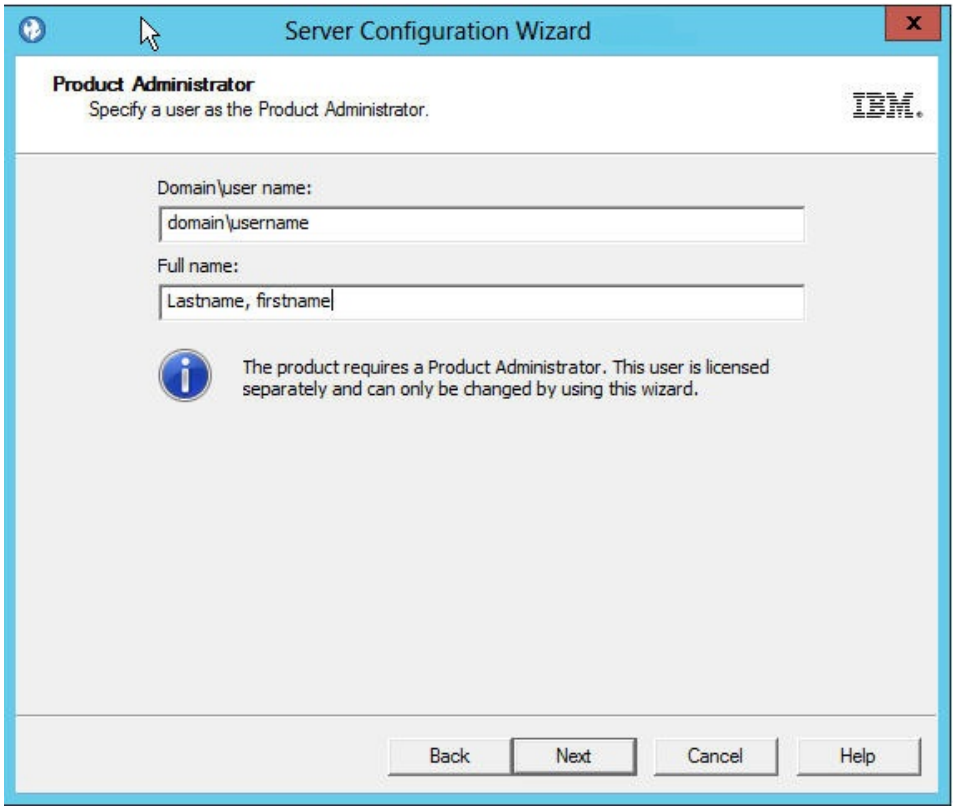
Note: While it is not a recommended practice, you can allow SSL connections with invalid or untrusted certificates during scanning. When the option is disabled, messages will appear in the scan log to indicate that the insecure server could not be reached for scanning. This option also affects the Manual Explore functionality.

13. (upgrade only) In the Database Encryption Changes window, click **Help** to learn how to protect the SQL Server where the database is located. If you decide not to enable TDE, select the check box so you can continue configuration.



Note: AppScan Enterprise uses transparent data encryption (TDE) technology that is available in SQL Server 2008 and later. TDE encrypts the data that is stored in the database or in backups on physical media. If you are using an older version of SQL Server, any data that is contained in that database is at risk of compromise by unauthorized access.

14. In the Product Administrator window, specify a user as Product Administrator. This user is licensed separately; if you want to reassign the Product Administrator license, you must rerun the configuration wizard. See "Product Administrator" on page 151.



15. Ensure that nobody is accessing the database, and click **Finish** in the Specifications Complete window to complete the configuration. This process might take awhile.

    Note:

    a. IIS AppPool settings on Windows 2008 Server R2 are set during configuration:
       - IIS recycling is set at 2:00am
       - Idle timeout is set at 120 minutes

    b. If you see an error message that the proxy server certificate cannot be configured, it might be expired. Contact your Product Administrator to investigate further.

16. Optional: Select the **Start the Services** check box to automatically start the services.

    Note: If you do not choose to automatically start the agent service, the agents do not pick up any jobs that are created by users. You can manually start the service by using the Administrative tools; see "Verifying the agent service and alerting service installation" on page 81.

17. Run the **Default Settings Wizard**. This wizard helps you to install sample data in by providing defaults for a number of configurable options.
18. Click **Exit**.

Running the Default Settings wizard:

This wizard helps you install sample data in by providing defaults for a number of configurable options. You can create users, add security test policies, create scan

templates, add pre-created dashboards, and configure defect tracking integration with Rational Quality Manager or Rational Team Concert.

About this task

Ensure that the **Launch Default Settings Wizard** check box is selected when the Configuration wizard finishes.

Procedure

1. In the Welcome page, choose the instance that you want to update, and click **Next**.
2. In the Initialization Type window, select one of the available initializations, and click **Next**.
3. In the Default Setting window, configure the following options and click **Next**:
   a. **Instance**: Select the instance name for this setup. The Instance that was configured in the Configuration wizard is selected here by default.
   b. **Contact**: The name or a point of contact for the items that are created by the wizard. You can edit these items later if necessary.
   c. **Root folder name**: Enter a name for the default root folder. The default folder acts as the root folder for all other folders you create.
   d. **Application URL**: Enter the URL for the application users to access the application. By default, this URL is the current computer's FQDN (fully qualified domain name). (for example, `http://myserver/mydomain/appscan/`).
4. (Windows authentication only): In the LDAP Settings page, select the **Enable LDAP** check box if you use an LDAP server.
   a. In the **Server Name** field, enter the LDAP group name.
   b. In the **Group Query** field, enter the path of the group query that is used to retrieve user group information. You can use an LDAP server or an Active Directory server.
   c. Optional: If you want to integrate with the LDAP server by using anonymous access, select the **Anonymous access** check box. This option is disabled by default.
   d. Click **Test LDAP** to confirm the configuration works.
5. In the IP Security Permissions page, configure the IP addresses and ranges that are allowed for scanning. Use a dash to define IPv4 ranges (such as 1.2.3.4–); use a prefix to define IPv6 ranges (such as fe80::/10).
6. In the Populate Database with Sample Data page, select the **Populate Sample Data** check box to populate the database with scan templates, pre-created dashboards, server groups, and test policies.
7. Click **Next**. The Default Settings Wizard Progress page opens, displaying the setup's progress.
8. When the wizard is complete, the Default Settings Wizard Complete page opens.
9. Click **Exit** to close the wizard.

Installing IBM Security Dynamic Analysis Scanner:

Use this procedure to install the agents that are used for scanning and testing your website applications.

Before you begin

Note:

1. Make sure you read "Required user account information during installation and configuration" on page 22 so that you know which user account to use during installation.
2. Any technologies that you use on your website must also be installed with the Scanner. For example, if you use Flash on any web pages, you must have the correct version of Flash installed.

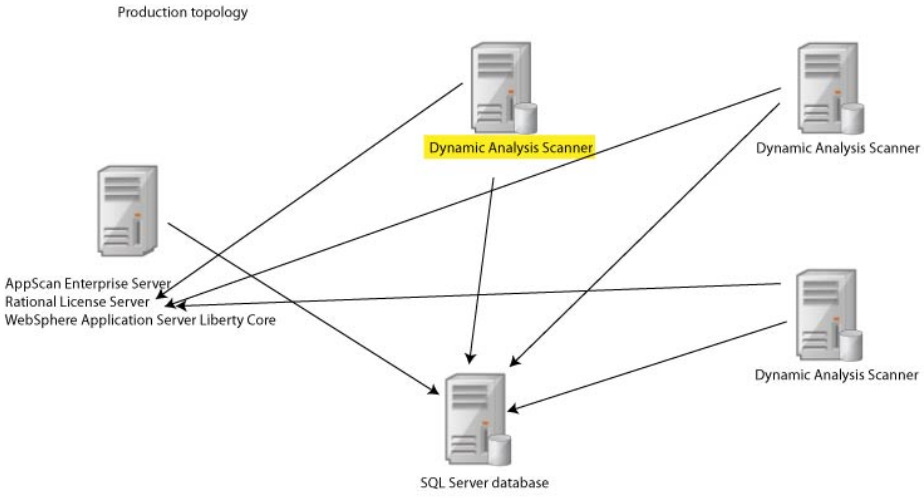
Procedure

1. Go to the directory where you downloaded the executable file (`ASE_DASSetup_<version>.exe`) and double-click the file.

   Note: It might take a while for the next screen to display.
2. In the License Agreement window, select the **I accept the terms in the license agreement** option, and click **Next**.
3. Optional: In the Program Features window, select **Web Services Explorer** to add the ability to test web services for security vulnerabilities, and click **Next**.

   Note: Approximately 330 MB is required for the Web Services Explorer – GSC (Generic Service Client tool) version 8.1 that is used to test Web Services for security vulnerabilities
4. In the Destination Folder window, click **Next**.
5. In the Ready to Install the Program window, click **Install** to proceed with the installation, and then click **Finish**.

Results



Running the Configuration wizard:

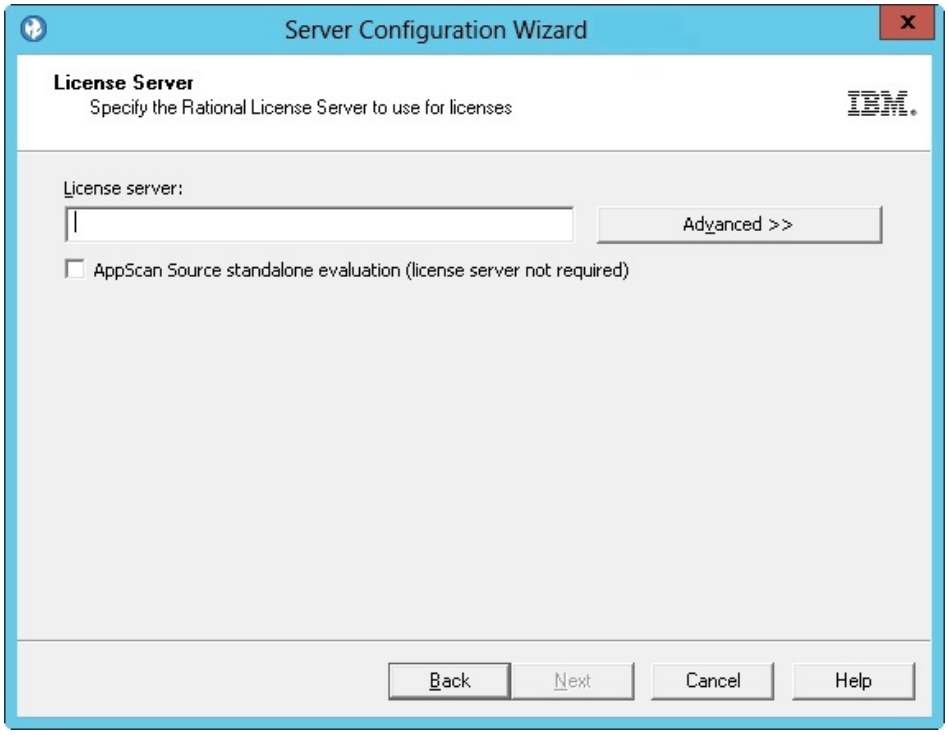
After you install or upgrade the Server or Scanner, you must configure each installed component and run the Configuration wizard on all instances and on all servers.

Before you begin

1. During configuration, you define the name and location of the SQL Server database to be used, and the service account name and password. The user who runs the configuration wizard must be able to create a database and grant rights.
2. Running the wizard after you install the AppScan Enterprise Server sets up the database on the SQL Server and does the initial setup of the component.
3. Running the wizard after you install the Dynamic Analysis Scanner registers the Scanner with AppScan Enterprise Server.

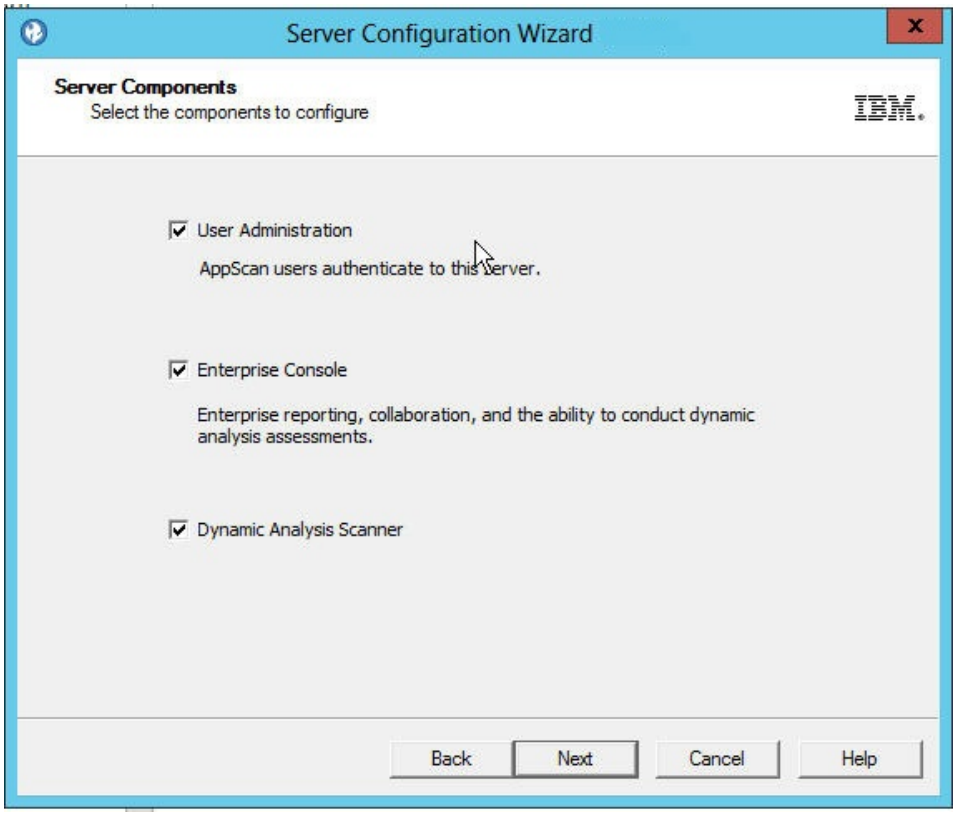
Procedure

1. When the installation is complete, the Configuration wizard launches automatically. You can also start it by selecting **Configuration Wizard** from the Windows **Start** menu.
2. In the Welcome screen, click **Next**.
3. In the License Server window, specify the Rational License Server to use for licenses. See "License Server" on page 147.

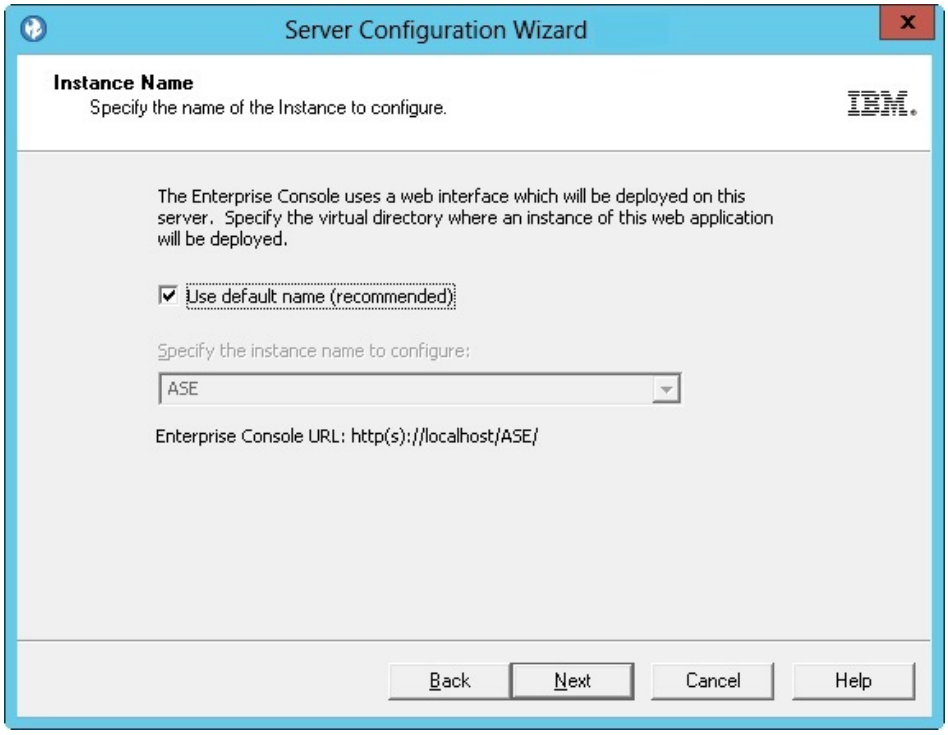


Do not check the **AppScan Source standalone evaluation** check box.

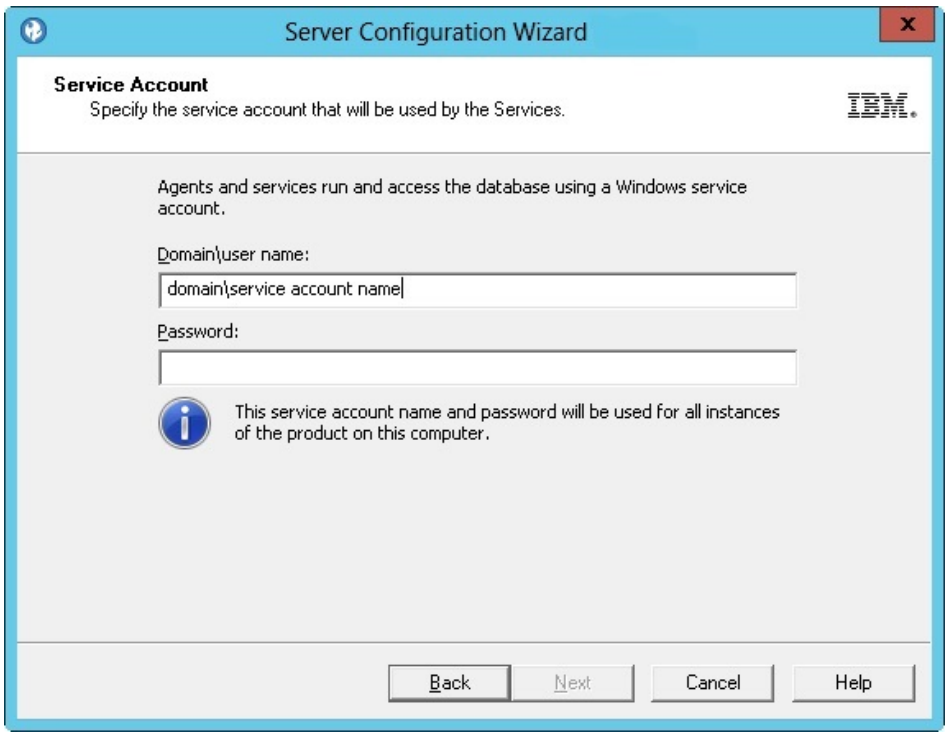
4. In the Server Components window, select the components that you want to configure. The components available to you depend on your license. See "Server Components" on page 147. **If you are installing the components on one machine, select all the check boxes, even if you have installed one of the components previously.**



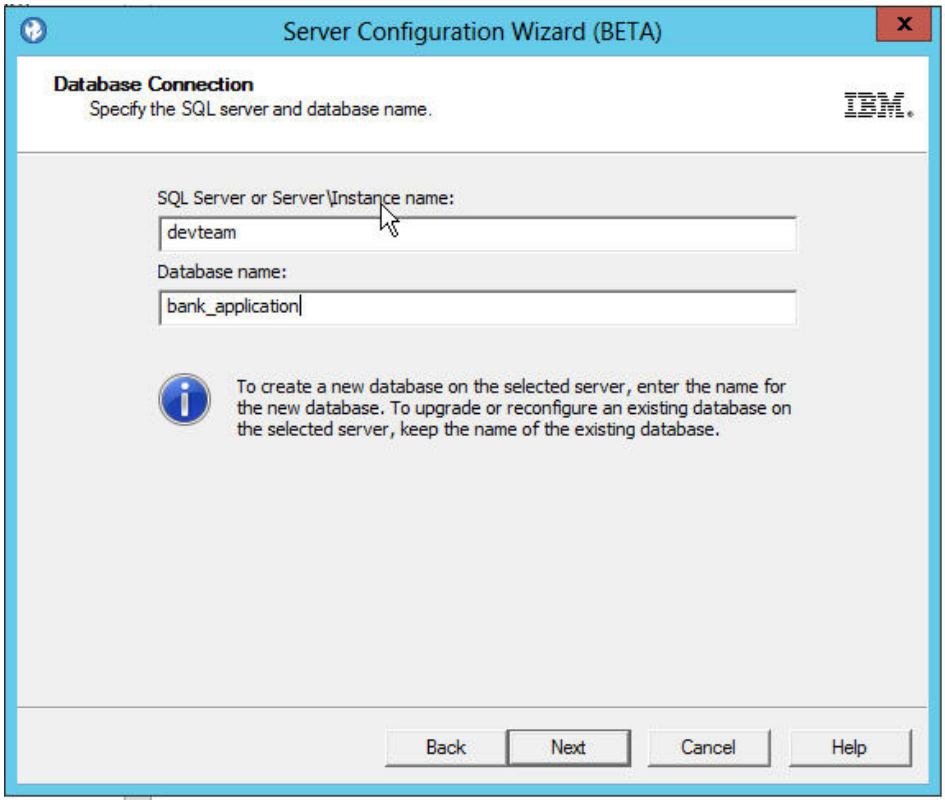
5. In the Instance Name window, specify the name of the instance you want to configure. See "Instance Name" on page 148.



6. In the Service Account window, enter the **Domain/Username Service Account** and password, and click **Next**. See "Service Account" on page 149.



7. In the Database Connection window, enter the SQL Server name, port number, and the name of the database you are connecting to. You can click **Test Connection** to make sure you can connect to the SQL Server. The configuration wizard does not proceed until the connection is successful. Enter the database name. When AppScan Enterprise Server creates the database in SQL Server, it automatically configures the collation for it.

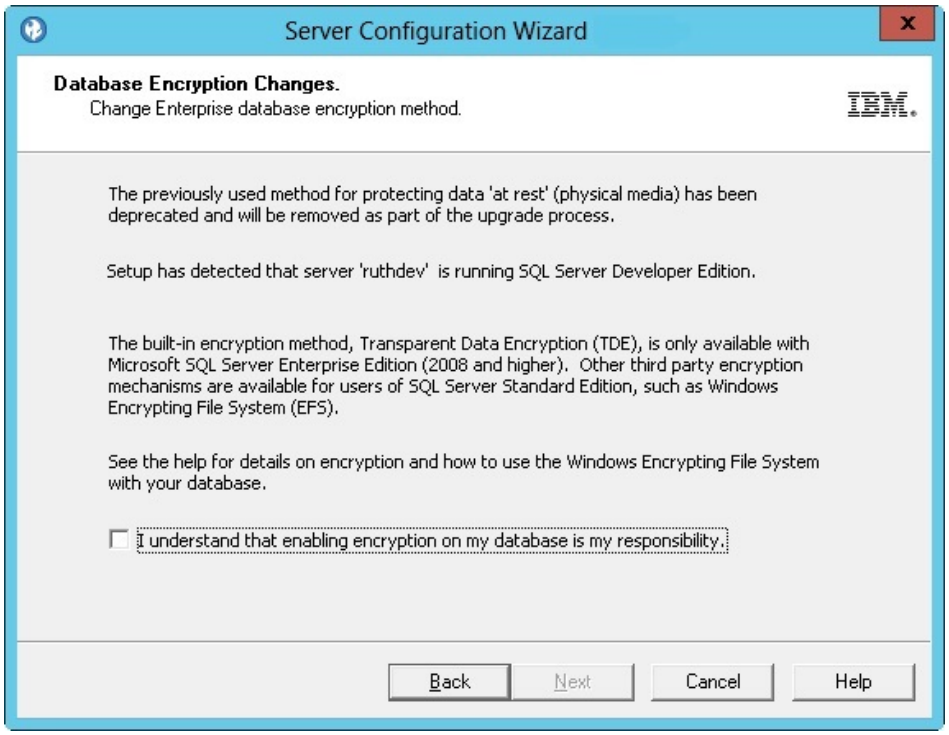


Note:

a. If you are upgrading an existing database from v8.6 or earlier, enter the **Database Master Key Password** on the next screen to access it. Keep this password in a secure location.

b. If your environment uses a named SQL Server instance for the AppScan Enterprise database or SQL Server Express, make sure that TCP/IP is enabled in the SQL Server configuration manager, and restart the SQL services for SQL Server. Use the port number of the named SQL Server instance instead of the default port number (1443).

8. (upgrade only) In the Database Encryption Changes window, click **Help** to learn how to protect the SQL Server where the database is located. If you decide not to enable TDE, select the check box so you can continue configuration.



Note: AppScan Enterprise uses transparent data encryption (TDE) technology that is available in SQL Server 2008 and later. TDE encrypts the data that is stored in the database or in backups on physical media. If you are using an older version of SQL Server, any data that is contained in that database is at risk of compromise by unauthorized access.

9. Ensure that nobody is accessing the database, and click **Finish** in the Specifications Complete window to complete the configuration. This process might take awhile.

Note:

a. IIS AppPool settings on Windows 2008 Server R2 are set during configuration:
   - IIS recycling is set at 2:00am
   - Idle timeout is set at 120 minutes

b. If you see an error message that the proxy server certificate cannot be configured, it might be expired. Contact your Product Administrator to investigate further.

10. Optional: Select the **Start the Services** check box to automatically start the services.

    Note: If you do not choose to automatically start the agent service, the agents do not pick up any jobs that are created by users. You can manually start the service by using the Administrative tools; see "Verifying the agent service and alerting service installation" on page 81.

11. Click **Exit**.

Verifying the installation of the Enterprise Console:

After the installation process is complete, you can verify the installation of the Enterprise Console.

Procedure

Go to https://localhost/ase/ and log in.

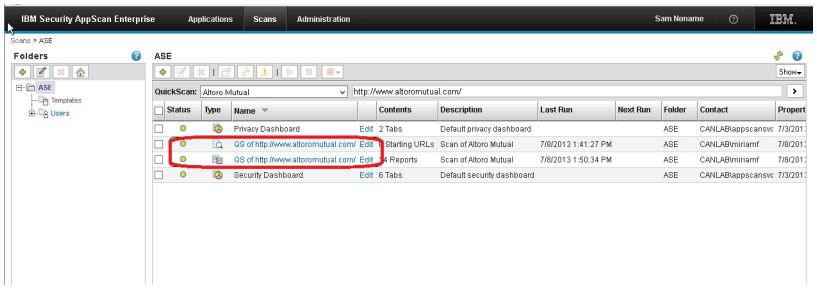
Verifying the scanner installation:

Run a QuickScan to verify that the agents installed properly. It is a simple way to make sure that everything is working before you start configuring more complex web application scans.

Procedure

1. In the Scans view, select *AltoroMutual* from the list QuickScan template list, and click the **Create QuickScan** icon. This scans the Altoro Mutual website, which is published by IBM Corporation for the sole purpose of demonstrating the effectiveness of AppScan in detecting web application vulnerabilities and website defects.
2. Install the Manual Explore plug-in from the pop-up window. Close the window and click **Run** to start the scan.
3. When the scan is completed, click **Close** to return to the folder explorer view. Two items that are called *QS of http://www.altoromutual.com/* are added to the view: a scan job and a report pack. Look at the Status column. When both items are in a **Ready** state, you can click the report pack link and see the scan results.

Results



Related concepts:

"Installing multiple instances of the Enterprise Console on a single server" on page 98
You have the option of installing a default instance, or multiple instances on a single computer. Each instance is an independent set of configuration information with its own database.

Installing the required components in a multi-machine environment

AppScan Enterprise components can be installed on multiple machines. In this scenario, components are deployed in a multi-machine environment. Rational® License Server, AppScan Enterprise Server, AppScan Dynamic Analysis Scanner, and the SQL Server Database are all installed on different machines.

About this task

This scenario is divided into seven sections:

- "Installing IBM Rational License Server on Machine A"
- "Installing AppScan Enterprise Server on Machine B" on page 61
- "Running the Configuration wizard" on page 63
- "Running the Default Settings wizard" on page 73
- "Verifying the installation of the Enterprise Console" on page 74
- "Installing IBM Security Dynamic Analysis Scanner on Machine C" on page 75
- "Running the Configuration Wizard on the Scanner" on page 76
- Verifying the scanner installation

Note:

1. This scenario assumes that you have installed and configured the SQL Server Database so that key information is available during configuration of AppScan Enterprise Server.
2. If you already have a Rational License Key Server deployed on your network, skip to the "Installing AppScan Enterprise Server on Machine B" on page 61 task.
3. If you are upgrading from a previous version of AppScan Enterprise, read "Replacing Jazz Team Server with WebSphere Liberty - Frequently asked questions" on page 108 before you begin upgrading.
4. To migrate Jazz Team Users users to use the Liberty authentication method, export a .csv file of users by using the **cd <install-dir>\Appscan Enterpise\JazzTeamServer\server\ repotools-jts.bat -exportUsers toFile=C:\users.csv repositoryURL=https://<hostname>:9443/jts** before you begin upgrading to v9.0.1. Then follow the steps in this topic: Configuring a basic user registry for the Liberty profile to import the users into Liberty.

Installing IBM Rational License Server on Machine A:

The Rational License Key Server is used for hosting your AppScan Enterprise Server license. If you do not have a Rational License Key Server on your network, you can install it locally when you install AppScan Enterprise Server.

About this task

If you already have a supported version of Rational License Server that is installed, you can skip the portion of these instructions that cover Rational License Server installation - and proceed to the portion of the instructions that covers starting

License Key Administrator and importing your license.)

Procedure

1. Go to the directory where you downloaded the executable file (`AppScanEnterpriseServerSetup_<version>.exe`) and double-click the file. (The Rational License Key Server is bundled in this .exe file.)

   Note: It might take a while for the next screen to display.
2. Click **Yes** when you are asked to install Rational License Key Server.
3. In the Rational License Server installer, click **Install or Update IBM Rational License Key Server**.
4. If IBM Installation Manager is not already installed on your system, it launches for installation purposes. Click **Install**.
5. On the first page of the Install Packages wizard, ensure that the **IBM Rational License Key Server** check box, and check boxes for all entries beneath it, are selected. Click **Next**.
6. In the Prerequisites page, you are instructed to close all applications and disable anti-virus software. Complete these precautionary tasks and then click **Next**.
7. On the Licenses page, read the license agreement. If you agree to the terms of the license agreement, click **I accept the terms in the license agreement** and then click **Next**.
8. In the Location page, specify the installation directory and then click **Next**.
9. Complete the Package Group page according to your needs (for example, if you are using Installation Manager for the first time and have no existing package group, leave the default settings as-is). Click **Next**.
10. In the Translation Selection page, select the national languages that you want to install. Click **Next**.
11. On the Features page, ensure that all features are selected and then click **Next**.
12. A summary of what is installed is shown on the Summary page. If you want to change your selections, click **Back** to return to the previous pages. When you are satisfied with your installation choices, click **Install**.
13. When the installation is complete, click **Finish** and close IBM Installation Manager.
14. Start the IBM Rational License Key Administrator from the **Windows Start** menu (in the **Programs** menu, launch **IBM Rational** > **License Key Administrator**).
15. When the IBM Rational License Key Administrator starts, you are prompted with the License Key Administrator wizard (if the wizard does not open automatically, select **License Keys** > **License Key Wizard** from the main menu). In this wizard, select **Import a Rational License File** and then click **Next**.
16. In the Import a License File panel, click **Browse** and then browse to your AppScan Enterprise Server license file. Open the file with the browse dialog box and then click **Import**. This table maps the license names in LKAD to the license types in AppScan Enterprise.

Table 12. AppScan Enterprise licenses

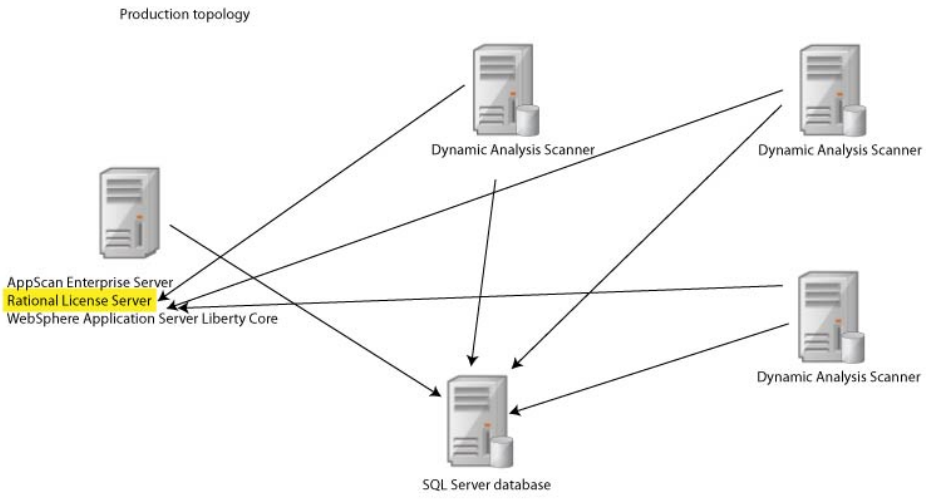
License	What it is for
AppScan Enterprise Dynamic Analysis Scanner Per Install License Key	Dynamic Analysis Scanner

Table 12. AppScan Enterprise licenses (continued)

License	What it is for
AppScan Enterprise Dynamic Analysis User Authorized User Single Install License Key	Authorized Scanning
AppScan Enterprise Dynamic Analysis User Floating User Single Install License Key	Floating Scanning
AppScan Enterprise Server Basic Per Install License Key	Enterprise Server Basic
AppScan Enterprise Server Per Install License Key	Enterprise Server Premium
Appscan Enterprise Edition Reporting Only User Authorized User Single Install License Key	Authorized Reporting
Appscan Enterprise Edition Reporting Only User Floating User Single Install License Key	Floating Reporting

17. After you confirm the license or licenses to import, the Restart License Server dialog box will open. Click **Yes** to restart the license server. If the License Server service fails to start, open the Windows Services administrative tool. In the tool, locate **FLEXlm License Manager** and start it.

Results



Installing AppScan Enterprise Server on Machine B:

Use this procedure to install the User Administration component and Enterprise Console for reporting and user administration tasks.

Before you begin

Make sure you read "Required user account information during installation and configuration" on page 22 so that you know which user account to use during installation.

About this task

If you have a Rational License Key Server that is already deployed elsewhere on your network, start at Step 1; otherwise start at Step 2.

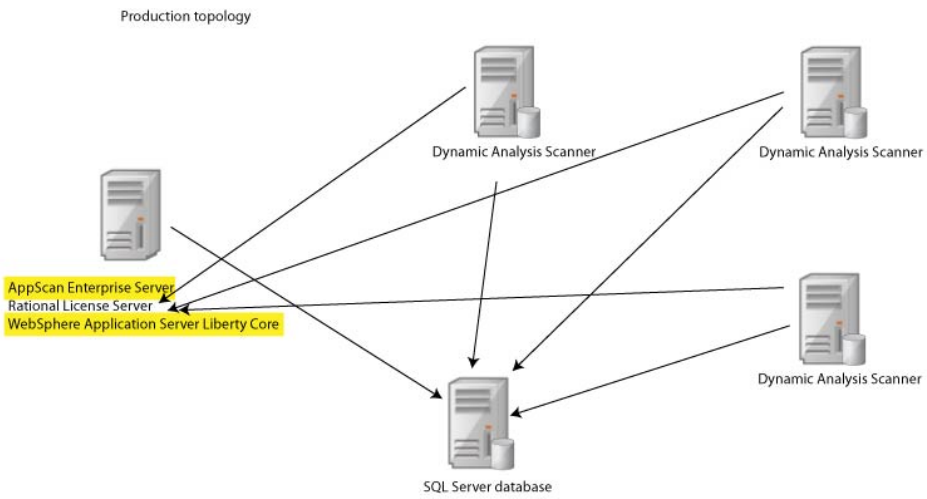
Procedure

1. Go to the directory where you downloaded the compressed file (`AppScanEnterpriseServerSetup_<version>.zip`), extract the files, and double-click the `AppScanEnterpriseServerSetup_<version>.exe` file.

   Note: It might take a while for the next screen to display. The compressed file includes these files:

   - `AppScanEnterpriseServerSetup_<version>.exe`
   - `IBM Security AppScan Enterprise Server.msi` - **do not run this file**
   - `Data1.cab`
2. If you do not already have Rational License Key Server that is installed on your network, install it when prompted, and follow the procedure in the **Installing Rational License Key Server** task. Otherwise, click **No**.
3. In the Setup wizard Welcome screen, click **Next**.
4. In the License Agreement window, select the **I accept the terms in the license agreement** option, and click **Next**.
5. In the Destination Folder window, do one of the following actions and click **Next**:
   a. Click **Next** to accept the default installation location.
   b. Click **Change** to select a different installation location.
6. In the Ready to Install the Program window, click **Install** to proceed with the installation.
7. On the Setup Wizard Completed screen, click **Finish** to launch the Configuration Wizard.

Results



Running the Configuration wizard:

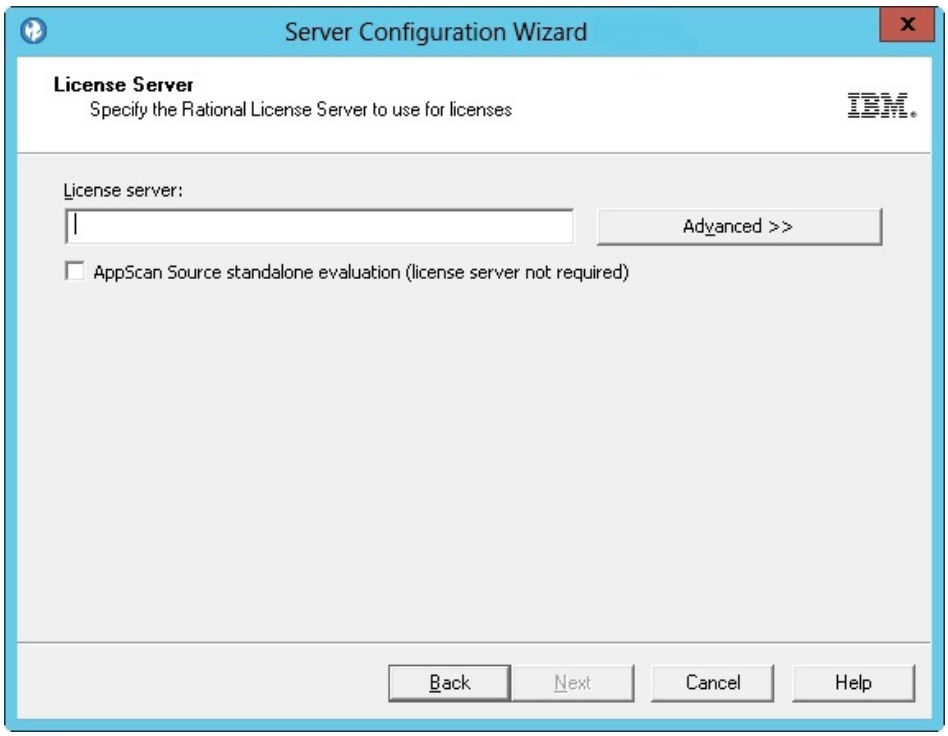
After you install or upgrade the Server or Scanner, you must configure each installed component and run the Configuration wizard on all instances and on all servers.

Before you begin

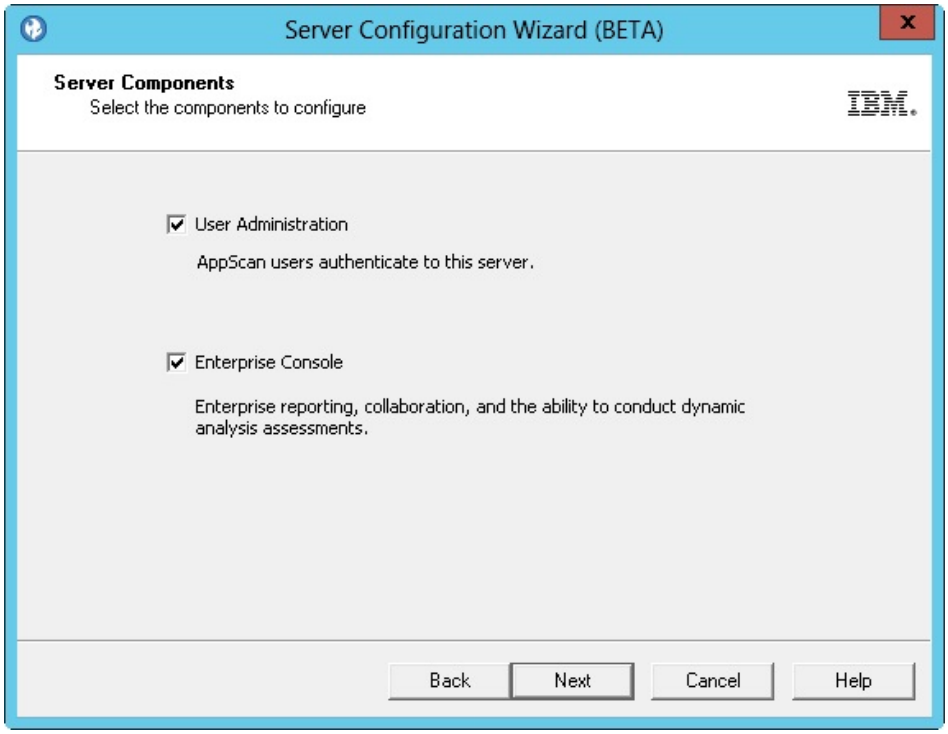
1. During configuration, you define the name and location of the SQL Server database to be used, and the service account name and password. The user who runs the configuration wizard must be able to create a database and grant rights.
2. Running the wizard after you install the AppScan Enterprise Server sets up the database on the SQL Server and does the initial setup of the component.
3. Running the wizard after you install the Dynamic Analysis Scanner registers the Scanner with AppScan Enterprise Server.

Procedure

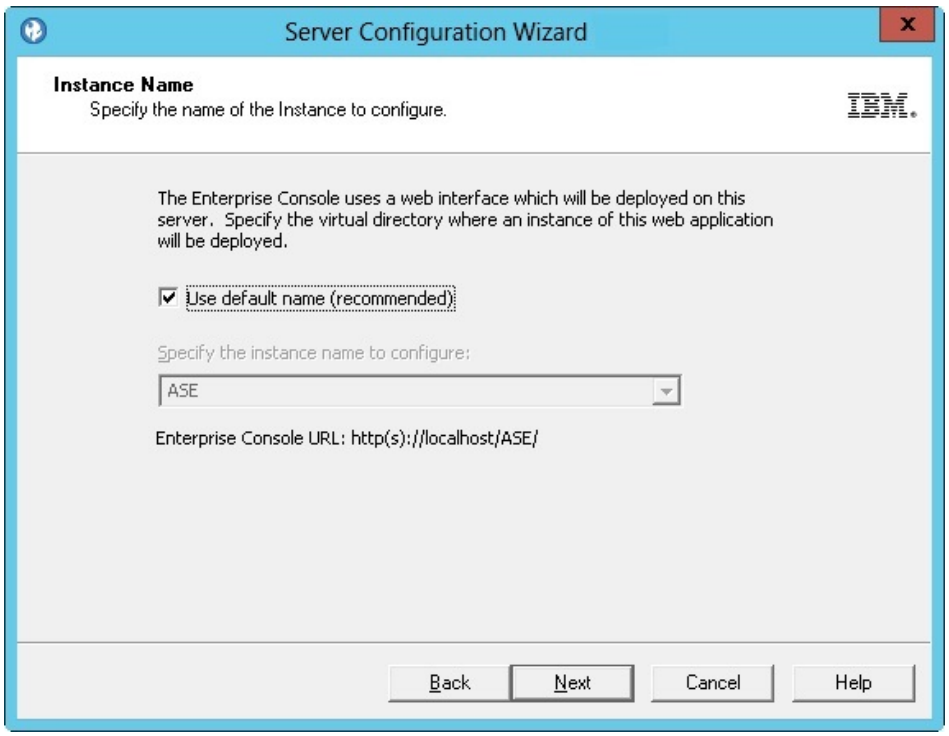
1. When the installation is complete, the Configuration wizard launches automatically. You can also start it by selecting **Configuration Wizard** from the Windows **Start** menu.
2. In the Welcome screen, click **Next**.
3. In the License Server window, specify the Rational License Server to use for licenses. See “License Server” on page 147.



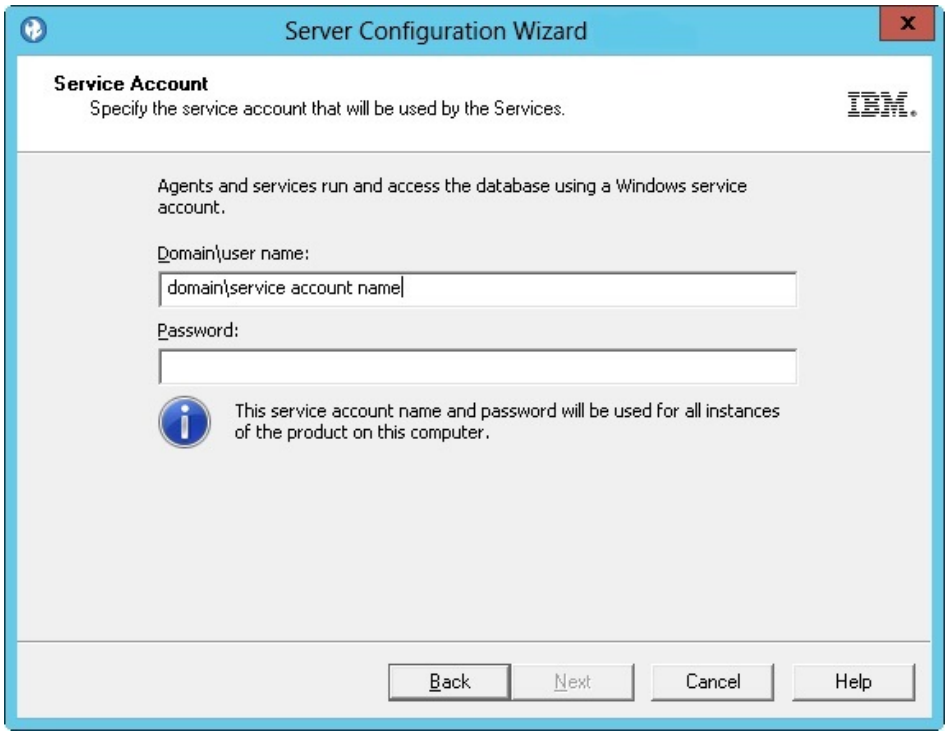
4. In the Server Components window, select the components that you want to configure. The components available to you depend on your license. See "Server Components" on page 147. **If you are installing the components on one machine, select all the check boxes, even if you have installed one of the components previously.**



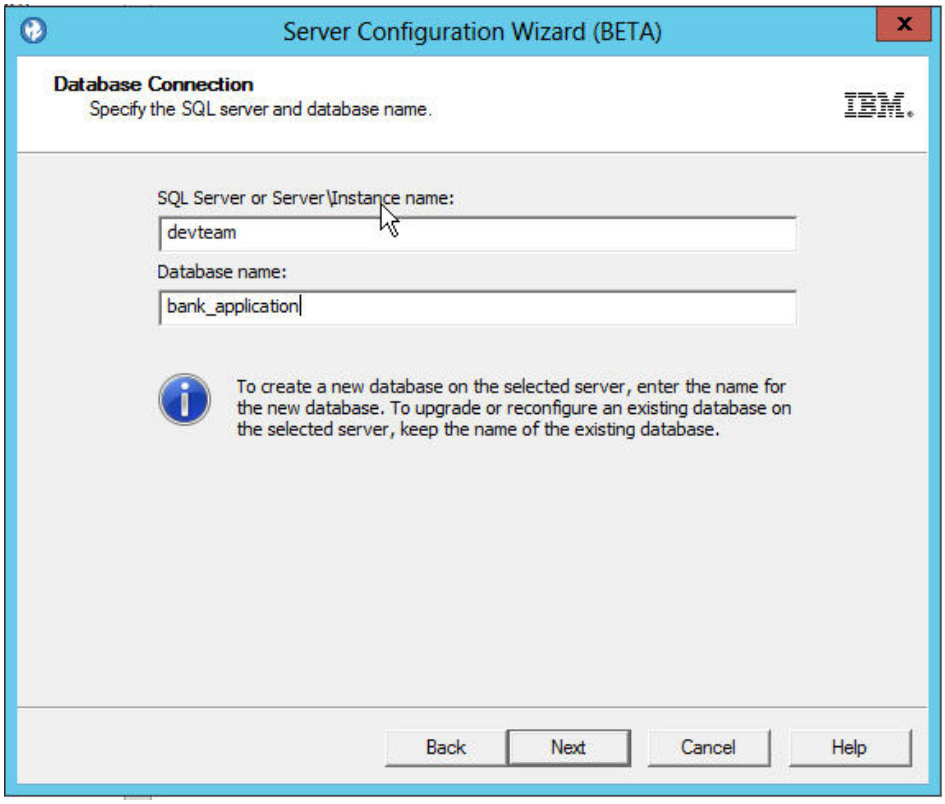
5. In the Instance Name window, specify the name of the instance you want to configure. See "Instance Name" on page 148.



6. In the Service Account window, enter the **Domain/Username Service Account** and password, and click **Next**. See "Service Account" on page 149.



7. In the Database Connection window, enter the SQL Server name, port number, and the name of the database you are connecting to. You can click **Test Connection** to make sure you can connect to the SQL Server. The configuration wizard does not proceed until the connection is successful. When AppScan Enterprise Server creates the database in SQL Server, it automatically configures the collation for it.

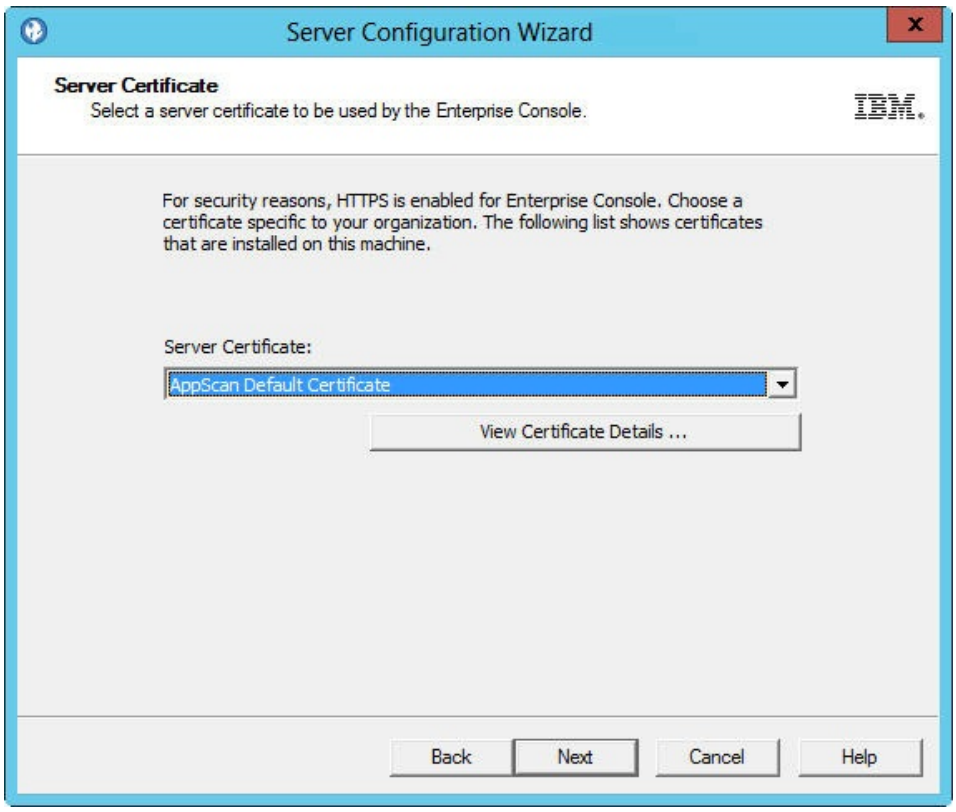


Note:

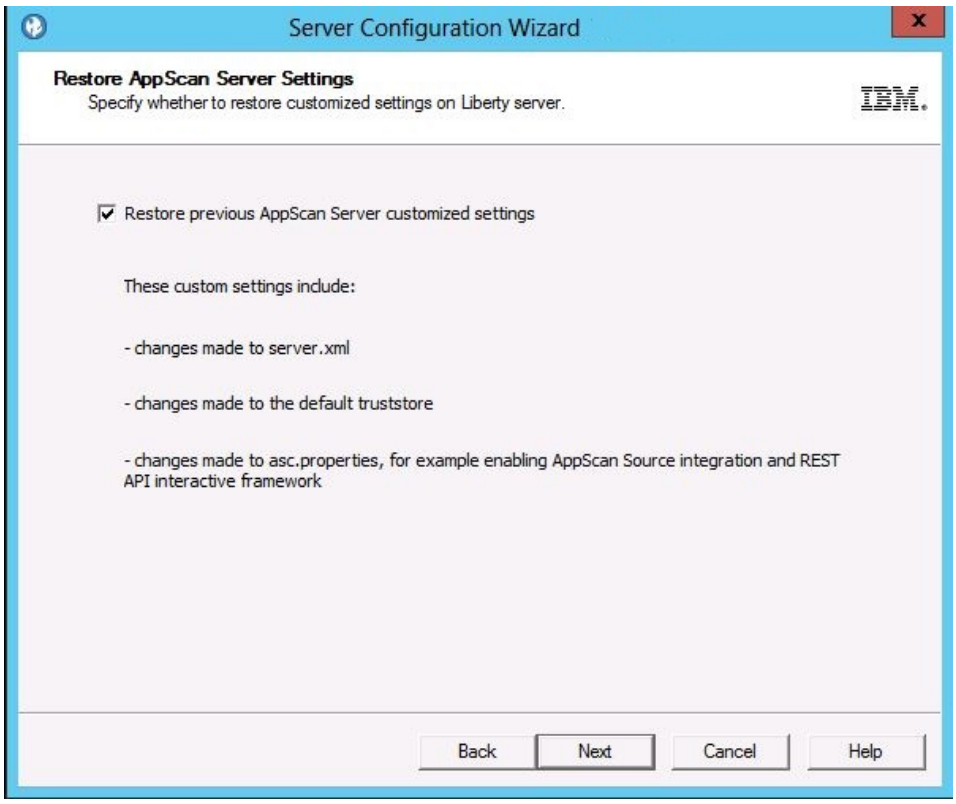
a. If you are upgrading an existing database from v8.6 or earlier, enter the **Database Master Key Password** on the next screen to access it. Keep this password in a secure location.

b. If your environment uses a named SQL Server instance for the AppScan Enterprise database or SQL Server Express, make sure that TCP/IP is enabled in the SQL Server configuration manager, and restart the SQL services for SQL Server. Use the port number of the named SQL Server instance instead of the default port number (1443).

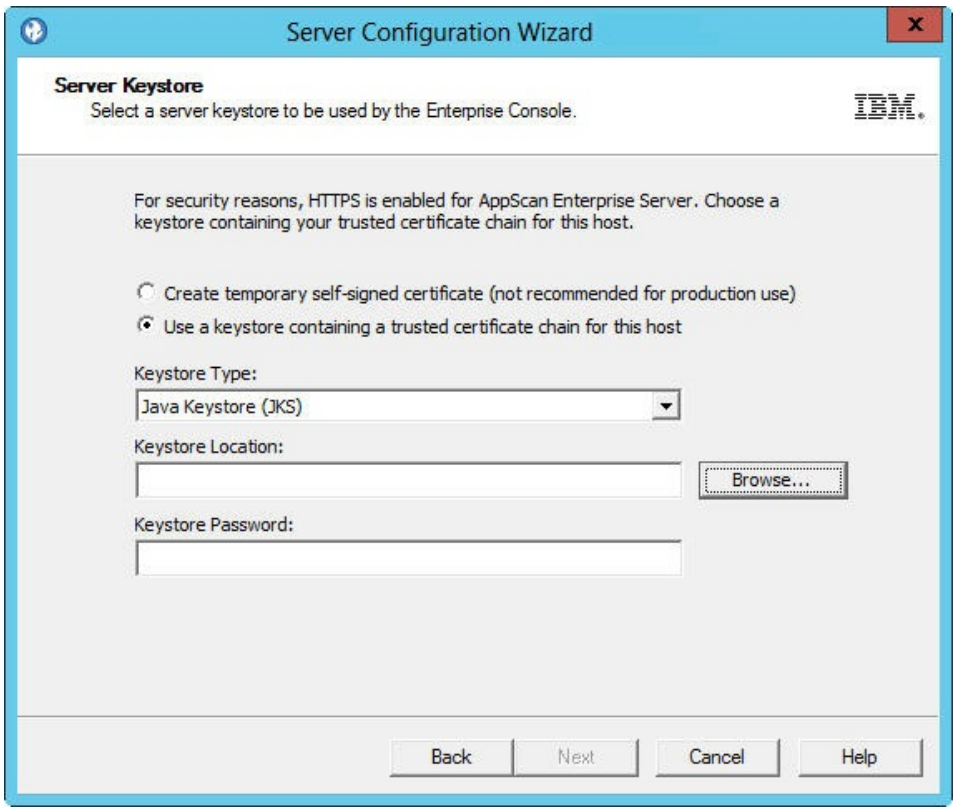
8. In the Server Certificate window, choose a certificate specific to your organization. This step helps you deploy a secure AppScan Enterprise in your environment. See “Server Certificate” on page 150.



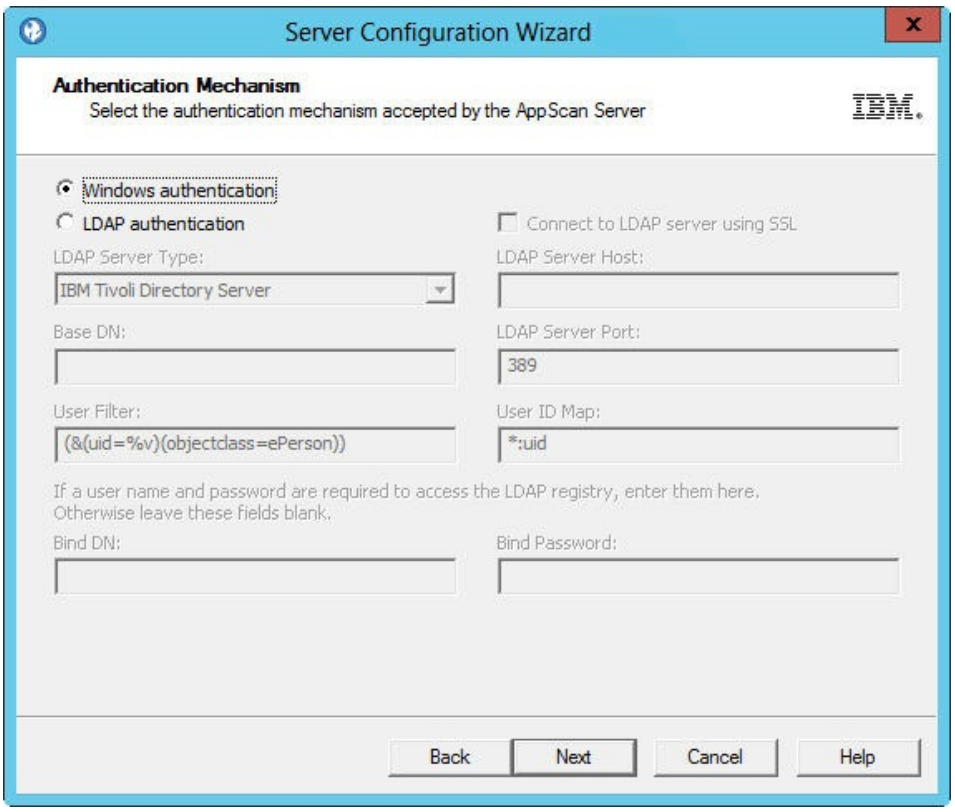
9. (Upgrade only). In the **Restore AppScan Server Settings** screen, you can choose to restore previous AppScan Server customized settings on the Liberty Server (default). This screen appears once upon upgrade; if you run the configuration wizard later, this screen won't appear. See Restore AppScan Server settings.



10. In the **Server Keystore** screen, select a server keystore to be used by the Enterprise Console. If you exported a .pfx file, select **Public key cryptography standards #12 (PKCS #12)**. Browse to the location where you saved the .pfx file, import it and enter the password you created when you exported the file. See "Server Keystore" on page 150.

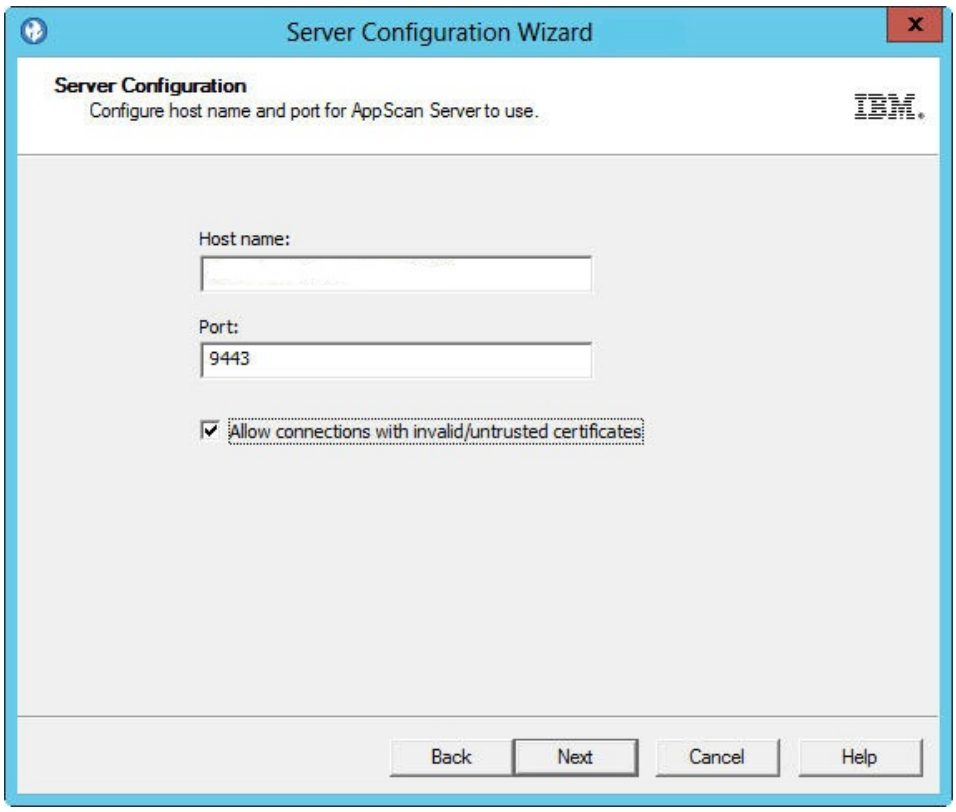


11. In the Authentication Mechanism window, select an **Authentication Mechanism** to use to log in to the Enterprise Console. The default is to authenticate via Windows. To use LDAP, see "Authentication Mechanism" on page 150.



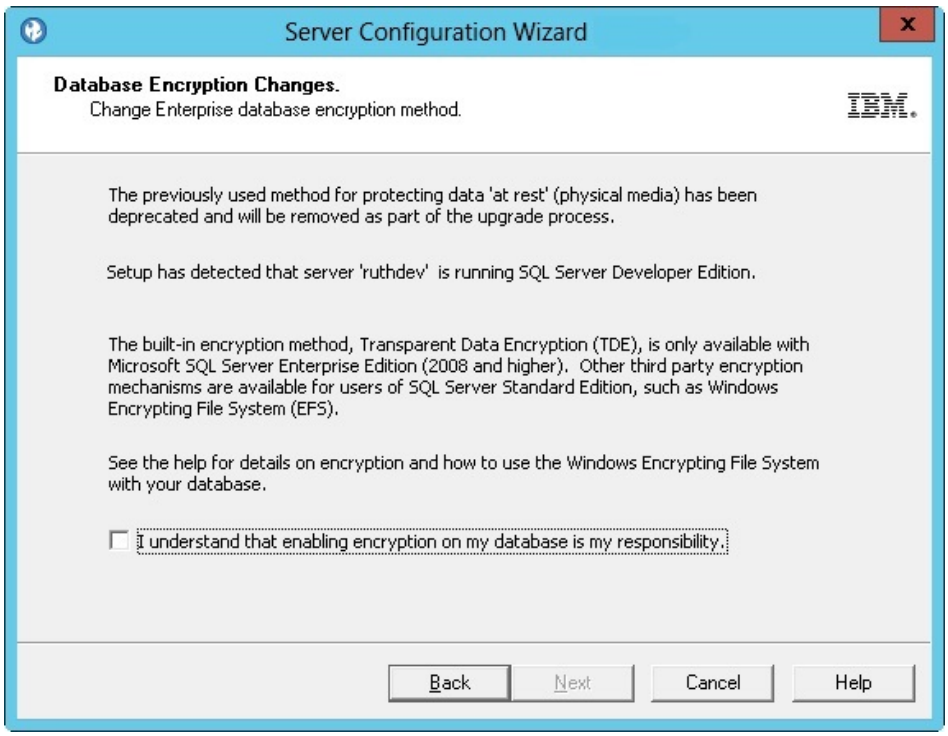
Note: If you need to authenticate with the Common Access Card (CAC), make sure you choose LDAP as your authentication mechanism. Once AppScan Enterprise is configured, follow the instructions in "Authenticating with the Common Access Card (CAC)" on page 95 to authenticate with CAC.

12. In the Server Configuration window, configure the host name and port of the Liberty server for AppScan Server to use. If you are using Windows authentication, prefix the host name with your domain name.



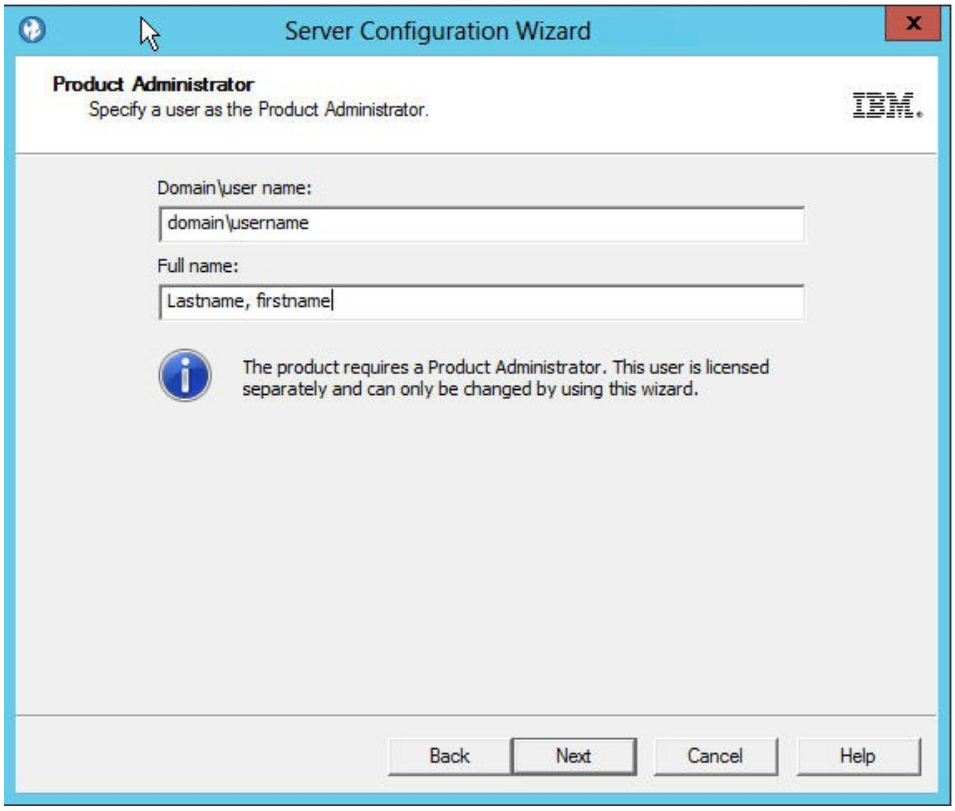
Note: While it is not a recommended practice, you can allow SSL connections with invalid or untrusted certificates during scanning. When the option is disabled, messages will appear in the scan log to indicate that the insecure server could not be reached for scanning. This option also affects the Manual Explore functionality.

13. (upgrade only) In the Database Encryption Changes window, click **Help** to learn how to protect the SQL Server where the database is located. If you decide not to enable TDE, select the check box so you can continue configuration.



Note: AppScan Enterprise uses transparent data encryption (TDE) technology that is available in SQL Server 2008 and later. TDE encrypts the data that is stored in the database or in backups on physical media. If you are using an older version of SQL Server, any data that is contained in that database is at risk of compromise by unauthorized access.

14. In the Product Administrator window, specify a user as Product Administrator. This user is licensed separately; if you want to reassign the Product Administrator license, you must rerun the configuration wizard. See "Product Administrator" on page 151.



15. Ensure that nobody is accessing the database, and click **Finish** in the Specifications Complete window to complete the configuration. This process might take awhile.

    Note:

    a. IIS AppPool settings on Windows 2008 Server R2 are set during configuration:
       - IIS recycling is set at 2:00am
       - Idle timeout is set at 120 minutes

    b. If you see an error message that the proxy server certificate cannot be configured, it might be expired. Contact your Product Administrator to investigate further.

16. Optional: Select the **Start the Services** check box to automatically start the services.

    Note: If you do not choose to automatically start the agent service, the agents do not pick up any jobs that are created by users. You can manually start the service by using the Administrative tools; see "Verifying the agent service and alerting service installation" on page 81.

17. Run the **Default Settings Wizard**. This wizard helps you to install sample data in by providing defaults for a number of configurable options.
18. Click **Exit**.

Running the Default Settings wizard:

This wizard helps you install sample data in by providing defaults for a number of configurable options. You can create users, add security test policies, create scan

templates, add pre-created dashboards, and configure defect tracking integration with Rational Quality Manager or Rational Team Concert.

About this task

Ensure that the **Launch Default Settings Wizard** check box is selected when the Configuration wizard finishes.

Procedure

1. In the Welcome page, choose the instance that you want to update, and click **Next**.
2. In the Initialization Type window, select one of the available initializations, and click **Next**.
3. In the Default Setting window, configure the following options and click **Next**:
   a. **Instance**: Select the instance name for this setup. The Instance that was configured in the Configuration wizard is selected here by default.
   b. **Contact**: The name or a point of contact for the items that are created by the wizard. You can edit these items later if necessary.
   c. **Root folder name**: Enter a name for the default root folder. The default folder acts as the root folder for all other folders you create.
   d. **Application URL**: Enter the URL for the application users to access the application. By default, this URL is the current computer's FQDN (fully qualified domain name). (for example, `http://myserver/mydomain/appscan/`).
4. (Windows authentication only): In the LDAP Settings page, select the **Enable LDAP** check box if you use an LDAP server.
   a. In the **Server Name** field, enter the LDAP group name.
   b. In the **Group Query** field, enter the path of the group query that is used to retrieve user group information. You can use an LDAP server or an Active Directory server.
   c. Optional: If you want to integrate with the LDAP server by using anonymous access, select the **Anonymous access** check box. This option is disabled by default.
   d. Click **Test LDAP** to confirm the configuration works.
5. In the IP Security Permissions page, configure the IP addresses and ranges that are allowed for scanning. Use a dash to define IPv4 ranges (such as 1.2.3.4–); use a prefix to define IPv6 ranges (such as fe80::/10).
6. In the Populate Database with Sample Data page, select the **Populate Sample Data** check box to populate the database with scan templates, pre-created dashboards, server groups, and test policies.
7. Click **Next**. The Default Settings Wizard Progress page opens, displaying the setup's progress.
8. When the wizard is complete, the Default Settings Wizard Complete page opens.
9. Click **Exit** to close the wizard.

Verifying the installation of the Enterprise Console:

After the installation process is complete, you can verify the installation of the Enterprise Console.

Procedure

Go to https://localhost/ase/ and log in.

Installing IBM Security Dynamic Analysis Scanner on Machine C:

Use this procedure to install the agents used for scanning and testing your website applications. You can install the Scanner on multiple machines.

Before you begin

Note:

1. Make sure you read "Required user account information during installation and configuration" on page 22 so that you know which user account to use during installation.
2. Any technologies that you use on your website must also be installed with the Scanner. For example, if you use Flash on any web pages, you must have the correct version of Flash installed.

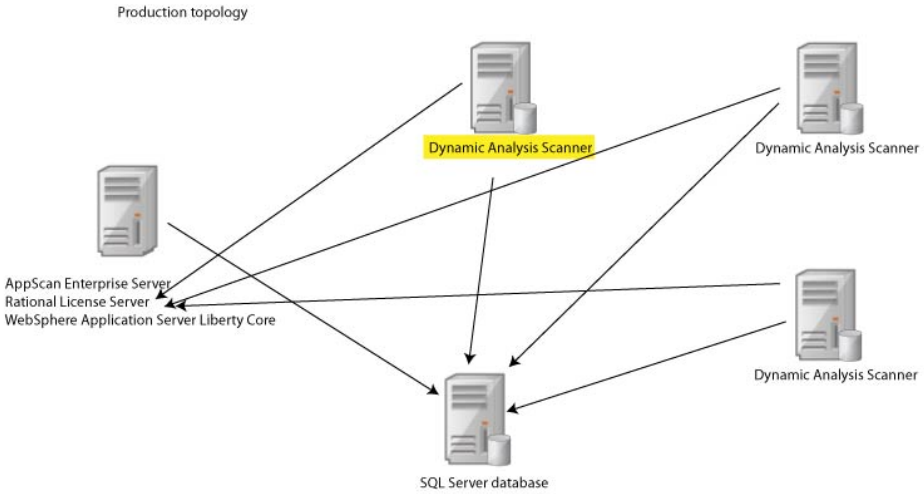
Procedure

1. Go to the directory where you downloaded the executable file (`ASE_DASSetup_<version>.exe`) and double-click the file.

   Note: It might take a while for the next screen to display.
2. In the License Agreement window, select the **I accept the terms in the license agreement** option, and click **Next**.
3. Optional: In the Program Features window, select **Web Services Explorer** to add the ability to test web services for security vulnerabilities, and click **Next**.

   Note: Approximately 330 MB is required for the Web Services Explorer – GSC (Generic Service Client tool) version 8.1 that is used to test Web Services for security vulnerabilities
4. In the Destination Folder window, click **Next**.
5. In the Ready to Install the Program window, click **Install** to proceed with the installation, and then click **Finish**.

Results



Running the Configuration Wizard on the Scanner:

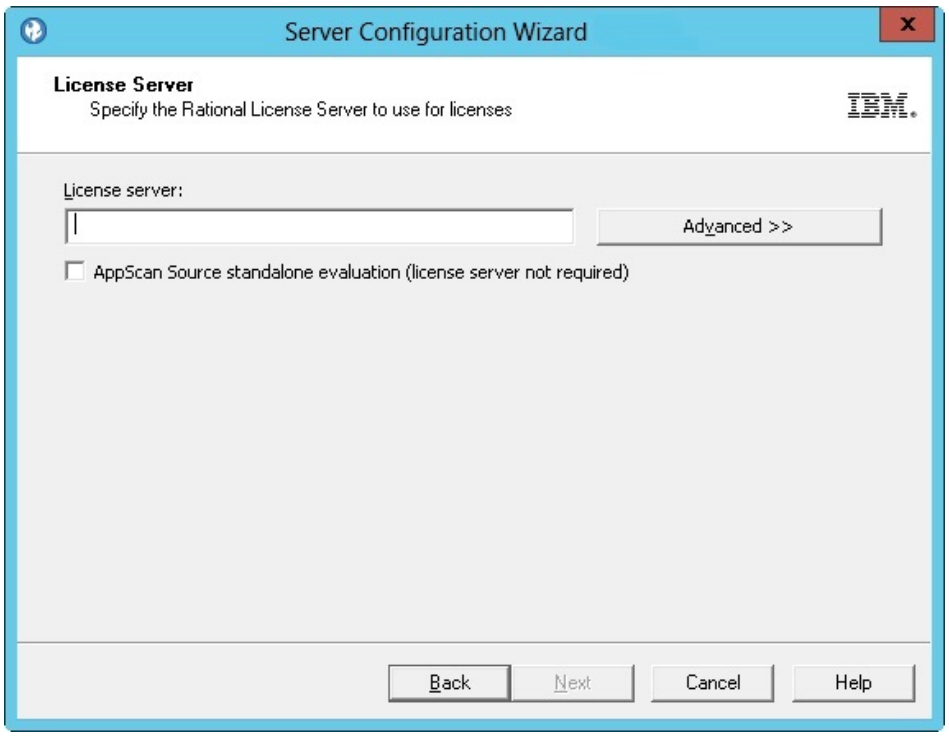
After you install or upgrade the Server or Scanner, you must configure each installed component and run the Configuration wizard on all instances and on all servers.

Before you begin

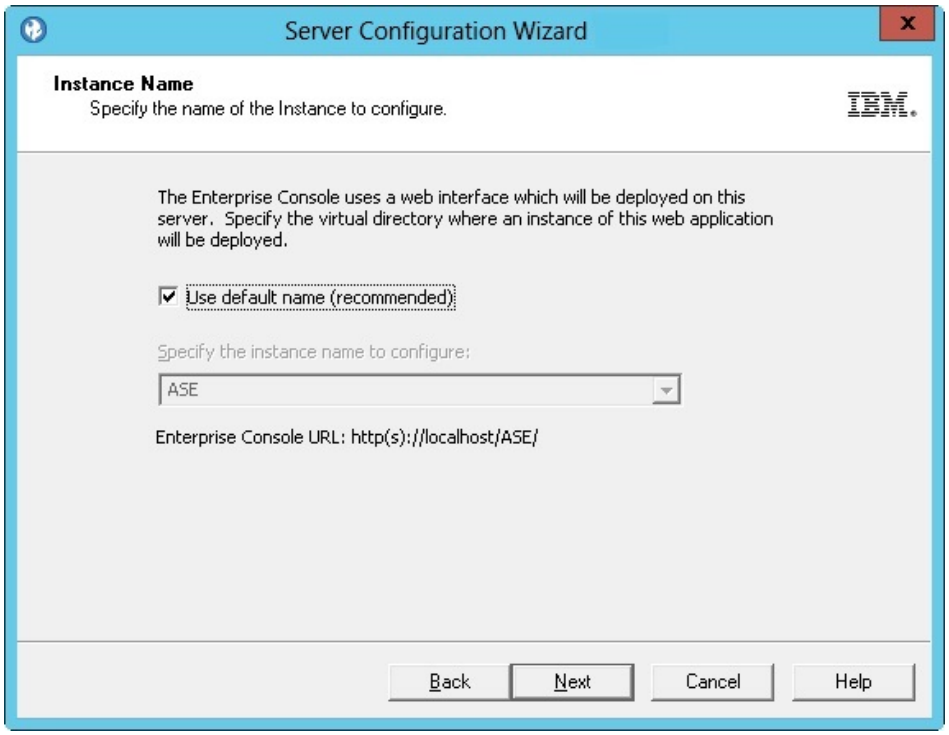
1. During configuration, you define the name and location of the SQL Server database to be used, and the service account name and password. The user who runs the configuration wizard must be able to create a database and grant rights.
2. Running the wizard after you install the AppScan Enterprise Server sets up the database on the SQL Server and does the initial setup of the component.
3. Running the wizard after you install the Dynamic Analysis Scanner registers the Scanner with AppScan Enterprise Server.

Procedure

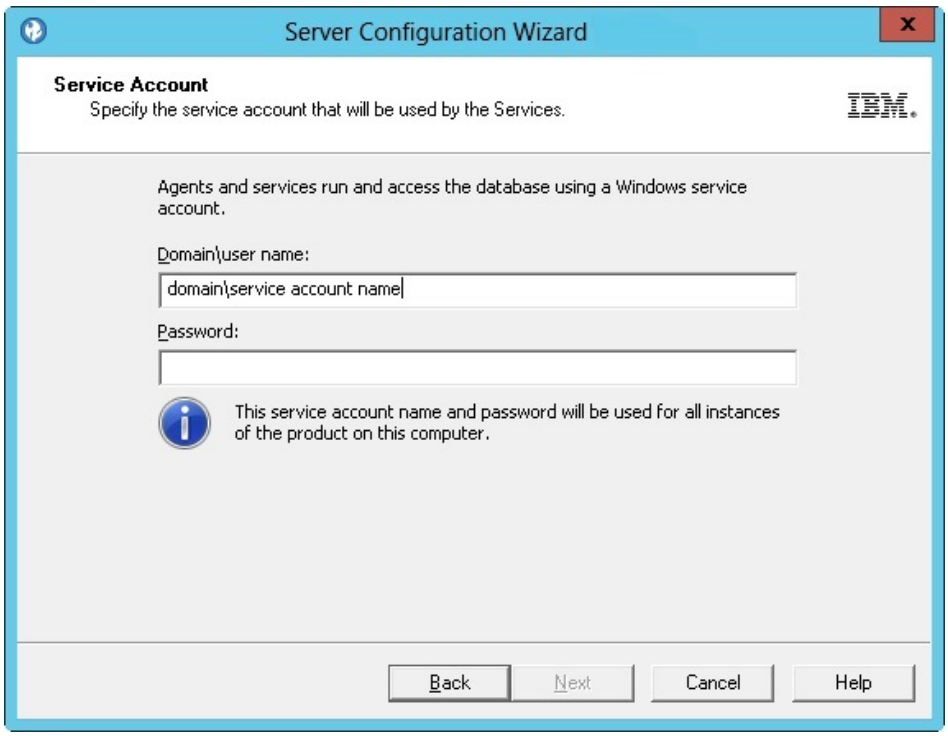
1. Start the Configuration wizard by using one of these methods:
   a. After installation, select the **Launch Configuration Wizard** check box in the Setup Wizard Completed window.
   b. From the Windows **Start** menu, select **Configuration Wizard**.
2. In the Welcome screen, click **Next**.
3. In the License Server window, specify the Rational License Server to use for licenses. See "License Server" on page 147.



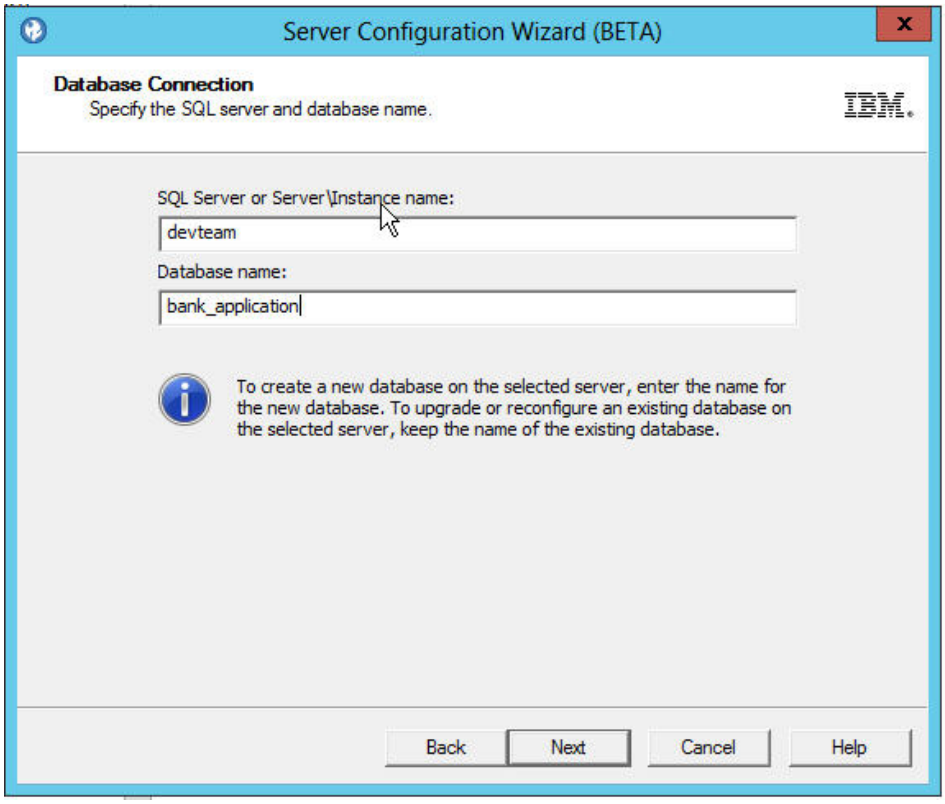
4. In the Instance Name window, specify the name of the instance you want to configure. See "Instance Name" on page 148.



5. In the Service Account window, enter the **Domain/Username Service Account** and password, and click **Next**. See "Service Account" on page 149.



6. In the Database Connection window, enter the SQL Server name, port number, and the name of the database you are connecting to. You can click **Test Connection** to make sure you can connect to the SQL Server. The configuration wizard does not proceed until the connection is successful. When AppScan Enterprise Server creates the database in SQL Server, it automatically configures the collation for it.

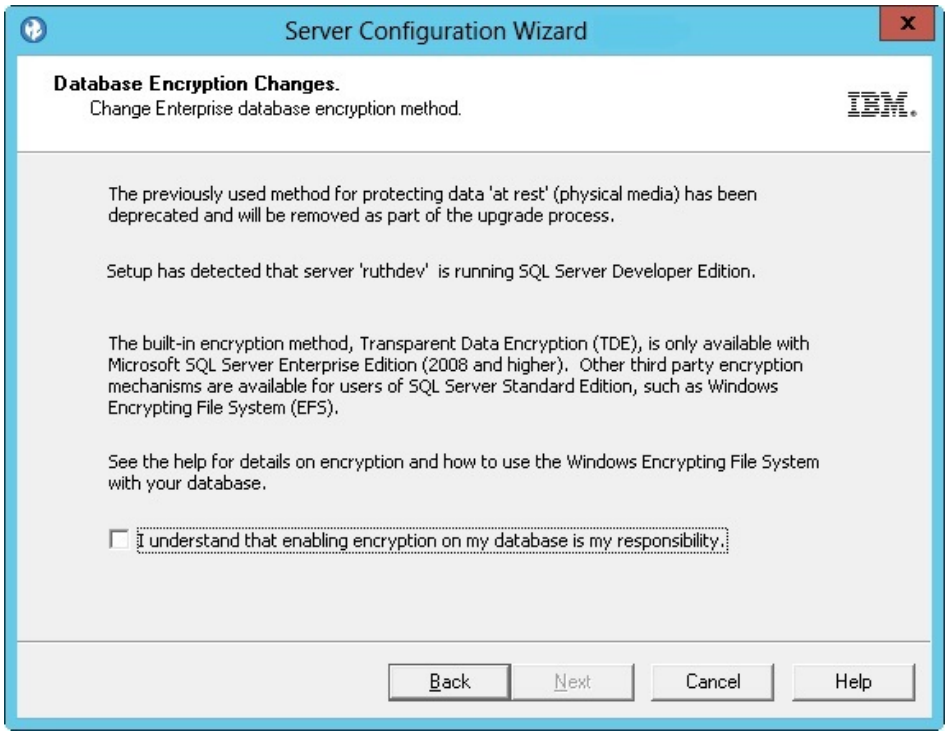


Note:

a. If you are upgrading an existing database from v8.6 or earlier, enter the **Database Master Key Password** on the next screen to access it. Keep this password in a secure location.

b. If your environment uses a named SQL Server instance for the AppScan Enterprise database or SQL Server Express, make sure that TCP/IP is enabled in the SQL Server configuration manager, and restart the SQL services for SQL Server. Use the port number of the named SQL Server instance instead of the default port number (1443).

7. (upgrade only) In the Database Encryption Changes window, click **Help** to learn how to protect the SQL Server where the database is located. If you decide not to enable TDE, select the check box so you can continue configuration.



Note: AppScan Enterprise uses transparent data encryption (TDE) technology that is available in SQL Server 2008 and later. TDE encrypts the data that is stored in the database or in backups on physical media. If you are using an older version of SQL Server, any data that is contained in that database is at risk of compromise by unauthorized access.

8. Ensure that nobody is accessing the database, and click **Finish** in the Specifications Complete window to complete the configuration. This process might take awhile.

Note:

a. IIS AppPool settings on Windows 2008 Server R2 are set during configuration:
   - IIS recycling is set at 2:00am
   - Idle timeout is set at 120 minutes

b. If you see an error message that the proxy server certificate cannot be configured, it might be expired. Contact your Product Administrator to investigate further.

9. Optional: Select the **Start the Services** check box to automatically start the services.

   Note: If you do not choose to automatically start the agent service, the agents do not pick up any jobs that are created by users. You can manually start the service by using the Administrative tools; see "Verifying the agent service and alerting service installation" on page 81.

10. Click **Exit**.

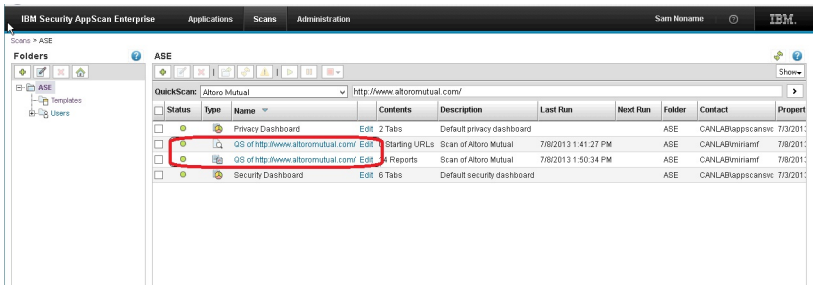
Verifying the scanner installation:

Run a QuickScan to verify that the agents installed properly. It is a simple way to make sure that everything is working before you start configuring more complex web application scans.

Procedure

1. In the Scans view, select *AltoroMutual* from the list QuickScan template list, and click the **Create QuickScan** icon. This scans the Altoro Mutual website, which is published by IBM Corporation for the sole purpose of demonstrating the effectiveness of AppScan in detecting web application vulnerabilities and website defects.
2. Install the Manual Explore plug-in from the pop-up window. Close the window and click **Run** to start the scan.
3. When the scan is completed, click **Close** to return to the folder explorer view. Two items that are called *QS of http://www.altoromutual.com/* are added to the view: a scan job and a report pack. Look at the Status column. When both items are in a **Ready** state, you can click the report pack link and see the scan results.

Results



Related concepts:

"Installing multiple instances of the Enterprise Console on a single server" on page 98
You have the option of installing a default instance, or multiple instances on a single computer. Each instance is an independent set of configuration information with its own database.

Installing the User Component on Linux for AppScan Source

Use these instructions to install the User Administration component to configure AppScan Source users.

Procedure

1. On the Linux computer, log in with root access privileges.
2. Type `ls -l AppScanServerSetup_9.0.2.bin`. Make sure that you see **-rwxrwxr-x** in the result listing.
3. Run the .bin file. Type `./AppScanServerSetup_9.0.2.bin`, and click **Enter** to start the installer.
4. Pick a language for installation and click **OK** > **Next**.
5. Accept the terms of the license agreement.
6. Choose an installation folder (the default location is `/opt/IBM/AppScan_Server`).
7. Review the installation summary and click **Install**. The files are copied onto the Linux computer.
8. Configure the **Liberty Server name**, **port number** (the default is 9443), and the **Rational License Server name**. Click **Next**.
9. Configure the LDAP settings. Select an **LDAP server type**. Some of the LDAP configuration fields are pre-populated for you. Check that they are correct for your environment.
   a. If your LDAP server supports SSL, select the **Connect to LDAP server using SSL** check box.
   b. Enter the **LDAP server host name** and **port** (389 is default), and the **Base DN**.
   c. If you need to be authenticated on the LDAP server, enter the **Bind DN** and the **Bind password**. Click **Next**.
10. Configure the product administrator's user name, and click **Next**. After the Liberty service is configured, the installation is complete.

Results

Now an AppScan Source administrator can connect to the AppScan Server on Linux to validate and administer their users.

Post installation tasks

After you install AppScan Enterprise, complete these postinstallation tasks.

Postinstallation checklist

After you install AppScan Enterprise, review and complete all of the necessary tasks on the postinstallation checklist.

Table 13. Postinstallation checklist

Task	Check when complete
Verify the agent service and alerting service installation	☐
Secure the deployment.	☐
Enable FIPS or enable NIST. (Federal government agencies)	☐

Verifying the agent service and alerting service installation

During installation, two services were installed: the Agent Service and the Alert Service. You need to ensure that these services have been installed and are started. If the agent service is not started, any jobs that users create will not be picked up

and run by the Server. If the alerting service is not started, any alerts that have been configured for users will not be issued. Make sure that only one instance of the alerting service is installed; otherwise, duplicate notifications might be sent out.

About this task

If you installed Server components on different machines, you must verify that the services are started on each one.

Procedure

1. Using the Control Panel or the Start Menu, select **Administrative Tools** > **Services**.
2. In the list of services, select **`Agent Service`**. If the service was properly installed and started, a *Started* status will be displayed in the Status column. If this is not the case, you can start the service by right-clicking the service name and selecting **Start**.
3. Repeat Step 2 for the Alert Service.

Securing the deployment

Follow these steps during installation and configuration to ensure your AppScan Enterprise instance is secure.

Procedure

1. During configuration, choose a certificate specific to your organization in the Server Certificate dialog.
2. To secure IIS on the Enterprise Console Server:
   a. Disable **WebDAV**.
   b. Disable the **EnableTraceMethod**. This method determines whether IIS recognizes the HTTP TRACE method. The TRACE method is used to invoke a remote, application-layer loop-back of a request message. TRACE allows a client to see what is being received at the other end of the request chain and use that data for testing and debugging information.

      Note: Do not leave EnableTraceMethod enabled on a production system, because it can reveal backend server address information to a malicious user.

Trusting the certificate authority

If your certificate is not from a trusted authority, you will need to trust it on your client machine.

Procedure

1. In Internet Explorer, navigate to AppScan Enterprise and choose to proceed when you get the certificate warning.
2. Right-click on the page, choose properties, click **Certificates**.
3. Select `Install Certificate` and click **Next**.
4. Select `Place all certificates in the following store`, and click **Browse**.
5. Select `Show physical stores`.
6. Select **Trusted Root Certification Authorities** > **Local Computer**.
7. Click **Next** > **Finish**.

Disabling weak cipher suites in IIS

By default, IIS is installed with 2 weak SSL 2.0 cipher suites that are enabled: *SSL2_RC4_128_WITH_MD5* and *SSL2_DES_192_EDE3_CBC_WITH_MD5*. This can impact the security of AppScan Enterprise, and the cipher suites should be disabled.

Before you begin

Incorrectly editing the registry may severely damage your system. Before making changes to the registry, you should back up any valued data on your computer.

Procedure

1. Open the Registry Editor (**Start** > **Run** > **regedit**).
2. In the `HKEY_LOCAL_MAC HINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers` directory:
   a. Create a new key called `RC4 128/128` (**Ciphers** > **New** > **KeyRC4 128/128**).
   b. Right-click the key's name and create a new DWORD (32-bit) Value called 'Enabled'. (**New** > **DWORD (32-bit) Value** > **Enabled**).
   c. Leave the default value as '0'.
3. In the `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Hashes` directory:
   a. Create a key called `MD5` (**Hashes** > **New** > **Key** > **MD5**).
   b. Right-click the key's name and create a new DWORD (32-bit) Value called 'Enabled'. (**New** > **DWORD (32-bit) Value** > **Enabled**).
   c. Leave the default value as '0'.
4. Close the Registry Editor.

Updating the Java SDK policy files

AppScan Enterprise provides Java SDK 7.0 that contains strong but limited jurisdiction policy files. Some key formats (such as PKCS #12) that are provided by a Certificate Authority (CA) might be protected with algorithms that are not provided with the limited policy files in Java SDK 7.0. Before you replace self-signed certificates with CA-issued certificates, update your Java SDK policy files.

About this task

The unrestricted JCE policy files that are provided in the policy file update can ensure that you have the correct algorithms for CA-issued certificates.

Procedure

1. Use a browser to go to http://www.ibm.com/developerworks/java/jdk/security/index.html.
2. Click `Java SE 7`.
3. On the website that launches, click **IBM SDK Policy files** in the table of contents and then **ibm.com**® on the page that opens in the content pane.
4. On the website, enter your IBM®.com ID and password.
5. Select `Files for Java 5.0 SR16, Java 6 SR13, Java 6 SR5 (J9 VM2.6), Java 7 SR4, and all later releases` and click **Continue**.
6. View the license, check `I agree`, and click `I confirm`.
7. Click **Download now**.

8. Extract the unlimited jurisdiction policy files that are packaged in a compressed file. The compressed file contains a `US_export_policy.jar` file and a `local_policy.jar` file.
9. On the server where AppScan Enterprise is installed, back up the following files:
   - US_export_policy.jar
   - local_policy.jar

   Note: These files are installed in the following directory by default: `<installdir>/AppScan Enterprise/Liberty/jre/lib/security/`.
10. Replace the `US_export_policy.jar` and `local_policy.jar` files with the updated files from the compressed file that you downloaded.

Securing the SQL Server database

Depending on whether you have the Enterprise or Standard version of SQL Server, securing your data is a critical database maintenance practice.

Securing the connection from AppScan Enterprise to SQL Server:

This procedure describes how to install a certificate on a computer that is running Microsoft SQL Server by using Microsoft Management Console (MMC) and describes how to enable SSL Encryption at the server.

Procedure

1. Create an SSL certificate:
   a. Go to **Control Panel** > **Administrative Tools** > **IIS Manager** > **Server Certificates** > **Create Self-Signed Certificate**.
   b. Give the certificate a name, click **OK** and **Export** the certificate.
   c. Close IIS Manager.
2. Start MMC console (**Start** > **Run** > **mmc**).
   a. Go to **File** > **Add/Remove Snap-in** > **Certificates** > **Add** > **Computer account**.
   b. Select the computer that you want the snap-in to manage and click **Finish** > **OK**.
   c. Expand **Certificates** and right-click the **Personal** folder and go to **All Tasks** > **Import**.
   d. Follow the wizard instructions and import the certificate.
   e. Close the MMC Console and restart the SQL service.

      Important: Make sure that the service account has access to certificates. It might need to run as a local account.
3. Open SQLServer Configuration Manager:
   a. Expand **SQL Server Network Configuration** right-click **Protocols for <sql server name>** and then select **Properties**.
   b. On the Flags tab, select **Yes** in the **Force encryption** box, and then click **OK**.
   c. Select the certificate from the Certificate tab and click **OK** to close the dialog.
   d. Restart the SQL Server service.

4. If you are running SQL Server with a non-privileged service account, you must enable the private key to be readable by the SQL Server service account. Follow the steps in this article: **Permissions required for SQL Server Service account to use SSL certificate**.

   Note: Read these sections: "Few more tips while enabling the encrypted connection" and "Permissions to the Private Key portion of the Imported Certificate - FIX" in this article: Enable Encrypted Connections to the Database Engine (SQL Server Configuration Manager).

Data protection through encryption:

Data that is stored on a physical media can be a target of unauthorized access attack. The physical media might be stolen, or the data might be accessed remotely. While you can use physical and computer security methods to protect your data from these types of attacks, encrypting the data offers more protection by preventing an attacker from reading the stolen files.

Encrypting the data is only effective if the attacker is not able to hijack computer accounts or passwords that were used to protect the data in the first place. Data that is stored in Microsoft SQL Server database files can be protected by using various encryption methods, such as:

- Hard disk drive encryption
- Encrypted file system
- Transparent data encryption (TDE) - which is a feature of MS SQL Server 2008 Enterprise Edition
- Cell encryption, which is done by encrypting individual columns in the tables of the database

Cell encryption is the method that is least dependent on the computer that hosts the database server, and can be used by any application that has access to the database because the data that is being written is encrypted by the application. However, this method has a significant impact on the application performance, and Microsoft cautions against using this method and suggests Transparent Data Encryption (TDE) as the alternative.

To improve product performance, AppScan Enterprise no longer uses cell encryption. For some organizations, the cell encryption that was provided by AppScan Enterprise was an added layer of protection in addition to existing data encryption measures required by their organizational standards, and so the data would remain protected in these situations.

For organizations that have not used any additional data encryption methods other than what was provided through cell encryption by AppScan Enterprise, read the information in the Related Links section about how to enable data encryption and protect your data:

Related tasks:

“Enabling Transparent Data Encryption on SQL Server databases” on page 86
SQL Server has a built-in encryption TDE mechanism (Transparent Data Encryption) encrypts the data residing in the database or in backups on physical media.

"Encrypting, backing up, and restoring a SQL Server database with EFS" on page 89
The Encrypting File System (EFS) is a feature of Microsoft Windows that lets you store information on your hard disk in an encrypted format. EFS enables transparent encryption and decryption of files by using advanced, standard cryptographic algorithms. Use this method to encrypt the database file if you have SQL Server Standard Edition 2008, 2008 SP3, 2008 R2 SP2, 2012, and 2014.

Enabling TDE on SQL Server Enterprise Edition:

Enabling Transparent Data Encryption on SQL Server databases:

SQL Server has a built-in encryption TDE mechanism (Transparent Data Encryption) encrypts the data residing in the database or in backups on physical media.

Before you begin

TDE is only available on the Enterprise edition of Microsoft SQL Server 2008 and higher. For the Standard edition option, read "Encrypting, backing up, and restoring a SQL Server database with EFS" on page 89.

About this task

To enable TDE on SQL Server, you must have the normal permissions associated with creating a database master key and certificates in the master database. You must also have CONTROL permissions on the user database.

Enabling encryption is a common task for database administrators; for convenience, we have provided a SQL script to use which is suitable for a typical SQL Server configuration: EnableTDE.zip. (If file doesn't download, right-click the link and save the file to your hard drive.)

Note: For upgrade users:

1. To improve database upgrade performance, enable TDE after the database upgrade has completed.
2. While you can perform these steps at any time, the database will not be encrypted until you have completed the steps. Enabling TDE before the upgrade process will protect your database throughout the upgrade and afterwards.

Procedure

1. Open the SQL Management Studio of your installation of SQL Server 2008, 2008R2, 2012, or 2014.
2. Connect to the database you want to encrypt. This will help ensure the database has been created and is available.
3. Go to the location where you downloaded the *EnableTDE.zip* file. Extract the file and open the script. (**File** > **Open** > **File**). You will notice several commands that will be executed on the server.
4. Before you execute the script, you must set three fields for your environment. In the comments section of the script, they are all marked with 'ACTION REQUIRED' :
   a. DECLARE **@MKPassword**: The Master Key Password used to create the master key in the [master] database.

b. DECLARE **@DatabaseName** : The name of the database you want to enable encryption on.
c. (Optional) DECLARE **@BackupPassword**: The Certificate Backup Password. This password is used to secure the certificate backup and is required to restore the certificate on another machine.

5. After the fields have been updated, launch the script (Query >Execute). "How the script enables TDE on SQL Server."
6. After the script has completed, the result will be displayed in the 'Messages' window of SQL Management Studio.

   Note: You can also verify through SQL Management Studio. Right-click on "Database Name->Tasks->Manage Database Encryption". You will see that the check box for 'Set Database Encryption On' is selected.

Results

Important: Once completed, be sure to write down the passwords used in this script, and make a copy of the certificate backup. The certificate backup consists of two files, AppScanEntCert.bak and AppScanEntCert.pvk. They will be stored with the database .mdf file, by default in the folder:

- **(SQL 2014)** C:\Program Files\Microsoft SQL Server\MSSQL12.MSSQLSERVER\MSSQL\DATA
- **(SQL 2012)** C:\Program Files\Microsoft SQL Server\MSSQL11.MSSQLSERVER\MSSQL\DATA
- **(SQL 2008)** C:\Program Files\Microsoft SQL Server\MSSQL10.MSSQLSERVER\MSSQL\DATA
- **(SQL 2008 R2)** C:\Program Files\Microsoft SQL Server\MSSQL10_50.MSSQLSERVER\MSSQL\DATA

Related tasks:

"Moving a TDE-protected database to another SQL Server" on page 88
Follow these steps when you need to restore or move a TDE-protected database to another server.

Related information:

Transparent Data Encryption (TDE)

How the script enables TDE on SQL Server:

The script is a convenient way to perform end-to-end steps required to configure TDE on a user database.

1. Create the master key, if required.

   TDE requires that a master key be created in the [master] database. Each database server can only have one master key that is shared amongst all user databases. **The password must be provided in the script in this step.** If the master key does not already exist, it will be created with the provided password.
2. Open the master key.

   The master key must be open to perform the subsequent steps. This step ensures the master key is open before continuing. In cases where a master key is already present on the database server this step verifies that the password entered matches the password used to initially create the master key.
3. Create the 'AppScan' certificate.

A certificate is created to be used by all AppScan Enterprise databases on this database server. The name of the certificate is 'APPSCAN_ENT_CERT'.

Once the certificate is created, it is immediately backed up. This step generates two files: AppScanEntCert.bak and AppScanEntCert.pvk. The file are stored with the database .mdf file in the relevant location:

- **(SQL 2014)** C:\Program Files\Microsoft SQL Server\MSSQL12.MSSQLSERVER\MSSQL\DATA
- **(SQL 2012)** C:\Program Files\Microsoft SQL Server\MSSQL11.MSSQLSERVER\MSSQL\DATA
- **(SQL 2008)** C:\Program Files\Microsoft SQL Server\MSSQL10.MSSQLSERVER\MSSQL\DATA
- **(SQL 2008 R2)** C:\Program Files\Microsoft SQL Server\MSSQL10_50.MSSQLSERVER\MSSQL\DATA

4. Associate the AppScan certificate with the AppScan Enterprise database.

   This step creates an encryption key on the database based on the certificate created in Step 3.
5. Enable encryption.

   This step enables encryption on the AppScan Enterprise database.
6. Test and display results

   A message is printed to the 'Messages' view in SQL Management Studio indicating if the previous steps were successful, and displays the percentage of TDE completion.

Tasks related to Transparent Data Encryption on SQL Server:

The articles listed below provide further details that should be part of your SQL Server database maintenance plan.

Related information:

Understanding Transparent Data Encryption (TDE)

Move a TDE Protected Database to Another SQL Server

SQL Server Certificates and Asymmetric Keys

SQL Server and Database Encryption Keys (Database Engine)

Moving a TDE-protected database to another SQL Server:

Follow these steps when you need to restore or move a TDE-protected database to another server.

Before you begin

Download this compressed file to the SQL Server machine: RestoreDBCertificate.zip. (If file doesn't download, right-click the link and save the file to your hard drive.)

Procedure

1. Copy the two certificate files (AppScanEntCert.bak and AppScanEntCert.pvk) that you created in the "Enabling Transparent Data Encryption on SQL Server databases" on page 86 task to a location on your machine (for example, `C:\Certificate\`).
2. Open the SQL Management Studio of your SQL Server 2008 or 2012 installation.

3. Go to the location where you downloaded the RestoreTDECertificate.zip file. Unzip the file and open the script. (**File** > **Open** > **File**). You will notice several commands that will be executed on the server.
4. Before you execute the script, you must set three fields for your environment (they are all marked with 'ACTION REQUIRED' in the comments section of the script):
   - **DECLARE @MKPassword**: The Master Key Password used to create the master key in the [master] database where you enabled TDE
   - **DECLARE @BackupPassword**: The password that was used to back up the certificate if it is different from @MKPassword
   - **DECLARE @Path**: The path of the location that you copied the two files AppScanEntCert.bak and AppScanEntCert.pvk
5. After the fields have been updated, click **Query** > **Execute** to launch the script.

Results

After the script has completed, the result will be displayed in the 'Messages' window of SQL Management Studio. If you see the message: "The certificate is restored successfully, you can restore the database.", you should be able to restore the database on this SQL Server.

Using Encrypting File System on SQL Server Standard Edition:

Encrypting, backing up, and restoring a SQL Server database with EFS:

The Encrypting File System (EFS) is a feature of Microsoft Windows that lets you store information on your hard disk in an encrypted format. EFS enables transparent encryption and decryption of files by using advanced, standard cryptographic algorithms. Use this method to encrypt the database file if you have SQL Server Standard Edition 2008, 2008 SP3, 2008 R2 SP2, 2012, and 2014.

Before you begin

This task assumes that you have:

1. Chosen a service account for SQL server service that
   - remains available for the lifetime of the encrypted database and its backup.
   - can be used to transfer the database or its backup across the network, if needed.

   Note:
   - The service account can be the same or different than the one you use for AppScan Enterprise.
   - Use one service account to log in to the SQL Server service and to encrypt any of the databases that are hosted through that service.
   - The SQL Server service account will be referred to as 'the service account' in these instructions.
2. Located the filepath of the database, if different than the default locations listed here. You will need this information for step 3. You can find the default location by opening Microsoft SQL Server Management Studio. Right-click the SQL Server that hosts the database. Click **Properties** > **Database settings** > **Database default locations**.

About this task

This procedure must be completed before you run the configuration wizard; otherwise, you won't be able to access the database. See "Configuring the SQL Server database for AppScan Enterprise" on page 32.

Procedure

1. Go to **Start** > **Administrative Tools** > **Services** and stop the SQL Server service that hosts the AppScan Enterprise database you are going to encrypt. The default service is *SQL Server (MSSQLSERVER)*.
2. Right-click the name of the service to open the properties dialog. On the **Log on** tab, select **This account**, enter the credentials of the service account, and then click **OK**.
3. In Windows Explorer, right-click the folder where the database resides, and go to **Properties** > **Security** to give the service account *Read and execute* and *read* access to both the `<databasename.mdf>` file and the parent folder.

   Note: The credentials of the user that is logged in will be used to encrypt the database. If you are not logged in as the service account, do that now.
4. Right-click the folder that contains the <databasename.mdf> file and go to **Properties** > **General** > **Advanced Attributes**. Select the **Encrypt contents to secure data** check box and click **OK**.

   Note:

   If the folder is not encrypted yet, select **Apply changes to this folder, subfolders and files** when prompted. If you select this option after you run the Server Configuration Wizard, then the database is not encrypted. If this process is applied to the database and the corresponding log file after the Server configuration wizard is run, then the database might get into a "Recovery Pending" state. Then, the encrypted database is not accessible in SQL Server Management tools and AppScan Enterprise.
5. In the Services window, start the SQL Server that hosts the AppScan Enterprise database.

Results

The DATA folder `C:\Program Files\Microsoft SQL Server\MSSQL12.MSSQLSERVER\MSSQL\DATA` (if defaults were used during Microsoft SQL Server 2014 Standard installation) will appear in green in Windows Explorer after it gets encrypted. Any databases that are added after this procedure are encrypted, including the AppScan Enterprise database created by the Server Configuration Wizard.

Note: Only the user who encrypted the file can decrypt it. You can determine who encrypted specific files in the Details section on the **Properties** > **Advanced Attributes** window. The backup of the encrypted database will NOT be encrypted automatically. Follow the steps in **Backing up and restoring an EFS-encrypted database**.

Backing up and restoring an EFS-encrypted database:

You can move an encrypted backup database file to a network-shared location hosted on the same Windows version to preserve the file encryption. You can restore the database from any location where the encrypted database file is stored. When restoring into a SQL Server, that Server's service should be running with the

service account credentials of the user who encrypted the database. However, a restored database file is NOT encrypted, so you must encrypt it using the steps in the above task.

Procedure

1. In Windows Explorer, expand the folder where the database backup resides, and give the service account *Read and execute* and *read* access to the <databasename.bak> file.

   Note: The credentials of the user that is logged in will be used to encrypt the database. If you are not logged in as the service account, do that now.
2. Right-click the <databasename.bak> file and go to **Properties** > **General** > **Advanced** > **Encrypt contents to secure data**, and click **OK**.

Detaching, encrypting, and attaching a database encrypted with EFS:

There might be times when you do not want to stop the SQL Server service during database encryption; for example, when there are several databases running on that service and you do not want them to be unavailable. You can detach, encrypt, and attach the database instead.

Before you begin

'The service account' must be used to log in to the SQL Server service and to encrypt any other databases on the same SQL Server.

Procedure

1. Go to **Start** > **Administrative Tools** > **Services** and stop the SQL Server service that hosts the AppScan Enterprise database you are going to encrypt. The default service is *SQL Server (MSSQLSERVER)*.
2. Right-click the name of the service to open the properties dialog. On the **Log on** tab, select **This account**, enter the credentials of the service account, and then click **OK**.
3. In the Services window, start the SQL Server that hosts the AppScan Enterprise database.
4. In Windows Explorer, right-click the <databasename.mdf> file and go to **Properties** > **General** > **Advanced** > **Encrypt contents to secure data**, and click **OK**.
5. Open Microsoft SQL Server Management Studio and connect to the SQL Server that serves that database.
6. Under the 'Databases' tree, right-click the database you want to encrypt and click **Tasks** > **Detach**.
7. In the Detach Database window, if there are open connections, select the **Drop Connections** check box and click **OK**.
8. In Windows Explorer, right-click the <databasename.mdf> file and go to **Properties** > **General** > **Advanced** > **Encrypt contents to secure data**, and click **OK**.
9. Repeat Steps 3 and 4 for the <databasename.ldf> file.
10. In Microsoft SQL Server Management Studio, right-click the **Databases** tree, and choose **Attach**.
11. In the Attach Databases window, click **Add** and navigate to the encrypted <databasename.mdf> file. Select it and click **OK** > **OK**
12. Repeat Step 11 for the <databasename.ldf> file.

Support for FIPS 140-2 and NIST SP800-131a security standards

The National Institute of Standards and Technology (NIST) is the US federal technology agency that works with industry to develop and apply technology, measurements, and standards. AppScan Enterprise Server can be configured to work with various security standards to meet security requirements required by the US government.

Overview

Government agencies and financial institutions use these standards to ensure that their products conform to specified security requirements. Recently, new security standards have become available. The National Institute of Standards and Technology (NIST) developed a new standard, Special Publications 800-131a (or SP 800-131a), to replace the current FIPS standards (FIPS 140-2). NIST SP800-131a replaces FIPS 140-2. SP800-131a strengthens the algorithms and increases the key lengths to increase security, and provides both transition mode and strict mode.

FIPS 140-2

One of the standards published by NIST is the Federal Information Processing Standard Security Requirements for Cryptographic Modules, referred to as FIPS 140-2. FIPS 140-2 provides a standard that can be required by US federal agencies who specify that cryptographic-based security systems are to be used to provide protection for sensitive or valuable data. Many US federal agencies can be configured to use this level, but might be required to move up to the newer SP800-131a standard. See The National Institute of Standards and Technology for more information about the 140-2 standard. AppScan Enterprise is compliant with FIPS 140-2.

NIST SP800-131a

SP800-131a is a requirement originated by the National Institute of Standards and Technology (NIST) which requires longer key lengths and stronger cryptography. The specification also provides a transition configuration to enable US federal agencies to move to a strict enforcement of SP800-131a. The transition configuration also enables US federal agencies to run with a mixture of settings from both FIPS140-2 and SP800-131a. SP800-131a can be run in two modes: transition and strict. AppScan Enterprise is compliant with NIST transition mode.

Enabling FIPS 140-2/NIST 800-131a compliance in the Enterprise Console

When FIPS 140-2 compliance is enabled in the Enterprise Console, some functionality that is not FIPS 140-2 compliant will not work as expected or will be disabled, including the Manual Explore plugin. By default, the Enterprise Console is compliant with the NIST 800-131a transition mode. When you run AppScan Server Configuration Wizard, it will detect whether or not your environment is in NIST strict mode and will respect those settings.

About this task

User role: Product Administrator

Procedure

1. In the Enterprise Console, go to the General Settings page of the Administration view, and click **Edit** in the Enterprise Console Settings section.
2. By default, the check box in the *Enable enhanced security* section is cleared. Select the option if your organization must be compliant with FIPS 140-2 or NIST SP 800-131a. When the option is selected, use the Manual Explorer tool to manually explore your application for additional URLs. See Manually exploring your site to add more URLs to the scan to learn how to download and use the tool.

   Note: Upon upgrade from version 8.7, the check box keeps the value it had before upgrade. If you were FIPS compliant, then this checkbox remains selected; otherwise, it remains cleared.
3. Click **Done**.

Enabling FIPS 140-2 compliance on your operating system

After you upgrade AppScan Enterprise Server and the Dynamic Analysis Scanner, enable FIPS compliance on your operating system.

Procedure

- On Windows:
  1. Go to **Start** > **Control Panel** > **Administative tools** > **Local Security Policy**.
  2. Go to **Security Settings** > **Local Policies** > **Security Options** > **System Cryptography** and enable the `Use FIPS compliant algorithms for encryption, hashing, and signing` security setting.
- On Linux:
  1. Follow the steps in https://access.redhat.com/knowledge/docs/en-US/Red_Hat_Enterprise_Linux/6/html/Security_Guide/sect-Security_Guide-Federal_Standards_And_Regulations-Federal_Information_Processing_Standard.html.

Enabling FIPS 140-2 or NIST SP800-131a on WebSphere Liberty Profile

Use one of these procedures to enable FIPS 140-2 or NIST SP800-131a on WebSphere Liberty Profile.

Before you begin

Run the configuration wizard and start the services before you start this task.

Procedure

1. To enable FIPS 140-2:
   a. Locate the installation directory of Liberty at `<install-dir>\AppScan Enterprise\Liberty\usr\servers\ase`.
   b. Add the *-Dcom.ibm.jsse2.usefipsprovider=true* property to the `jvm.options` file to enable the JSSE2 provider to run in FIPS 140-2 mode.
   c. Go to `<install-dir>\AppScan Enterprise\Liberty\jre\lib\security` directory.
   d. In a text editor, edit the *java.security* master security properties file to register additional cryptographic package providers.
   e. Update these two lines:

```
#ssl.SocketFactory.provider=
#ssl.ServerSocketFactory.provider=
```

to

```
ssl.SocketFactory.provider=com.ibm.jsse2.SSLSocketFactoryImpl
ssl.ServerSocketFactory.provider=com.ibm.jsse2.SSLServerSocketFactoryImpl
```

f. Locate the list of cryptographic providers that are located after the line # *List of providers and their preference orders* and replace it with the following list:

```
security.provider.1=com.ibm.crypto.fips.provider.IBMJCEFIPS
security.provider.2=com.ibm.jsse2.IBMJSSEProvider2
security.provider.3=com.ibm.crypto.provider.IBMJCE
security.provider.4=com.ibm.security.jgss.IBMJGSSProvider
security.provider.5=com.ibm.security.cert.IBMCertPath
security.provider.6=com.ibm.security.sasl.IBMSASL
security.provider.7=com.ibm.xml.crypto.IBMXMLCryptoProvider
security.provider.8=com.ibm.xml.enc.IBMXMLEncProvider
security.provider.9=org.apache.harmony.security.provider.PolicyProvider
security.provider.10=com.ibm.security.jgss.mech.spnego.IBMSPNEGO
```

g. Optional: Go to `<install-dir>\AppScan Enterprise\Liberty\jre\bin` and open a **cmd** window. Your certificates must be at least 1024 in size and can be signed with a DSA or RSA signature algorithm. The keytool utility can be used to generate a compatible keypair: *1 keytool -genkey -alias default -keyalg RSA -keysize 1024 -dname CN=example -keystore fips.jks -storepass Liberty -keypass Liberty*.

h. Save and close the file, and then rerun the configuration wizard.

2. To enable NIST SP800-131a:
   a. Locate the installation directory of Liberty at `<install-dir>\AppScan Enterprise\Liberty\usr\servers\ase`.
   b. Add the *-Dcom.ibm.jsse2.sp800-131=transition* property to the `jvm.options` file to enable the JSSE2 provider to run in NIST transition mode.
   c. Go to the *server.xml* file in the same directory and replace the *sslProtocol="SSL_TLSv2"* property with *sslProtocol="TLSv1.2"*.
   d. Save and close the file, and then rerun the configuration wizard.

Enabling FIPS 140-2/NIST 800-131a compliance in the Enterprise Console

When FIPS 140-2 compliance is enabled in the Enterprise Console, some functionality that is not FIPS 140-2 compliant will not work as expected or will be disabled, including the Manual Explore plugin. By default, the Enterprise Console is compliant with the NIST 800-131a transition mode. When you run AppScan Server Configuration Wizard, it will detect whether or not your environment is in NIST strict mode and will respect those settings.

About this task

User role: Product Administrator

Procedure

1. In the Enterprise Console, go to the General Settings page of the Administration view, and click **Edit** in the Enterprise Console Settings section.
2. By default, the check box in the *Enable enhanced security* section is cleared. Select the option if your organization must be compliant with FIPS 140-2 or NIST SP

800-131a. When the option is selected, use the Manual Explorer tool to manually explore your application for additional URLs. See Manually exploring your site to add more URLs to the scan to learn how to download and use the tool.

Note: Upon upgrade from version 8.7, the check box keeps the value it had before upgrade. If you were FIPS compliant, then this checkbox remains selected; otherwise, it remains cleared.

3. Click **Done**.

Enabling NIST compliance on AppScan Enterprise to work with SiteProtector

SP800-131a is a requirement that is originated by the National Institute of Standards and Technology (NIST) which requires longer key lengths and stronger cryptography. The specification also provides a transition configuration to enable users to move to a strict enforcement of SP800-131a. The transition configuration also enables users to run with a mixture of settings from both FIPS140-2 and SP800-131a. SP800-131a can be run in two modes: transition and strict. Out of the box, AppScan Enterprise is compliant with NIST transition mode.

Procedure

1. Go to `<install-dir>IBM\AppScan Enterprise\localsetttings.xml`, and make the appropriate edits:
   - For NIST transition (called 'NIST compatible' in SiteProtector), keep the default setting **`<param name='sslCipherMode' value='FIPS' xmins='http://www.iss.net/cml/CorePolicyCommon' ordinal='8' />`**.

     Note: AppScan Enterprise works with SiteProtector 2.9, SiteProtector 3.0 in compatible mode, and SiteProtector 3.0 in strict mode.
   - For NIST strict, replace **`<param name='sslCipherMode' value='FIPS' xmins='http://www.iss.net/cml/CorePolicyCommon' ordinal='8' />`** with **`<param name='sslCipherMode' value='SP800131' xmins='http://www.iss.net/cml/CorePolicyCommon' ordinal='8' />`**.

     Note: AppScan Enterprise works with SiteProtector 3.0 in strict mode, but not with SiteProtector 3.0 in compatible mode nor SiteProtector 2.9.
2. Save and close the file.

Authenticating with the Common Access Card (CAC)

The Common Access Card is the standard identification for active duty uniformed service personnel, Selected Reserve, DoD civilian employees, and eligible contractor personnel in the United States. It is used to enable physical access to buildings and controlled spaces, and provides access to DoD computer networks and systems. The CAC can be used for access into computers and networks that are equipped with various smart card readers. When it is inserted into the reader, the device asks the user for a PIN.

About this task

This task helps you set up AppScan Enterprise to allow CAC authentication over LDAP so that users can log in to AppScan Enterprise without providing a user name and password.

Note: No user actions are required to enable authentication by using Microsoft Internet Explorer. For Mozilla Firefox users, your organization might have specific instructions for enabling CAC in the browser.

Procedure

1. Install AppScan Enterprise by using an LDAP server that contains the CAC users.
2. Make the Product Administrator a CAC user.

   Important: After AppScan Enterprise is configured, there is no other way (except by using a database query) to create the Admin account of the CAC user.
3. Import the full certificate authority chain into the truststore.
   a. Create a keystore file or use your existing keystore.

      Note: To generate a keystore, you can use keytool. AppScan Enterprise ships with keytool, and can be downloaded from `<install-dir>\AppScan Enterprise\Liberty\jre\bin\`

      Use this command:
      ```
      keytool -genkey -alias mydomain.com -keyalg RSA -keystore MyKeystore.jks
      -keysize 2048 - keypass storePassword
      ```
   b. Import the full CA certificate chain that signed the client certificates that exist on the CAC cards.

      Note: You can use a Java iKeyman tool to manage your digital certificates. With iKeyman, you can add certificate authority (CA) roots to your database, copy certificates form one database to another, request and receive a digital certificate from a CA, set default keys, and change passwords. The iKeyman utility is shipped with AppScan Enterprise and is stored in `<install-dir>\AppScan Enterprise\Liberty\jre\bin\ikeyman.exe`. You can download additional information on iKeyman from IBM DeveloperWorks: iKeyman Guide.
   c. Add the CA certificates, one at a time, and create a label for each one. If you use iKeyman, you can also create a label for each one. Once you finish adding all the certificates of the full chain, close the iKeyman tool.
4. Modify the `web.xml` file to replace Form-Based Authentication with Client-Certificate Authentication.
   a. Stop the *IBM Security AppScan Enterprise Server* service.
   b. Locate the `AppScanServerWeb.war` file of your AppScan Enterprise instance that is in: `<install-dir>\AppScan Enterprise\Liberty\usr\servers\ase\apps\AppScanServerWeb.war`.
   c. Rename the `AppScanServerWeb.war` file to `AppScanServerWeb.zip` and navigate into the `WEB-INF` folder to retrieve the `web.xml` file for editing.
   d. Replace the following section of the file:

      ```
      <login-config>
           <auth-method>FORM</auth-method>
           <form-login-config>
              <form-login-page>/pages/Login.jsp</form-login-page>
              <form-error-page>/pages/Login.jsp?Retry=True</form-error-page?
           </form-login-config>
         </login-config>
      ```

with

```
<login-config>
     <auth-method>CLIENT-CERT</auth-method>
   </login-config>
```

e. Save the file and rename `AppScanServerWeb.zip` to `AppScanServerWeb.war`.

5. Modify the `server.xml` file to enforce SSL protocol, set the trust keystore and set the LDAP certificate mapping.
   a. Locate the `server.xml` file at `<install-dir>\AppScan Enterprise\Liberty\usr\servers\<ase instance name>\server.xml`.
   b. Make sure that the `<featureManager>` section contains `<feature>ssl-1.0</feature>`.
   c. Locate the `<keystore>` section of the file and add this line: `<keyStore id="cacTrustKeyStoreID" password="store password" location="cacTrustKeyStore.jks" type="jks" />`, where
      - **id** is a string that uniquely identifies the keystore (use any string)
      - **password** is the password of the keystore (this value can be stored in clear text or encoded form; use the *securityUtility* from Liberty to encode the password)
      - **location** is an absolute or relative path to the keystore file (the relative path points to `<install-dir>\AppScan Enterprise\Liberty\usr\servers\<ase instance name>\resources\security\`
      - **type** is the type of the keystore. *jks* is the default value.

      Note: See Liberty profile: Keystores.
   d. Locate the `<ssl>` section of the file, and make sure that it includes `<ssl-Protocol="SSL_TLSv2">`.
   e. Add these attributes to `<ssl>`
      - `trustStoreRef="cacTrustKeyStoreID"` where `cacTrustKeyStoreID` is the ID of the keystore that was configured in the `<keystore>` section of the file.
      - `clientAuthenticationSupported="true"`

      The section might look like this example when you're done editing: `<ssl id="defaultSSLConfig" sslProtocol="SSL_TLSv2" keyStoreRef="defaultKeyStore" trustStoreRef="defaultKeyStore" clientAuthenticationSupported="true" />`.
   a. Locate the `<ldapRegistry>` section of the file and add these attributes:
      - `certificateMapMode="CERTIFICATE_FILTER"`
      - `certificateFilter="uid=${SubjectCN}"` .

      Note: The "uid" in the LDAP directory must match the attribute of the certificate. Modify this example of a filter so that it maps to your environment. In this example, if the "SubjectCN" of the certificate is "CN=IBM", then the user name (uid) in the LDAP directory must also be "IBM".

      This example shows an LDAP registry configuration that uses IBM Tivoli® Directory Server. The LDAP user ids match the subject CN in the certificates that are stored on the CAC card:

```
<ldapRegistry ldapType="IBM Tivoli Directory Server" host="<<host name>>"
port="<<Port no>>" sslEnabled="false" baseDN="o=IBM,c=US"
```

```
certificateMapMode="CERTIFICATE_FILTER" certificateFilter="uid=${SubjectCN}">
<activedFilters userFilter="(objectclass=Person)" userIdMap="*:uid"/ >
</ldapRegistry>
```

6. Restart the *IBM Security AppScan Enterprise Server* service.

Results

Users that use Common Access Cards are able to log in to AppScan Enterprise without providing a user name and password.

Advanced installation scenarios

Installing multiple instances of the Enterprise Console on a single server

You have the option of installing a default instance, or multiple instances on a single computer. Each instance is an independent set of configuration information with its own database.

You might want to consider installing multiple instances when you need to support multiple environments on a single large server. For example, if your organization is structured into business units, each with its own website, you can install one instance of the Server for each. Each group can have its own Enterprise Console and database, independent of the others.

You can install multiple instances of the Enterprise Console or the Agents. For installation instructions, see Running the Server Configuration Wizard.

You might want to install the default instance first, and then install additional named instances as required. There is no limit to the number of named instances that you can run on a single computer.

Note:

- If you add a new instance using the Configuration Wizard, you must restart the Agent Service to incorporate the change.
- If you are installing more than one instance on a single computer, you might want to consider scaling the hardware accordingly. Running a number of instances should not adversely affect the performance of the scan; however, how your web server is structured, the kinds of technologies used on the website, and so on, can affect the amount of resources required by each instance.
- You can only install one alerting service per installation; otherwise, you might receive duplicate notifications.

Related tasks:

"Uninstalling an instance of the Enterprise Console" on page 100
Remove instances that are no longer needed on a single server.

Setting up an external scanner for AppScan Enterprise in the DMZ

If you're testing websites that are outside the firewall, you can set AppScan Enterprise to go through the firewall to test them. However, opening a port through the firewall poses a security risk, as does having a system that stores potentially sensitive files outside the firewall (such as logs and scan data). As an alternative, consider setting up a proxy to provide access outside the firewall.

Procedure

1. Create local accounts on all of the Dynamic Analysis Scanners with the same user name/password to be used as the service account and for login during installation. Administrative accounts are preferred; see “Required user account information during installation and configuration” on page 22 for a list of specific permissions.
2. A connection between the scanner and ASE database is required. Open the standard MS SQL ports 1433/1434 in the firewall, or add a custom port if communication with SQL Server is configured this way and is preferred.
3. Run the configuration wizard. In the Database Connection window, enter the server name and port numbers when prompted.
4. While the configuration wizard is running, you will encounter this error: "The server or role does not exist." This message displays because you are using local accounts, but it doesn't affect the installation. To bypass the error, use the Ctrl key while you click OK in the message dialog.
5. Finish the configuration wizard and exit.

Installation roadmap for AppScan Source deployment

Information to help you understand the requirements for a successful installation.

1. Search for AppScan Enterprise Server 9.0.1 on Passport Advantage and download the eAssembly for your operating system and begin the installation.
2. If you do not already have a Rational License Server in your organization, install it when prompted during the installation wizard.
3. Log into the Rational License Key Center to get your license keys for AppScan Enterprise.
4. Import licenses into the Rational License Server. Determine which licenses you need for AppScan Enterprise Server.
5. **Optional for a distributed installation:**
   - Install SQL Server and configure the database.
   - Create a wizard user account for the database.
6. If you will be using an LDAP Server, configure it now.
7. Run the Server Configuration Wizard. Follow the screen prompts, and if you are using LDAP authentication, choose **LDAP authentication** in the Authentication Mechanism screen. Otherwise, choose **Windows authentication**, which is the default mechanism for new users.

   Note: If you need to run and view reports, configure the Enterprise Console as well as the User Administration component.
8. Install AppScan Source. See the documentation for complete details.
9. “Configuring an AppScan Source Oracle database with AppScan Enterprise Server.”

Configuring an AppScan Source Oracle database with AppScan Enterprise Server

If you are configuring AppScan Source to log into AppScan Enterprise, a Java Virtual Machine (JVM) parameter needs to be added to tell AppScan Enterprise where your AppScan Source Oracle `tnsnames.ora` file is located. How you do this depends on your OS and configuration.

Procedure

1. The parameter to add is: -Doracle.net.tns_admin={path to directory containing the tnsnames.ora file). For example: **-Doracle.net.tns_admin=c:\oracle\product\10.2.0\client_1\NETWORK\ADMIN**
2. Choose your deployment:
   a. If you are running on Windows, update the <install-dir>/appscan enterprise/Liberty/usr/servers/ase/jvm.options file.
   b. If you are running on Linux, update the /opt/IBM/AppScan_Server/Liberty/usr/servers/ase jvm.options file.
3. Stop the Liberty service and restart it for the changes to take effect.

Configuring more than one IP address for the host computer

If the computer that hosts AppScan Enterprise Server uses more than one IP address, you must modify the server.xml file so that AppScan Enterprise can properly authenticate with Liberty.

Before you begin

This procedure assumes that you added the multiple IP addresses to your host file on the computer where AppScan Enterprise is installed.

Procedure

1. Stop the **IBM Security AppScan Enterprise Server** service.
2. Locate the server.xml file at <install-dir>\AppScan Enterprise\Liberty\usr\servers\<ase instance name>\server.xml and open it in an XML editor.
3. Locate the <httpEndPoint> section and if the "host" equals a host name, replace it with an asterisk instead, such as host="*".
4. Save and exit the file.
5. Start the **IBM Security AppScan Enterprise Server** service.

Uninstalling an instance of the Enterprise Console

Remove instances that are no longer needed on a single server.

About this task

If you have more than one instance of the Enterprise Console, use this procedure to remove the instance that is no longer required.

Procedure

1. Go to **Start** > **AppScan Enterprise Configuration Wizard**.
2. Go through the wizard until you get to the Instance screen.
3. Clear the **Use default name** check box.
4. Select the name of the relevant instance, click **Remove**, confirm the removal when prompted, and finish the wizard.

Un-installing the software

You might want to uninstall and reinstall the Server if the installation failed.

Procedure

1. Go to Control Panel and remove the IBM Security Dynamic Analysis Scanner and IBM Security AppScan Enterprise Server software.

2. After you remove the application from the hard disk drive, go to the application installation directory in Program Files and delete the application folder.
3. Reinstall the application.

Chapter 3. Upgrading and migrating

Product changes when you upgrade from a previous version

Learn about changes that might affect your scans or report data when you upgrade from a previous version. Make sure that you read all the topics so that you understand the upgrade process.

Upgrading from 9.0.2.1

- On the **Restore AppScan Server Settings** screen of the configuration wizard, an additional option has been added that preserves custom scanner *.jar files that might have been added to the `<install-dir>\IBM\AppScan Enterprise\Liberty\usr\servers\<instance_name>\lib\scanners`.

Upgrading from 9.0.2

- In previous releases, imported issues were cumulative. In v9.0.2.1, you can remove issues that were previously found in an application but are not included in subsequent imports. In scanner profiles from v9.0.1, the **Remove Orphaned Issues** check box is disabled in v9.0.2.1 to respect previous behavior (can be overridden by clearing the check box).
- When you add a new issue attribute name to a scanner profile, the **Use Imported Values** check box is enabled by default. Keep the **Use Imported Values** check box enabled if you want to update an existing issue attribute with values contained in the imported file. If you clear the check box, AppScan Enterprise will retain the value previously used. If you select the **Unique** check box, you cannot clear the **Use Imported Values** check box.
- There were changes to the REST APIs.

Upgrading from 9.0.1

- There is a **`New`** issue status. Upon upgrade, the **`New issue`** column is available for display in the Portfolio tab in the Monitor view. Formulas are updated to include issues with a **`New`** status. Upgrade does not affect the status of issues that were discovered in previous versions.
- A new Dashboard tab displays the charts that were displayed in the Portfolio tab in v9.0.1. The new dashboard includes trend charts for **`Security Risk Rating`**, **`Testing Status`**, **`Applications with Open Issues`**, and **`Open Issues`**.

  Note:

  Possible naming conflicts between v9.0.1 application attribute customizations and new v9.0.2 dashboard trend charts

  The **`Open Issues`** and **`Applications with Open Issues`** charts rely on a new application attribute called "Open Issues" that is defined as a formula. However, if you previously created an application attribute called "Open Issues" of any type other than formula, the upgrade does not attempt to resolve the conflict between your attribute and the one that version 9.0.2 needs for the new charts.

  The new charts will not display as intended after upgrade, and you must resolve this problem manually. Rename your "Open Issues" attribute to something else if you want to preserve its values. Update all formulas where you referenced your

"Open Issues" attribute to reflect the new name. Then, rerun the configuration wizard to create the "Open Issues" formula attribute that the new charts require.

- A new approach to create scans consistent with AppScan Standard, for both the security team who creates the templates and for the developers who create the scans. See “Overview of scan configuration differences in v9.0.2 and previous versions” on page 143.
  - The new method is accessed from both the Monitor and Scans views.
  - Existing scan templates from v9.0.1.1 are kept after upgrade, and the old method of QuickScan template creation still exists.
  - To take advantage of this new method, during upgrade you must run the Default Settings Wizard after the Configuration Wizard to install the templates for v9.0.2.
  - To avoid any template name conflicts in the **Templates** directory in the Folder Explorer, **(v9.0.2)** is appended to the template name.
  - If you install a new instance of AppScan Enterprise, you can still access the templates from v9.0.1.1. When you create a new content scan or template from the Scans view, select **Create using previously saved settings file** and go to `<install-dir>\AppScan Enterprise\Initializations\ASE\DefaultTemplates\Job\Version 9.0.1.1` to select the *.xml file.
- The embedded version of Liberty is now v8.5.5.4. During configuration, you can choose to restore previous AppScan Server customized settings on the Liberty Server. See Restore AppScan Server settings.

For further details on what's new and changed since v9.0.1.1, read this whitepaper.

Upgrading from 9.0

- AppScan Enterprise v9.0.1 includes an architecture redesign to reduce the installation footprint and to remove IBM Rational Jazz Team Server (Jazz Team Server) as the user authentication component. With the removal of Jazz Team Server, the Apache Tomcat and WebSphere Application Server deployment servers are no longer supported in v9.0.1. They are replaced with IBM WebSphere Application Server Liberty Core v8.5.5.2. See “Replacing Jazz Team Server with WebSphere Liberty - Frequently asked questions” on page 108.
- For new instances of v9.0.1, the risk rating formula has changed. If you are upgrading from v9.0, the risk rating formula remains the same, and your risk ratings remain consistent. However, you can use the new formula `IF(businessimpact = 0, 0, IF(testingstatus > 0, 0, businessimpact * rr_maxseverity))` by replacing the old formula in the application profile template in AppScan Enterprise.
- **Issue management through application view**: In v9.0, issue management privileges were set on the folder that contained a scan. In v9.0.1, issue management is set on the application. Upon upgrade from 9.0, if a scan is already associated with an application, users who used to have issue management privileges on the folder will now have basic permissions on the application so they can continue managing these issues. There is the potential of giving them access to scans they previously were not allowed to access. For example,

v9.0	v9.0.1	Result
Folder A: (Bob has an Issue Manager role) • Scan X • Scan Y Folder B: (Mary has an Issue Manager role) • Scan A • Scan B	Application 1 is associated with these scan jobs: • Scan X • Scan B	Mary now has basic access permissions to Scan B so that she can continue to do her job but she also has access to Scan X, which she didn't have in v9.0.

To restrict a user's permissions to managing issues on specific applications, remove them from the Basic Access on the applications they are not allowed to access. In the example above, remove Mary's Basic Access permissions on Scan X. To find the application that contains Scan X, go to the Scans view and flatten the hierarchy to show only jobs. Find Scan X and click the link for the application name it is associated with. On the Application tab, click **View details** and in the **Users** section of the dialog, remove Mary's Basic Access permissions.

Upgrading from 8.8

- Server Groups are no longer defined by URLs. Any existing URL definitions will be removed from existing Server Groups. Check the WFCfgWiz.log for details.
- HTTPS has replaced HTTP as the scheme required for login and REST Services.
- Some reports have been removed because they no longer fit the product direction. Read the Deprecated features topic.

Upgrading from 8.7

- **Common scan engine between AppScan Standard and AppScan Enterprise**: A new common scan engine provides a more standardized scan job option configuration. As such, some reports are no longer available in AppScan Enterprise:
  - Correlated Security Issues (AppScan DE) report
  - Image Catalog report
  - Metadata Catalog report
  - Missing Alt Text report
  - Missing Titles report
  - Multimedia Content report
  - Server Side Image Maps report
  - Third Party Links report
  - Web Applications report
  - Web Beacons report
  - Website Technologies report
- **Load balancing option removed**: Load balancing on starting URLs and domains is no longer available with the new standardized scan job option configuration. Upon upgrade, jobs that had load balancing set will use the new common engine to run without the load balancing option.
- **User licensing**: The service account license type has been removed. Upon database upgrade, the Configuration Wizard will set the service account license type to the same license type as the Default User (one of floating user scanning, floating user reporting, authorized user scanning, or authorized user reporting).
- **Enabling FIPS 140-2 compliance on the Enterprise Console**: Name and behavioral changes to incorporate NIST compliance have been made to the

General Settings page where this is enabled on the Administration tab. The "Enable enhanced security" check box has been renamed "Disable Manual Explorer Plugin", and upon upgrade, the check box keeps the value it had before upgrade. If you were FIPS compliant, then this check box remains selected; otherwise, it remains cleared. If your organization is a US federal agency and must comply with FIPS 140-2 or NIST SP800-131a, enable the check box to make the Enterprise Console compliant with those security standards.

- **Case-sensitivity** has moved from the domain to the job level. Set it on the job's What to Scan page.
- **Deprecated reports**: The OWASP Top 10 2010 report has been replaced with the 2013 version in v8.8. However, if you have report packs and dashboards that used the 2010 report, the data will not be lost. New instances of AppScan Enterprise 8.8 will only use the 2013 report.
- **Login attempts algorithm changes:** Prior to version 8.8, the scan would attempt to log in three times before suspending. Now the scan attempts for 90 seconds before suspending.

Upgrading from 8.6

Note: Upgrading to 8.7 includes a one-time database optimization step that requires additional time and could extend the overall upgrade process.

- **The previously used method for protecting data "at rest" (physical media) has been deprecated and will be removed as part of the upgrade process.** Read "Data protection through encryption" on page 85 before you begin upgrading.
  - A new method is available, Transparent Data Encryption (TDE), which is built into **Microsoft SQL Server 2008 Enterprise Edition** and higher. See "Enabling Transparent Data Encryption on SQL Server databases" on page 86 for details on encryption and how to enable TDE. To improve database upgrade performance, enable TDE after the database upgrade has completed.
  - For **Microsoft SQL Server 2008 Standard Edition** and higher, other third party encryption methods are also available, including MS Windows Encrypting File System. See "Encrypting, backing up, and restoring a SQL Server database with EFS" on page 89.
- **Additional disk space is required during the upgrade process on the database server**, roughly equal to the size of the existing AppScan Enterprise database. This space will be used temporarily during upgrade and returned after upgrade is completed.
- **Scans will now use a local (embedded) database file.** It is important to have sufficient disk space that is allocated to Agent Server machines. For more information, see the Dynamic Analysis Scanner section in the"Installing all required components on one computer" on page 37 topic for more information about how the local database file works during scanning.
- **Enabling FIPS 140-2 compliance:** Products that support FIPS 140-2 standards can be set into a mode where the product uses only FIPS 140-2 approved algorithms and methods.
- **Previous folder items that were suspended are now "Ready" after upgrade**. Any folder items that were in a suspended state before upgrade are now in a ready state. An icon will identify these items so that you can decide whether further investigation or actions are required.
- **XRule filters on report packs**: XRule filters were removed from report packs. Any reports that contain XRules will contain more data after the report pack is rerun.

Upgrading from 8.5.0.1

- **Aligning default scan job options with AppScan Standard:** Existing jobs and templates that are created in versions before 8.6 do not automatically update to use new job options that have new default values. Only new job/templates use new default values.
- **Installer/config wizard workflow**: During installation of v8.6, you can choose to install a brand new Jazz Team Server or use an existing one.

Upgrading from 8.5.0.0

- **User Licenses**: During upgrade, the License Serve is queried to determine which user license you have the most licenses for, and changes the license type for all users (excluding the Service Account and Product Administrator) to that license type. If you must change the license type for any of your users, go to **Administration** > **Users and Groups** and change them there.
- **Finding variants**: When you import an assessment file from AppScan Source, if the findings differ only by the trace, AppScan Enterprise rolls up those findings into a single issue with multiple variants.
- **Changes to service account:** Service account impersonation no longer supported. Any jobs that use that service account will suspend. Edit the properties with a proper username/password and re-run the job.

Upgrading from 8.0.0.0

Version 8.5 and 8.6 use the Rational License Server. It is critical that you read and understand "Product and user licenses" on page 28 before you install the current version.

Fix pack installation

Fix packs are available for download from Fix Central.

Before you begin

You will need to know your Passport Advantage login credentials for this task.

Procedure

To download the fix pack:

1. Go to http://www.ibm.com/support/fixcentral/ and sign in using your IBM ID and password.
2. Select *Security Systems* in the Product Group list and click **Continue**.
3. Select *IBM Security AppScan Enterprise* in the Product list.
4. Select the latest version number in the Installed Version list.
5. Select *Windows* or *Linux* in the Platform list, and click **Continue**.
6. In the Identify fixes page, select *Browse for fixes* (or choose another search method), and click **Continue**.
7. In the Select fixes page, select the *Interim fix* check box, and click **Continue**.
8. Enter in your Passport Advantage credentials into the *Sign in* page and click **Continue**.
9. In the Download options page, choose your download method (Download Director or your browser), and click **Continue**.

To install the fix pack:

10. Navigate to the directory where you downloaded the executable and double-click the files you downloaded..
11. In the Setup Wizard, click **Next**.
12. In the License Agreement dialog box, choose the "I accept the terms in the license agreement" option, and click **Next**.
13. The Fix pack is installed. When the installation is finished, it will launch the Configuration Wizard (If Config Instances is selected); click **Next**.
14. Exit the installation.

Replacing Jazz Team Server with WebSphere Liberty - Frequently asked questions

Beginning with v9.0.1, AppScan Enterprise includes an architecture redesign to reduce the installation footprint and to remove IBM Rational Jazz Team Server (Jazz Team Server) as the user authentication component.

1. *What exactly is being replaced, and why?*

   With the removal of Jazz Team Server, the Apache Tomcat and WebSphere Application Server deployment servers are no longer supported in v9.0.1. They are replaced with IBM WebSphere Application Server Liberty Core v8.5.5.2. Liberty is a lightweight version of IBM WebSphere, and because it is embedded in AppScan Enterprise, there are no separate installation and configuration steps required. Liberty has a lighter footprint, optimizes resource usage, and eliminates the need to administer users in an extra database.

   Note: In AppScan Enterprise v9.0.2, support for Liberty Server v8.5.5.2 has been replaced with v8.5.5.4.

2. *What is WebSphere Liberty?*

   IBM WebSphere Liberty is a lightweight version of WebSphere, and is easier to install and configure. Liberty is embedded into AppScan Enterprise 9.0.1, eliminating the need to install an extra component in your environment.

3. *What operating systems does it run on?*

   Liberty runs on the same OS as AppScan Enterprise: Windows and Linux Redhat (for AppScan Source user administration component only).

4. *What happens to my Jazz Team Server settings during upgrade to v9.0.1?*

   During upgrade, the Jazz Team Server folder is backed up and stored in the installation folder (`JazzTeamServer.bak`) and the Liberty server is installed. Static credentials are not preserved in case LDAP does not allow anonymous access. During configuration, you are prompted to provide your user name and password for the LDAP server.

5. *Can I roll back to using Jazz Team Server?*

   You can roll back to AppScan Enterprise v9.0.0.1 and use Jazz Team Server. You will not be able to take advantage of any new products features in v9.0.1, as Jazz Team Server is not supported.

6. *I am using Jazz Team Server users without LDAP or Windows authentication. How do I migrate my users to this new authentication method?*

   You can export a .csv file of users by using the **cd <install-dir>\Appscan Enterprise\JazzTeamServer\server\ repotools-jts.bat -exportUsers toFile=C:\users.csv repositoryURL=https://<hostname>:9443/jts**. Then follow the steps in “Migrating Jazz Team Server users to Liberty in AppScan Enterprise” on page 111 to import the users into Liberty.

7. *I still use WebSphere Application Server for other IBM applications. Will I need to do anything to make sure that nothing is affected by these new changes in v9.0.1?*

   WebSphere Application Server can co-exist with Liberty, provided they use different ports. During AppScan Enterprise configuration, you can change the port number for Liberty from 9443 to use a different number.

8. *What happens to the ASC application of AppScan Enterprise that runs on Tomcat?*

   WebSphere Liberty Profile replaces Tomcat + Jazz Team Server + ASC. A Liberty profile is created, and uses the same instance name as AppScan Enterprise. The configuration wizard makes all of these changes for you. You can remove the reference to the ASC application in WebSphere Application Server if you wish. The `asc.properties` file is kept after upgrade for use if you use AppScan Source with an Oracle database.

9. *In my current environment, I have a Jazz Team Server for ASE and a different Jazz Team Server for Rational Quality Manager. They are both pointing to the same LDAP server. What happens to My RQM Jazz Team Server instance if you are removing Jazz Team Server from AppScan Enterprise v9.0.1?*

   Both products use different versions of Jazz Team Server, and so the Jazz Team Server version used by Rational Quality Manager will not be affected by the removal of Jazz Team Server in AppScan Enterprise v9.0.1. During upgrade, the AppScan Enterprise installer removes the Jazz Team Server that the previous version used and replace it with Liberty. The new Liberty server is used to point to the LDAP server. Because Rational Quality Manager and AppScan Enterprise have the same user base registered in the LDAP server, users are still recognized by both products. No extra work is required to re-input users.

10. *Will AppScan Enterprise retain the mapping between user groups and LDAP groups?*

    Yes. We retain the server host, server port, base dn, and the uid mapping.

11. *Do I need any certificates for Liberty to secure IIS?*

    Yes. If you don't have a server certificate, you can request one from your certificate authority and then use it during the configuration wizard. See "Using a certificate in your certificate store with Liberty" on page 34.

12. *I'm a US federal government agency. Does Liberty support FIPS 140-2 and NIST SP800-131a security standards?*

    Switching to Liberty does not affect the level of support that is provided in previous versions. See "Enabling FIPS 140-2 or NIST SP800-131a on WebSphere Liberty Profile" on page 93.

13. *I use a non-standard port number for Jazz Team Server. Will the move to Liberty respect this use?*

    Yes. Using a non-standard port is supported; modify the default port during configuration.

14. *Can I upgrade from all previous versions of AppScan Enterprise? What happens for my particular deployment scenario?*

    All previous versions can upgrade to use Liberty. This table explains how the upgrade works for each deployment scenario:

Table 14. Scenario migrations

Scenario	Upgrading from older versions to V9.0.1
Jazz Team Server + LDAP on local server	During upgrade, the Jazz Team Server folder is backed up and stored in the installation folder (`JazzTeamServer.bak`) and the Liberty server is installed. Static credentials are not preserved in case LDAP does not allow anonymous access. During configuration, you are prompted to provide your user name and password for the LDAP server. During configuration, AppScan Enterprise pre-populates as many of the LDAP settings from the backup it made during installation. You must complete the LDAP settings.
AppScan Source (using LDAP users with SolidDB)	During upgrade, the Jazz Team Server folder is backed up and stored in the installation folder (`JazzTeamServer.bak`) and the Liberty server is installed. Static credentials are not preserved in case LDAP does not allow anonymous access. During configuration, you are prompted to provide your user name and password for the LDAP server. During configuration, AppScan Enterprise pre-populates as many of the LDAP settings from the backup it made during installation. You must complete the LDAP settings.
Jazz Team Server with Windows authentication (also applies to AppScan Source with Windows authentication)	During installation and configuration, all the necessary settings are propagated. No user action is required.
Jazz Team Server + LDAP on remote server	During configuration, you must enter LDAP settings when prompted. You can delete the ASC application from Jazz Team Server if wanted.
Jazz Team Server (using JTS user authentication only) on local or remote server	You must manually add those users into the Liberty `server.xml` file. This file is stored in `<install-dir>\AppScan Enterprise\Liberty\usr\servers\ase`.
WebSphere Application Server + LDAP on remote server	During configuration, you must complete the LDAP settings when prompted. You can delete the ASC application from WebSphere if wanted.
AppScan Source (using ASE Jazz Team Server users)	During installation, AppScan Enterprise uninstalls Jazz Team Server on Tomcat, makes a backup of the settings, and then deletes Jazz Team Server. Nothing changes during configuration.
AppScan Source (using LDAP users with Oracle Source DB)	Change the filepath in the `asc.properties` file from Jazz Team Server to Liberty. See "Upgrading the AppScan Source LDAP connection with an Oracle database" on page 119.

Migrating Jazz Team Server users to Liberty in AppScan Enterprise

To migrate Jazz Team users to use the Liberty authentication method, export a .csv file of users by using a command before you begin upgrading to v9.0.1 and higher. Then, you can follow one of the following two methods and register the same users in Liberty so that they can access AppScan Enterprise v9.0.1 and higher.

```
cd <install-dir>\Appscan Enterpise\JazzTeamServer\server\ repotools-jts.bat
-exportUsers toFile=C:\users.csv repositoryURL=https://<hostname>:9443/jts
```

Note: User passwords are not exported in the .csv file.

Authenticating with Windows Local Account Users

The option to use this type of authentication is not explicitly displayed in the configuration wizard due to limited support for this option. The product administrator must follow several manual steps to set up this type of authentication.

Procedure

1. During configuration, select **Windows Authentication** in the Authentication Mechanism screen of the configuration wizard, click **Next**, and complete the wizard.
2. Create local Windows users on the computer that hosts the Enterprise Console. The administrator must have computer access to create local Windows users.

   Note:

   a. These local Windows user IDs and passwords are to be used to access AppScan Enterprise.
   b. In this case, password expiry is governed by Windows policies. Password management is handled by the AppScan Enterprise product administrator by manually changing the user's passwords on the computer that hosts the Enterprise Console.
   c. If you need to run the AppScan Enterprise configuration wizard again on the computer that hosts the Enterprise Console, the authentication option remains set as “Windows Authentication”. No further tweaking is necessary to preserve the authentication method that is already set up.
   d. If you are migrating users from Jazz Team Server into this authentication method, there is a way to preserve each user’s AppScan Enterprise user settings. A custom SQL script can be run to remap older user IDs to newer ones. Run this custom script with help from IBM.

Authenticating with Liberty Basic User Registry

The option to use this type of authentication is not explicitly displayed due to limited support for this option. A number of manual steps are required to set up this type of authentication.

About this task

After you follow this procedure, you must use the local user account to log in to AppScan Enterprise. You cannot use the service account.

Procedure

1. During configuration, select **Windows Authentication** in the Authentication Mechanism screen of the configuration wizard, click **Next**, and complete the wizard.
2. Stop the IBM Security AppScan Enterprise Server service. You can type "net stop IBM Security AppScan Enterprise Server" in a command prompt window, or follow these steps:
   a. Go to the Windows Service Management Console (**Start** > **Run** > **services.msc**).
   b. In the Services section, right-click *IBM Security AppScan Enterprise Server* and select **Stop Services** in the menu.
3. Locate the **server.xml** file at <install-dir>\AppScan Enterprise\Liberty\usr\servers\<ase instance name>\server.xml and open it in an XML editor.
4. Locate and remove the <feature>usr:WindowsRegistryFeature</feature> section.
5. Add a basic user registry section to the server.xml file as follows:

```
<basicRegistry id="basic">
     <user name="mlee" password="p@ssw0rd" />
     <user name="rkumar" password="pa$$w0rd" />
     <user name="gjones" password="{xor}Lz4sLCgwLTs=" />
   </basicRegistry>
```

   Note:
   a. You must use unique names for your users and groups.
   b. Remove all trailing and leading spaces from the user and group names.
   c. If user ID or password contains characters other than US-ASCII, make sure that the file is saved by using UTF-8 character encoding.
6. Optional: Encode the password for each user by using the **securityUtility encode** command. The securityUtility command line tool is available in the <install-dir>\AppScan Enterprise\Liberty\bin directory.
7. Optional: When you run the **securityUtility encode** command, you either supply the password to encode as an input from the command line. If no arguments are specified, the tool prompts you for the password. The tool then outputs the encoded value.
8. Optional: Copy the value output by the tool, and use that value for the password. For example, to encode the password "GiveMeLiberty", run the following command: securityUtility encode GiveMeLiberty. You can encode the password using the “aes” encoding type. If there is a key.xml file located in the <install-dir>\AppScan Enterprise\Liberty\usr\shared\config directory, provide the encryption key specified in key.xml to **securityUtility**. For example, securityUtility encode --encoding=aes --key=<the_key_in_key.xml> GiveMeLiberty. If you do not have a key.xml, you do not need to specify the **--key** option.
9. Restart the IBM Security AppScan Enterprise Server service. You can type "net start IBM Security AppScan Enterprise Server" in a command prompt window, or follow these steps:
   a. Go to the Windows Service Management Console (**Start** > **Run** > **services.msc**).
   b. In the Services section, right-click *IBM Security AppScan Enterprise Server* and select **Start Services** in the menu.

10. If you install the Enterprise Console on more than one computer, you must repeat this process on every computer.

    Note: Liberty does not provide a mechanism for password expiry, and changing passwords periodically is a manual process that involves encryption steps as described next.

Running the configuration wizard after user migration

If you need to run the AppScan Enterprise configuration wizard again, follow these steps BEFORE you rerun the wizard so that you preserve this authentication method.

Procedure

1. Copy `server.xml` to `server.xml.backup`.
2. Remove the following section from `server.xml`:

```
<basicRegistry id="basic">
     <user name="mlee" password="p@ssw0rd" />
     <user name="rkumar" password="pa$$w0rd" />
     <user name="gjones" password="{xor}Lz4sLCgwLTs=" />
   </basicRegistry>
```

3. Add the `<feature>usr:WindowsRegistryFeature</feature>` section back in.
4. Rerun the configuration wizard.
5. Delete `server.xml`.
6. Rename `server.xml.backup` to `server.xml`

Results

If the user IDs that are recorded in the Liberty basic user registry match the user IDs that were specified in Jazz Team Server, no further configuration is necessary, and the migration is complete. However, if the user IDs do not match after migration, you can run a custom SQL script to remap older user IDs to newer ones. Run this custom script with help from IBM.

Upgrading to the latest version of AppScan Enterprise

For a successful upgrade to the latest version of AppScan Enterprise, read this topic carefully.

Planning the upgrade

Planning an upgrade is similar to planning a deployment. It is important to review your environment and requirements carefully.

Procedure

1. Identify and document hardware elements that host software components:
   - AppScan Enterprise Server (main application server hosted by IIS)
   - AppScan Enterprise dynamic scanning agents
   - Microsoft SQL Server database
2. Create a table like this one to track your information:

Table 15. Proposed environment server requirements

Component	Server	Operating System	Technical Specifications	Required Software
AppScan Enterprise Server				
SQL Server				
AppScan Dynamic Analysis Scanner server				

3. Validate identified software and hardware elements meet the system requirements.
4. Identify and document security elements:
   - Installation account ID, rights and password
   - Service Account ID, rights and password (used for database interaction)
   - AppScan Enterprise URL
   - Product administrator ID and password
5. Export or create a server certificate to use with IBM WebSphere Application Server Liberty Core 8.5.5.6.
6. Check that you have the correct AppScan Enterprise Licenses for your upgrade.
7. Obtain AppScan Enterprise 9.0.2 software from IBM Passport Advantage:
   - AppScan Enterprise Server and License Key Server
   - AppScan Enterprise Dynamic Analysis Scanner
8. If you use AppScan Source, you must also obtain the 9.0.2 software from IBM Passport Advantage. The version number must match for AppScan Source and AppScan Enterprise so that the two products continue to work together. You also need to upgrade your Oracle database.
9. Back up your SQL Server database.
10. If you upgrade your SQL Server, configure the SQL Server database for AppScan Enterprise.
11. Verify product changes that might affect the version you are upgrading from.

Building the staging (testing) environment for upgrade

Use these instructions for building a staging environment or if you are only upgrading your production environment.

Procedure

1. Create three virtual or physical machines (one machine each for the SQL Server, AppScan Enterprise Server and the Dynamic Analysis Scanner) to meet the system requirements.
2. Install required software (Application Services, SQL Server Services, etc.) to support the three components which will make up the staging environment.

   Note: If you do not install SQL Server on a separate machine, make sure that you specify *"HOSTNAME\SQL_SERVER_NAME"* as the SQL Server name in the Database Connection window during configuration. Liberty server does not support "." as a replacement for 'localhost'.

3. Back up the production database, and load the database into the staging SQL Server.
4. Install AppScan Enterprise Server to the application server.
   a. Go to the directory where you downloaded the executable file (`AppScanEnterpriseServerSetup_<version>.exe`) and double-click the file.

      Note: It might take a while for the next screen to appear.
   b. If you do not have Rational License Key Server installed on your network, install it when prompted.
   c. In the Setup Wizard Welcome screen, click **Next**.
   d. In the License Agreement window, select the **I accept the terms in the license agreement** option, and click **Next**.
   e. In the Destination Folder window, select a target location and click **Next**.
   f. In the Ready to Install the Program window, click **Install** to proceed with the installation.
   g. On the Setup Wizard Completed screen, select the check box to launch the Configuration Wizard and click **Finish**.
   h. Run the Configuration Wizard.
   i. Run the Default Settings Wizard.
5. Install AppScan Enterprise Dynamic Analysis Scanner to the dynamic scanner machines. Unzip to machine and run `ASE_DASSetup_<version>.exe`. After you complete the installation, run the Server Configuration Wizard, and repeat for all Dynamic Analysis Scanner machines.
6. Optional: Upgrade AppScan Source to version 9.0.2. See Upgrading AppScan Source for complete instructions.
7. Optional: If you use AppScan Source and connect with an Oracle database, modify the filepath to point to Liberty instead of Jazz Team Server. See “Upgrading the AppScan Source LDAP connection with an Oracle database” on page 119.
8. Optional: If you upgrade from v8.8, the database is unencrypted. Read these topics to learn how to encrypt the database.
   - “Data protection through encryption” on page 85
   - “Enabling Transparent Data Encryption on SQL Server databases” on page 86
   - “Encrypting, backing up, and restoring a SQL Server database with EFS” on page 89

Testing the staging environment

Procedure

1. Verify all configured services are functioning as intended.
2. Verify usage of the IBM AppScan software is functioning as intended.
   - authentication
   - building scans
   - running scans
   - reporting

Results

Once the above steps have been completed, and your Information Security team is satisfied all components of the running software in staging are functioning, stable,

and ready for production use, upgrade to your production server.

Upgrading the AppScan Enterprise production environment

If you are only upgrading your production environment, refer to the detailed instructions explained in the "Building the staging (testing) environment for upgrade" topic above.

Preparing production for AppScan Enterprise Software upgrade

Procedure

1. Notify your users that services will be unavailable for the period of time while upgrade has been introduced, and testing has been completed.
2. Back up the production database.
3. Take existing agent servers out of service before upgrade is performed.
4. Take existing application server out of service before upgrade is performed.
5. Take existing SQL server out of service before upgrade is performed.

Upgrading production AppScan Enterprise software

Procedure

1. Upgrade production AppScan Enterprise Server to the latest release:

   Note:

   - Always uninstall AppScan Enterprise components before installing new versions or fixpacks.
   - Always leave existing components of AppScan Enterprise in place and install on top of these when you apply an iFix or a patch.
2. Upgrade production SQL server to the latest release that AppScan Enterprise supports.
3. Upgrade production Agent Dynamic Analysis Scanner servers to the latest release.
4. Perform system reboot, then put AppScan Enterprise server in service.
5. Perform system reboot, then put Agent Scanner servers in service.

Testing production AppScan Enterprise software post upgrade

Procedure

1. Verify all services are available and ready for use.
2. Verify usage of the IBM AppScan software is functioning as intended.
   - authentication
   - building scans
   - running scans
   - reporting

Configuring the SQL Server database for AppScan Enterprise

The AppScan Enterprise Server configuration needs information about SQL Server. Configure the SQL Server first to save time during the AppScan configuration. If you upgrade SQL Server to a newer version, follow these instructions as well.

SQL Server properties

To define server properties:

1. Right-click the server name and select **Properties** > **Security**.
2. In the Server Authentication section, choose *Windows Authentication mode* and click **OK**.

Note: If your environment uses a named SQL Server instance for the AppScan Enterprise database or SQL Server Express, make sure that TCP/IP is enabled in the SQL Server configuration manager, and restart the SQL services for SQL Server and SQL Server browser. For example, if you specify the instance name as:`SQL Server or Server\Instance name: <sql_server_host>\<sql_server_instance>` instead of `SQL Server or Server\Instance name: <sql_server_host>`.

Encrypting a SQL Server database with EFS

If your configuration uses Microsoft SQL Server Standard Edition, and you plan to encrypt your AppScan Enterprise databases, then this procedure needs to be performed before you install AppScan Enterprise.

Related information:

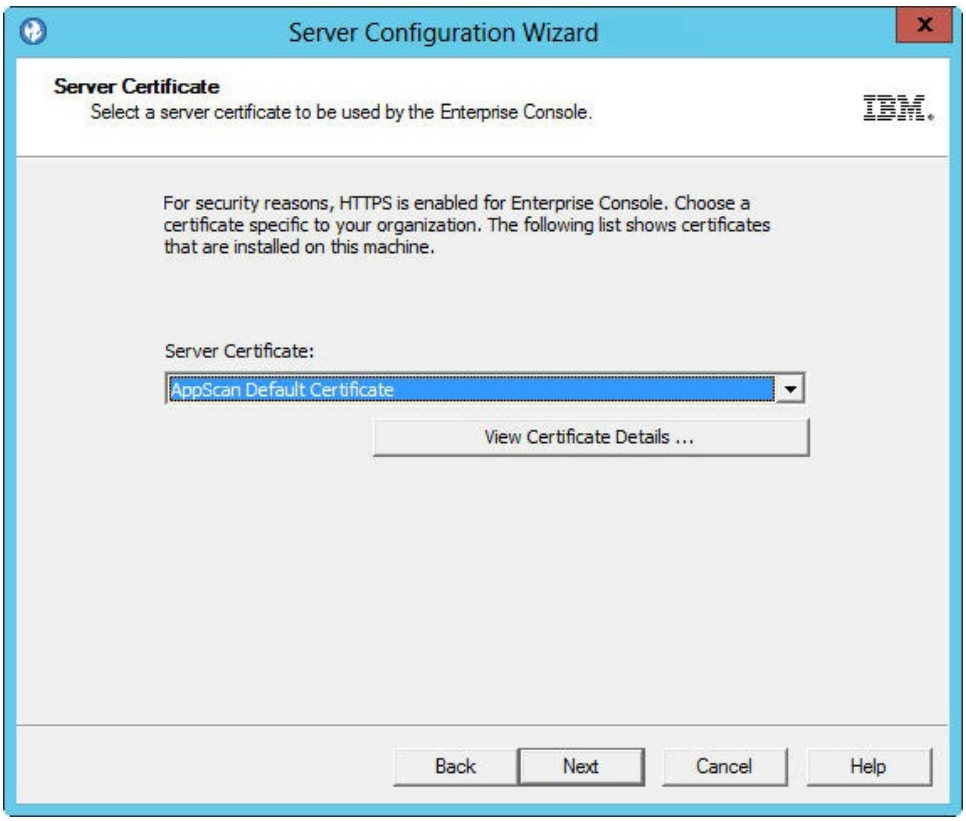
Building Secure ASP.NET Applications: Authentication, Authorization, and Secure Communication

Using a certificate in your certificate store with Liberty

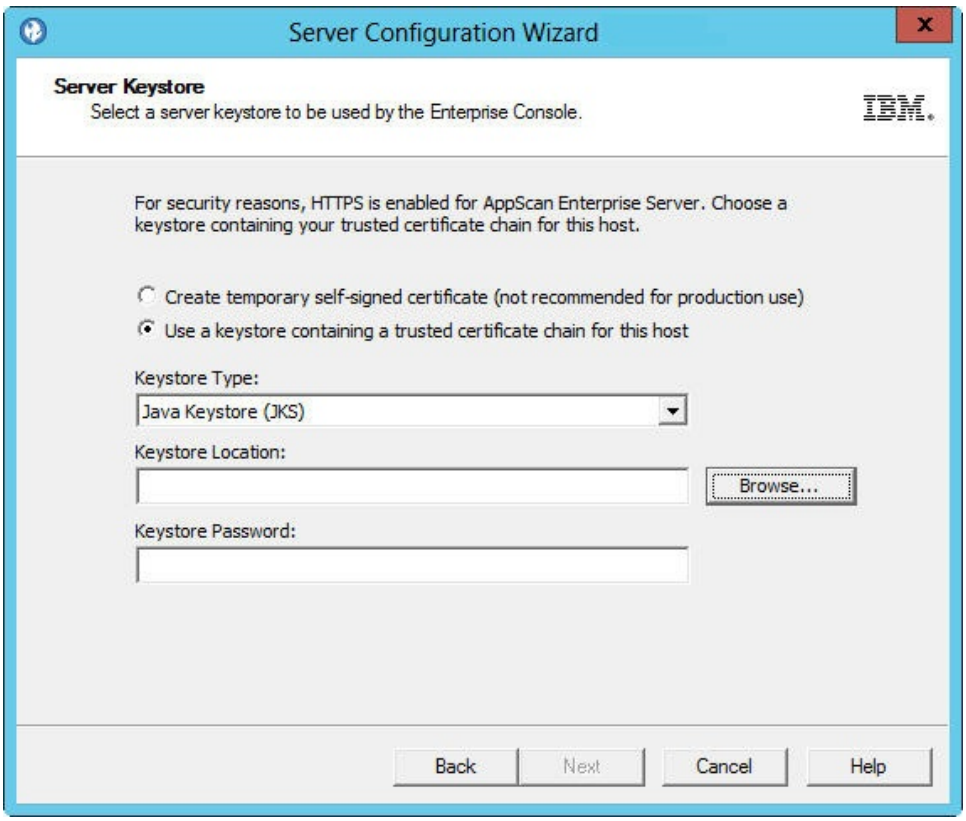
This procedure describes how to use Liberty certificates to secure IIS.

Procedure

1. Optional: If you don't have a server certificate, create one from your certificate authority.
   a. Generate a certificate request to send to your external certificate authority.
   b. Send the certificate request to the certificate authority using a method that the certificate authority accepts.
   c. When you receive the certificate, complete the certificate request.
2. Install AppScan Enterprise Server.
3. Run the configuration wizard.
4. In the Server Certificate window, choose a certificate specific to your organization. This step helps you deploy a secure AppScan Enterprise in your environment. See “Server Certificate” on page 150.



5. In the **Server Keystore** screen, select a server keystore to be used by the Enterprise Console. If you exported a .pfx file, select **Public key cryptography standards #12 (PKCS #12)**. Browse to the location where you saved the .pfx file, import it and enter the password you created when you exported the file. See "Server Keystore" on page 150.



6. Finish the configuration wizard.

Upgrading the AppScan Source LDAP connection with an Oracle database

If you are changing LDAP settings (such as the server name or alias name) or if you are moving the AppScan Enterprise Server to another computer, you must update the `asc.properties` file to reflect those changes.

Procedure

1. Stop the AppScan Enterprise Server services.
2. Edit the file `<install-dir>\AppScan Enterprise\Liberty\usr\servers\ase\config\asc.properties`.
3. Set the value of **`core.db.oracle.jdbc.connection.string`** to the appropriate connection string for the new server. For example, **`ldap://oid:389/r7sol001,cn=OracleContext,dc=company,dc=com`**
4. Make sure that the value of **`core.db.oracle.jdbc.connection.string`** is set to the appropriate alias.. For example, **`r7sol001`**
5. Save the changes and restart the AppScan Enterprise Server services.

Enabling FIPS 140-2 or NIST SP800-131a on WebSphere Liberty Profile

Use one of these procedures to enable FIPS 140-2 or NIST SP800-131a on WebSphere Liberty Profile.

Before you begin

Run the configuration wizard and start the services before you start this task.

Procedure

1. To enable FIPS 140-2:
   a. Locate the installation directory of Liberty at `<install-dir>\AppScan Enterprise\Liberty\usr\servers\ase`.
   b. Add the *-Dcom.ibm.jsse2.usefipsprovider=true* property to the `jvm.options` file to enable the JSSE2 provider to run in FIPS 140-2 mode.
   c. Go to `<install-dir>\AppScan Enterprise\Liberty\jre\lib\security` directory.
   d. In a text editor, edit the *java.security* master security properties file to register additional cryptographic package providers.
   e. Update these two lines:

      ```
      #ssl.SocketFactory.provider=
      #ssl.ServerSocketFactory.provider=
      ```

      to

      ```
      ssl.SocketFactory.provider=com.ibm.jsse2.SSLSocketFactoryImpl
      ssl.ServerSocketFactory.provider=com.ibm.jsse2.SSLServerSocketFactoryImpl
      ```

   f. Locate the list of cryptographic providers that are located after the line # *List of providers and their preference orders* and replace it with the following list:

      ```
      security.provider.1=com.ibm.crypto.fips.provider.IBMJCEFIPS
      security.provider.2=com.ibm.jsse2.IBMJSSEProvider2
      security.provider.3=com.ibm.crypto.provider.IBMJCE
      security.provider.4=com.ibm.security.jgss.IBMJGSSProvider
      security.provider.5=com.ibm.security.cert.IBMCertPath
      security.provider.6=com.ibm.security.sasl.IBMSASL
      security.provider.7=com.ibm.xml.crypto.IBMXMLCryptoProvider
      security.provider.8=com.ibm.xml.enc.IBMXMLEncProvider
      security.provider.9=org.apache.harmony.security.provider.PolicyProvider
      security.provider.10=com.ibm.security.jgss.mech.spnego.IBMSPNEGO
      ```

   g. Optional: Go to `<install-dir>\AppScan Enterprise\Liberty\jre\bin` and open a **cmd** window. Your certificates must be at least 1024 in size and can be signed with a DSA or RSA signature algorithm. The keytool utility can be used to generate a compatible keypair: *1 keytool -genkey -alias default -keyalg RSA -keysize 1024 -dname CN=example -keystore fips.jks -storepass Liberty -keypass Liberty*.
   h. Save and close the file, and then rerun the configuration wizard.
2. To enable NIST SP800-131a:
   a. Locate the installation directory of Liberty at `<install-dir>\AppScan Enterprise\Liberty\usr\servers\ase`.
   b. Add the *-Dcom.ibm.jsse2.sp800-131=transition* property to the `jvm.options` file to enable the JSSE2 provider to run in NIST transition mode.
   c. Go to the *server.xml* file in the same directory and replace the *sslProtocol="SSL_TLSv2"* property with *sslProtocol="TLSv1.2"*.
   d. Save and close the file, and then rerun the configuration wizard.

Chapter 4. Administering

Managing users, groups, and access permissions

User types and roles

User types

Every user is assigned a User Type by the Product Administrator. The User Type applies across an instance.

Product Administrator

The Product Administrator has full access to all areas and can perform the functions of any other type of user.

Standard User

Standard Users are users who are assigned a role in any folder. They can create applications. If the security model within your organization permits, the Default User type can be set to Standard User. That way, the first time a new user logs in, a new user account with a user type of Standard User will be automatically set up. This is a way of automating the creation of new user accounts. Within folders or applications that they can access, a Standard User can:

- Create applications
- Grant application access to users
- Create and delete folders in folders they can access
- Create, edit, run, view, and delete scan jobs
- Create, edit, run, view, and delete dashboards
- Create, edit, run, view, and delete report packs
- Grant or deny users access to report packs, dashboards and folders
- Classify issues according to their status
- Export report data
- Configure all options (Basic and Additional) in the AppScan Dynamic Analysis Client

No Access

Upon trying to log in, if the Default User is set to *No Access*, a new account will not be created. If the user has an existing account, the account remains, but access is denied.

The *No Access* user type is often used to create an account in anticipation of the arrival of a new employee who will require access at some future time.

Inherit Access

This user type only applies to users imported from an LDAP server. When a user with an *Inherit Access* user type logs in for the first time, they will automatically be created as a user (whatever the Default User is) and be assigned the user privileges associated with any LDAP group they belong to, if the group exists in the database

and has been granted access. If they belong to more than one group, they will inherit the highest permissions of all the groups they belong to. Otherwise, their type will be *No Access*.

QuickScan User

QuickScan Users use a simplified view of the Enterprise Console to create quick, easy-to-use scans to test the applications they are responsible for. Most users are QuickScan users. QuickScan Users can be given explicit permissions on specific applications, but they cannot create them.

If a QuickScan user is given access to the advanced scan configuration for the template they are using, there are restrictions on some of the scan options that they can modify. Here are some examples:

- **What to Scan > Additional server and domains**: Modify existing domains and make changes, but cannot add new domain or delete existing domain.
- **Exclude Paths and File > Overall Exceptions**: Add new overall URL exception but not remove them.
- **Explore options > Parser Setting**: Add Search Patterns and Exclusions but not delete any.
- **Explore options > WebSphere Portal Advanced Settings**: Modify the context root, but not delete them.
- **Parameter and Cookies > Normalization Rules**: Add new normalization rules but not delete them.
- **Parameter and Cookies > Custom Parameter Definitions**: Modify the existing parameters and cookies values but cannot add or delete any.
- **Parameter and Cookies**: Modify the existing parameters and cookies values but cannot add or delete any.
- **Login Management**: Cannot delete URL from login sequence.
- **Automatic form fill**: Disable and enable Auto form fill values, but cannot add/delete/modify any.
- **General Scan Options > Custom error pages**: Cannot add/delete/modify any custom error pages.
- **Malware**: Add new exclusion patterns but not delete any.
- **Advanced options > XRules**: Modify XRules but cannot add or delete any.

Other Custom User Types

Product administrators can create custom user types to align with the particular workflows of their organization. These types of users are assigned limited administrative permissions, such as the ability to create and edit users, to configure security test policies and server groups, to modify application attributes, or to manage AppScan Enterprise integrations with other IBM products. See “Custom user type permissions” on page 125 for more details.

Related tasks:

“Defining custom user types” on page 124
A user type is a set of permissions that are applied to a user so that they can perform certain administrative tasks. Before creating user accounts, you must create custom user types if you want to assign limited administrative tasks to Standard Users without making them full Product Administrators.

"Creating a user" on page 128
Create a user and assign a user type to them. As a best practice, when you first create a new user you should give them a No Access user type until you finish configuring their folder permissions, and then change their user type to whatever type you want them to have. This prevents new users from being able to access areas they shouldn't if they log in while you are still configuring their permissions.

User roles

One user can set up and run jobs that scan and analyze a website or application. Another user will only browse through reports that detail the problems that were found with a website or application. Yet another user can set up and administer users.

User roles are assigned on a per folder basis by a Product Administrator, and use a specific user license as well.

Job Administrator

Job Administrators can perform the following tasks:

- Create and delete folders
- Create, edit, and delete templates in Templates folders
- Create, edit, run, view, and delete scan jobs
- Create, edit, run, view, and delete dashboards
- Create, edit, run, view, and delete report packs
- Grant or deny users access to report packs, dashboards and folders
- Select test policies to run on allowed server groups in a content scan job
- Classify issues according to their status
- Retest security issues
- Export report data
- Create XRules using system-defined templates

Report Administrator

Report Administrators can perform the following tasks:

- Create and delete folders
- Edit report packs in Templates folders
- Create, edit, run, view and delete dashboards
- Create, edit, run, view and delete report packs
- Grant or deny users access to report packs, dashboards and folders
- Classify issues according to their status
- Export report data
- Retest security issues (only with scanning license)

Issue Manager

Issue Managers can perform the following tasks:

- Classify issues according to their status
- Retest security issues
- View dashboards and report packs

- Use templates
- Export report data

Report Consumer

Report Consumers can perform the following tasks:
- View dashboards and report packs
- Use templates
- Export report data

No Access (to a folder)

A user who has been assigned a role of No Access in a folder will not be able to see the folder, nor any items in the folder.

Users and groups

Before creating user accounts you need to determine who your users will be and what their role will be in any given folder. When you know this information, you can create users automatically with the default user settings by importing LDAP user groups, or creating them manually. Any valid member of your organization's Windows network can become a user.

As a best practice, when you first create a new user you should give them a *No Access* user type until you finish configuring their folder permissions, and then change their user type to whatever type you want them to have. This prevents new users from being able to access areas they shouldn't if they log in while you are still configuring their permissions.

You must understand:
- The different user types and roles available.
- You can create users automatically by using the Default User template
- You can create users manually if:
  - The Default User template has been assigned a *No Access* user type.
  - You want to assign a specific user type to users before they log in. In this case you must first create the user, then edit their user properties to change their user type. By default, the user type is automatically assumed from the Default User template, so it must be changed after you create a user.
  - You want to deny access to a specific user, and the Default User permits access to anyone with a Windows network account. You must specifically create the user and change their user type to *No Access*.

Defining custom user types

A user type is a set of permissions that are applied to a user so that they can perform certain administrative tasks. Before creating user accounts, you must create custom user types if you want to assign limited administrative tasks to Standard Users without making them full Product Administrators.

About this task

User role: Product administrator

Note:

1. As an organizational security measure, users that are assigned limited administrative permissions see a streamlined view of the Administration tab and will only be able to access the administrative pages they are permitted to use. For example, Rob's user type is set to Inherit Access and he belongs to two groups: the Developers group has a custom user type of Server Group Administrator, and the Business group has a custom user type of User Administrator. When Rob accesses the Administration tab, he will see both the Users and Groups and the Server Groups menu options. However, if Rob has explicitly been assigned a user type, the permissions of the user type will override the permissions of the groups he belongs to.
2. If you edit or delete a custom user type or one of their permissions, **all** users who have been given the custom user type will be affected by the change.
3. If you delete a user type that has been assigned to a user, that user will have a *No Access* user type until you assign them a new one.

Procedure

1. Go to the Administration view of the Enterprise Console.
2. On the User Types page, click **Create**.
3. Create the user type, select their user permissions, and click **Create**.

Related concepts:

"User types" on page 121
Every user is assigned a User Type by the Product Administrator. The User Type applies across an instance.

"How user types affect user groups" on page 131
Every user is assigned a User Type by the Product Administrator. The User Type applies across all folders in an installation.

Custom user type permissions:

These permissions are custom user permissions that you can assign to users to align with the workflows in your organization.

Table 16. Custom user type permissions

Permission	Description
Advanced View	Gives Standard users who have a QuickScan role the additional access to the advanced job configuration UI from the QuickScan configuration.
Add Users/Groups	Adds and edits users and groups but cannot edit user security scan permissions.
Edit Users/Groups	Edits users and groups, including user security scan permissions. The user who is editing security scan permissions can only assign scan permissions that they have, unless the user who is editing also has Server Groups or Security Test Policies permissions. Then all scan permissions are available.
Configure Server Groups	Creates server groups (a group of items that can be tested as a unit) and assigns them to job administrators.

Table 16. Custom user type permissions (continued)

Permission	Description
Configure Security Test Policies	Creates security test policy (a predefined set of security tests). Users must be assigned both a server group and a test policy before they can run security scans.
Configure Global Scan Settings	Provides access to the following pages in the Administration tab: Agent Servers, Servers and Domains, and Custom Error Pages.
Application permissions	
View Trends	Users can see the trend charts in the Dashboard tab.
Delete Any Application	Users can delete any application, regardless of the access that is given for the specific application.
Full DAST Client Configuration Access	Users can view and edit both Basic and Additional scan options in the AppScan Dynamic Analysis Client.
View Application Attributes on All Applications	Users can view all applications. For example, you can create a user type for a Chief Security Officer that allows them to view applications, but not modify or delete application properties.
Modify Application Attributes on All Applications	Users can modify all applications, regardless of the access that is given for the specific application.
Manage Access Control on All Applications	Users can change the access for any individual application, regardless of the access that is given for the specific application.
Modify Application Profile	Users can create, modify, or delete profile attributes (except predefined attributes) to describe applications.
Issue permissions	
Manage Issues on All Applications	Users can perform issue management on all applications. This permission is automatically added to the Basic and Full access type.
Modify Issue Profile	Users can create, modify, or delete profile attributes (except predefined attributes) to define issues.
Modify Scanner Profile	Users can create, modify, or delete profile attributes (except predefined attributes) to define scanners that import issues or findings.
Modify Application Profile	Users can create, modify, or delete profile attributes (except predefined attributes) to define applications and the scans and users that are assigned to them.
Third-party integration permissions	

Table 16. Custom user type permissions (continued)

Permission	Description
QRadar Service Account	This account uses a REST API to pull report data into QRadar. It does not access the user interface.
Publish to QRadar	Grants report access to QRadar.
Configure QRadar Integration	Configures integration with QRadar and can revoke report access.
Publish to SiteProtector	Exports vulnerabilities to SiteProtector.
Configure SiteProtector Integration	Configures integration with SiteProtector.

Access permissions on folders

Access permission control on folders begins at a high level and progresses down to a more granular level on folders and folder items. If a folder item contains sensitive information, you can restrict access to the item.

There are four separate aspects to access control:

1. **User Types**: Applies to all folders in an installation. There are several user types available:
   - *Product Administrator*: Full access, including all product administrative areas.
   - *Inherit Access*: Inherits the maximum access based on the LDAP groups the user belongs to.
   - *No Access*: No access. This user type is often used to create an account in anticipation of the arrival of a new employee who will require access at some future time.
   - *QuickScan User*: Access to a simplified view to create quick, easy-to-use scans to test the applications they are responsible for. **Most users are QuickScan users.**
   - *Standard User*: Access to regular features, with no administrative permissions. Can be assigned different roles in folders.

   Note: In addition to these user types, you can also create a *Custom User Type* to assign a limited set of administrative tasks users. These users only see the *Administration* and *Jobs & Reports* pages they are permitted to see.
2. **User Roles**: Assigned on a per folder basis by a Product Administrator. A user must be granted access permission to every folder where they will perform tasks. Folder permissions determine what the user can see and do within the folder.
3. **Per item/per user**: Assigned on a per folder item basis (report packs and dashboards) by an Administrator.
4. **Per folder**: Assigned per folder by a Product Administrator. When a folder is created, users will inherit the same user roles that exist in the parent folder. For example, all Standard Users in Folder A are Report Administrators. Those users will automatically be Report Administrators in any subfolder, unless an administrator (job, report, or system administrator) manually changes their permissions. system administrators can also propagate user permissions down the folder hierarchy at any time.

Note: All users with a Report Consumer role or greater in a folder are granted **implicit** access to a report pack or a dashboard when one is created in that folder.

You must specifically change their user access to *No Access* if you do not want users to inherit access to an item. Implicit access is inherited through `All Other Users' when the user is not listed on the *Users and Groups* page, and `All Other Users' is assigned access.

Access to a report pack or dashboard is considered **explicit** when you add a user/group to the Users and Groups page of a report pack or dashboard and grant them access.

Related information:

Viewing a report in Policy Tester results in error

The right user role for the right folder

Users can have a different role in each folder that affects what they can do and see in that folder.

For example, the Corporate folder contains *Consumer* and *Business* sub-folders. Mandy has a Report Administrator role in the Corporate folder, but only a Report Consumer role in the *Business* folder. She cannot create or edit the properties of any report pack inside the *Business* folder. She is restricted to creating and editing report packs in the Corporate folder. As a Report Administrator, Mandy cannot see any jobs inside the Corporate folder.

User access does not stop at the folder level. Report packs and dashboards also have access privileges, so that a user can have access to a folder but be restricted from some of the items inside that folder. For example, if Mandy has access to a folder but No Access to the Corporate report pack in that folder, then she can't see the Corporate report pack. The following table provides some common tasks in folders and their suitable roles. The table contains the minimum role necessary for the task, but with each task you can always choose a higher user role and get the same results.

Task in folder	User role to apply
View report pack contents	Report Consumer
Create, modify, and run report packs (to update their content)	Report Administrator
Classify issues in report packs	Issue Manager
View dashboard contents	Report Consumer
Create, modify, and run dashboards (to update their content)	Issue Manager
Navigate through dashboards to report packs and reports	Assign users a Report Consumer role in a dashboard and give them access to each of the report packs that contribute to the dashboard.
Export report data	Report Consumer
Create jobs and run scans	Job Administrator

Adding users to AppScan Enterprise

Creating a user

Create a user and assign a user type to them. As a best practice, when you first create a new user you should give them a No Access user type until you finish configuring their folder permissions, and then change their user type to whatever

type you want them to have. This prevents new users from being able to access areas they shouldn't if they log in while you are still configuring their permissions.

Before you begin

Learn more about creating users: The user will inherit some properties from the Default User template. To change the Default User properties the user inherits, you must edit the user's properties. If a user type is listed as "Restricted", you cannot change it because that user type has additional administrative permissions that you don't have. You can only change user types that have your access permission level or lower. For example, if you have a Standard User type, you cannot change the Product Administrator user type.

About this task

User role: Product Administrator

Procedure

1. Go to **Administration** > **Users and Groups**, and click **Create**.
2. On the Create User page:
   a. Enter a **Name** for the user that is easy to recognize; for example, Bill Smith.
   b. Enter the **User ID** using the Domain/Username format; for example, workgroup\billsmith.

      Note: Do not use special characters, such as the percent sign (%). It might cause a 'session expired' error.
   c. Choose a **Type** for this user.
3. Click **Create** to add the user is added to the list of users.

Related concepts:

"User types" on page 121
Every user is assigned a User Type by the Product Administrator. The User Type applies across an instance.

Related tasks:

"Creating users with the Default User template"
Most of the properties that a typical user will need can be given to the "Default User" template, and then used automatically every time you create a new user.

Creating users with the Default User template

Most of the properties that a typical user will need can be given to the "Default User" template, and then used automatically every time you create a new user.

About this task

User role: Product administrator

Learn more about assigning access privileges: By default, the "Default User" user type is *QuickScan User*. For example, you might want most users to only be able to review reports and not perform any job or report pack configuration. You can give the "Default User" a Report Consumer role and choose which folders they are allowed to access. When new users log in for the first time, they will automatically assume the access permissions of the Default User template. The "Default User" is displayed in the list of users on the Administration tab > Users and Groups page. If a user type is listed as "Restricted", you cannot change it because that user type has additional administrative permissions that you don't have. You can only

change user types that have your access permission level or lower. For example, if you have a Standard User type, you cannot change the Administrator user type.

New users will inherit the license type of the Default User (floating or authorized user), which is set the first time the product instance is configured.

Procedure

1. Go to the Administration view.
2. On the Users and Groups page, select the **Default User** from the list.
3. On the Edit User page, make your changes, and click **Save**.

Results

New users appear in the list of users under their Windows networking User name and Full name. The only exception is if the Default User has been assigned a *No Access* user type. In this instance, the new user is denied access, and no new account is created.

Related reference:

"Product and user licenses" on page 28
This topic on AppScan Enterprise licenses opens a technote in a separate browser.

Importing users

You can import individual users and assign a user type to them.

About this task

User role: Product Administrator

Procedure

1. Go to **Administration** > **Users and Groups**.
2. Click **Import Users**.
3. Enter a domain to retrieve a list of users and select the users you want to import and select a user type for those new users.
4. Click **Import** after you have selected users from the list.

Importing LDAP user groups

You can import individual groups of users from an LDAP Server, and assign a user type to them. All groups must have a valid LDAP account before they can be imported.

Before you begin

After you import an LDAP group, users from that group will automatically be created as a user when they first log in, if the default user type is 'inherit'.

About this task

User role: Product Administrator

Procedure

1. Go to the Administration view.

2. (Windows only): On the General Settings page, click **Edit Enterprise Console Settings** and configure the *LDAP server or domain* and the *LDAP group query* fields and click **Done**.
3. On the Users and Groups page, click **Import Groups**.
4. Select an Import Type from the list, select the user groups, and click **Import**.
5. Select the Default User and set the access permissions to "Inherit Access", and click **Apply**.

   Note:

   a. When a user logs in for the first time, they will automatically be assigned the user permissions associated with the groups they belong to.
   b. Nested groups are not supported. If a user belongs to more than one LDAP group, they will inherit the permissions of the top level of the group hierarchy they belong to.

Results

When a user logs in to the Enterprise Console, they will inherit the permission that their group has. When you assign or change folder access privileges for the group, that user will have access to it if their group does. When a user creates a content scan job, the Enterprise Console will check their scanning permissions of the group they belong to.

Related concepts:

"How user types affect user groups"
Every user is assigned a User Type by the Product Administrator. The User Type applies across all folders in an installation.

How user types affect user groups

Every user is assigned a User Type by the Product Administrator. The User Type applies across all folders in an installation.

When a user from an LDAP group has an `Inherit Access' user type, that user always inherits the **maximum permissions** of any groups he belongs to. For example, in the following table, Rob belongs to three groups. His maximum permissions of all these groups allow him to create/edit and delete users, and configure test policies.

Group	User Type	Advanced View	Create/ Edit Users	Delete Users	Configure Server Groups	Configure Test Policies
All Staff	Standard User	Y	N	N	N	N
Security Analysts	Test Policy Administrator	Y	N	N	N	Y
Developers	User Administrator	Y	Y	Y	N	N
Maximum Permissions	N/A	Y	Y	Y	N	Y

Related tasks:

"Defining custom user types" on page 124
A user type is a set of permissions that are applied to a user so that they can perform certain administrative tasks. Before creating user accounts, you must create custom user types if you want to assign limited administrative tasks to Standard Users without making them full Product Administrators.

"Importing LDAP user groups" on page 130
You can import individual groups of users from an LDAP Server, and assign a user type to them. All groups must have a valid LDAP account before they can be imported.

Configuring and downloading log files for Enterprise Console and AppScan Server

Administrators can configure the settings for log files for the Enterprise Console and AppScan Server and download them when they need to troubleshoot issues. This function eliminates the need to search the file system of the computer where the Enterprise Console or AppScan Server is installed.

Procedure

1. On the Administration view, go to **General Settings** > **Log Settings** > **Edit**.
2. Select the **Enable logging** check box (off by default).
3. Select a log level and a log size for both types of log files, and click **Save**.

   Note: These settings affect the Enterprise Console and AppScan Server log files independently (the log file size is the maximum for each type of log file).
4. If you download the log files without modifying the log level and size settings, you download existing logs for Enterprise Console and AppScan Server that are already collected. The downloaded compressed file contains the Enterprise Console logs and a compressed file that contains the AppScan Server logs.

   Note:
   a. If you modify the log level or size settings, the settings affect future log files that you download.
   b. Existing log files are not deleted; new information is appended to them.

Monitoring AppScan Enterprise usage

Create an Activity Log report to determine who is using AppScan Enterprise and what they are doing with it. The report lists the users that made changes and when the changes were made. Because the log is always recording activity, all you must do is create the report. Only Administrators can create the Activity Log report; however, any user can be given access to it as part of a report pack's properties. If you do not want other users to see the Activity Log report, change `All Other Users' to *No Access* on the Users and Groups page for the report pack.

Procedure

1. Go to the Folder Content Summary and open an existing report pack or create a new one.
2. Select **Source Jobs** and select a job. It does not matter which job you select, but you must select a job before you can create the report pack.
3. Select **Reports** > **Add Admin Reports**.
4. Select the **Activity Log** report and click **Add**.

5. Click **Save** to save and close the report pack.
6. Run the report pack to update its data.

What to do next

Make sure you restrict access to the report pack or to its folder so other users cannot see the Activity Log.

Managing a server

Product Administrators are responsible for managing each server to its optimal performance.

About this task

User role: Product Administrator

Procedure

1. Go to the Agent Servers page of the Administration view.
2. Check the number and status of items (jobs, report packs, or dashboards) associated with each server: Use the Current® Items section to see the status of items and click the **Refresh** icon to refresh the item's status. You might have locked the server and you want to see if anything is running on it. You might need to discover which server a particular job is running on. There might be too many items running (jobs, report packs, or dashboards) and you believe more agent servers are needed to distribute the load.
3. Specify the maximum number of agents that can run concurrently on a server. Change the maximum number when you want to optimize the load on your server.
4. Lock or enable a server. Lock a server to prevent any more items from running on it, such as before disconnecting the server from the network, rebooting the server, or installing software on it.
   a. Identify the server to be taken out of service.
   b. Click the **Name** of the server.
   c. On the Server Properties page, click **Lock** or **Enable**.
   d. Click **Save**.

   Note: The number of jobs running can exceed the maximum number of agents assigned to the server because the number of jobs running includes jobs that are now in postprocessing. These jobs are no longer using an agent on the server.

Managing the scan queue

See the status of scan jobs currently running or waiting to run so that you can prioritize the order in which your key scan jobs run. For example, you might have scan jobs that are part of a time-sensitive deliverable, like a holiday shopping special. You can move them to the top of the queue to make sure that they are prioritized first in the schedule.

About this task

User role: Product Administrator.

Procedure

1. In the main Folder Explorer, click **Scan Queue Management**. The list of jobs that opens automatically sorts according to the scans in progress first, and then by those jobs that are waiting in the queue to run. The jobs that are in progress are sorted by run time.

   Note: The scan queue view is empty unless scan jobs are running or waiting to run.
2. To change the running order of the jobs that are waiting to run, select the job and pick an option from the menu:
   - Move job to top of queue
   - Move job to bottom of queue
   - Move job to position: <position number>
3. There might be times where you must remove the job from the queue, suspend the job, or stop it before it finishes running. You can remove the job from the queue only if it is waiting to run. For jobs that are running, select the job and choose one of the following options from the menu:

Method	Description	Can be resumed
Suspend	Suspends the job because it is in a continuous loop, has developed an error, or because you want to free the agent to run another job. A suspended job is stopped, the data collected is stored, and the associated agent becomes available to handle another job. You can End, Cancel or Run (resume from where it left off) a suspended job. However, the data gathered will not display in your reports. If you later resume the job successfully, then the stored data can be used in your reports.	Yes
Save current results and stop	Saves the current results and stops the job. The run will finish normally and save the data collected so far in the database, but the reports will be incomplete.	No
Discard results and stop	Discards any data collected during the run and stops the job.	No

4. Click **Return to Folder View** when you are done to get back to the main folder explorer.

Updating security rules

You must have the latest version of AppScan Enterprise (including Fixpacks and iFixes) to receive the latest security rules updates. You can verify the version and release date of the security rules by looking in the About link in the AppScan Enterprise main menu.

Procedure

Manually install the updates downloaded from the IBM Fix Central website.

Maintaining your SQL Server database

Upgrading from SQL Server 2005 to SQL Server 2012

AppScan Enterprise Server 9.0 no longer supports SQL Server 2005. Follow the steps below to upgrade to SQL Server 2012.

Procedure

1. Back up your database on SQL Server before continuing with the upgrade process.
2. Make sure you have the latest operating system requirements for SQL Server 2012.

   Note: For Windows Server 2008 operating system, Service Pack 2 or later is required. For Windows 7 or Windows Server 2008 R2, Service Pack 1 or later is required. For more information, see Hardware and Software Requirements for installing SQL Server 2012 at: https://go.microsoft.com/fwlink/?LinkID=195092
3. Follow the instructions at Upgrading to SQL Server 2012.

SQL Server database maintenance strategies

You can maintain data integrity and improve performance by considering the following items when you configure the database and log files.

1. Pre-allocating the space that is required for database files and log files can improve performance. These options are available on the Data Files tab and the Transaction Log tab of the Database Properties window in SQL Server Enterprise Manager.
2. Allowing the log files to grow automatically (by 10%) is required to ensure that unexpected errors do not occur.
3. Placing the data files and log files on separate physical disk drives can improve performance substantially. Make sure that these physical disk drives have enough free space to allow for database growth.

SQL server database backup and maintenance

Like any enterprise application, the database must be backed up regularly, and other database maintenance tasks must be conducted from time to time. Microsoft SQL Server Management Studio provides a Maintenance Plan wizard that allows these tasks to be automated. Use this wizard to create the required scheduled tasks.

Note: Backing up the database is different from copying the database file and saving it in another location. Use the Backup feature in Microsoft SQL Server Management Studio to back up the SQL Server database, and consult its documentation for instructions.

Ensure matching database and SQL server collation

When you upgrade to a newer AppScan Enterprise version or backup the database to move it to another SQL Server, ensure that the collation (such as case sensitivity) matches between the two. Otherwise, the AppScan Enterprise database won't work properly.

Backup strategy

Because the database log files can grow in size between SQL Server backups, back up the database daily. Depending on the frequency with which activities (such as report pack and dashboard generation, import jobs) are run, it might be possible to do incremental backups frequently and full SQL Server backups less frequently. It is not necessary to conduct backups while the database is quiet, but backup operations can be scheduled for times when the database is known to be less busy. If your organization employs a regular maintenance window for servers, then this time might be an ideal time to conduct the SQL Server backup.

For large organizations where the database is never, or rarely, quiet, consider using commercial backup software that is configured to back up SQL incrementally.

Database recovery

If there is a catastrophic hardware failure, the database can be restored from the last SQL Server backup by using the 'Restore database' command in Microsoft SQL Server Management Studio.

Shrinking the database

Database growth can become an issue, especially after large content scan jobs are deleted. The 'Shrink Database' command can be used to remove the empty space. The database is most effectively shrunk at the "File" level. Choose "Files" from the "Shrink Database" window.

Alternatively, use the Database Maintenance wizard to periodically shrink a database.

Database maintenance

After the application is installed, a database maintenance plan must be established. Use the 'Maintenance Plan wizard' to create the plan and schedule it. In the wizard, select these options:

- Check database integrity
- Shrink the database
- Reorganize the index
- Update statistics
- Do a full backup of the database

Disk defragmentation

Disk fragmentation occurs over time as files are created, deleted, and change in size. Consider using the Windows tools to periodically defragment disks when the database is not being used and can be taken down for maintenance.

Maintenance plan to reorganize the index

Index fragmentation can cause slow database performance because of many page splits. This leads to high post processing times, report packs taking longer to generate, and slower web application performance.

The rebuild operation cannot be run while users are accessing the database. For this reason, it is necessary to stop users from accessing the database during the rebuild.

Here are some possible solutions:

- For SQL Standard, a rebuild of the indexes is necessary, for this to occur the indexes must be taken offline.
- Upgrade to SQL Enterprise, allowing for index rebuilds while keeping the index online.
- Adjust the SQL server fill factor to try and reduce internal fragmentation from occurring in the first place.

Upgrading to SQL Enterprise would help administrators complete index rebuilds without stopping access to the database. Create a maintenance plan that:

1. Stops all services;
2. Stops IIS and related services;
3. Kills any running Agent Host executables;
4. Waits for all Agent Hosts to finish processing;
5. Checks the level of index fragmentation, and logs it to a file;
6. Rebuilds the indexes using a fill factor of 80 (20% free space per page);
7. Checks the level of index fragmentation again, and appends it to the log file;
8. Starts IIS and related services; and
9. Starts all services.

SQL server database usage

The database contains all administration, configuration, and reporting data. This database contains all the table definitions, indexes, constraints, and database stored procedures used by the application.

The application uses database tables in five ways:

1. To store data that is independent of a particular content scan job.

   These types of tables are named in mixed case with the name denoting the data that is stored in the table; for example: Job, UserInfo.
2. As a template for tables that are used to create tables that store data for a particular content scan job.

   These tables have the suffix **_JII_** or **_NSI_** or **_SJI_** appended to their names; for example: RepEntity_JII_, Vulnerability_JII_.
3. To store data for a particular content scan job iteration.

These tables are created (based on the corresponding template table's definition) the first time that the job is run. The table names consist of the template table name with the **_JII_** or **_NSI_** or _SJI_ suffix replaced by the job identifier and job iteration; for example: RepEntity_32_0, Vulnerability_32_1. The data stored in these tables is temporary.

4. To store aggregated data from individual scan jobs.

   The tablename**_JR** job in the reference table identifies the scan job that found the object.

5. To store default options for a particular content scan job.

   This is a single table, per folder item, that is created the first time the folder item is created. The table name is **FolderItemOption**, followed by the item identifier and the string **_D**; for example: FolderItemOption_310_D.

Similarly, there are three types of stored procedures:

1. Stored procedures that perform operations that are independent of any particular content scan job.

   The names of these stored procedures being with the prefix **wp**_ and are named according to the operation that they perform; for example: wp_FolderItem_Delete, wp_Folder_Select.

2. Template stored procedures that are used to create stored procedures that perform an operation on the data for a particular content scan job.

   The names of these stored procedures begin with the prefix wt_; for example: wt_RepEntityInsert, wt_VulnerabilityInsert.

3. Stored procedures that perform operations on the data for a particular job iteration.

   These stored procedures are created from the template stored procedures the first time an item is run. The name of the stored procedure begins with the prefix **wi**_, followed by the item identifier, item iteration, and operation name; for example: wi_21_0_RepEntityInsert, wi_21_1_VulnerabilityInsert.

Referential integrity in the application is performed at the database level. All foreign key constraints are defined in the database.

Creating a wizard user account to run stored procedures

If granting db_owner rights to the service account contravenes your organization's security policies, you can create a role to run stored procedures.

Procedure

1. In SQL Server Management Studio, click **New Query** and select the database in the list.
2. Enter these two SQL statements:
   a. Create role db_executor
   b. Grant execute to db_executor
3. Click **Execute**.
4. Go to **Databases** > **asedatabasename** > **Security** > **Users**.
5. Right-click **Service account** > **Properties**.
6. From the Database Role Membership section of the Database User dialog, add these roles to the service account:
   - db_datareader
   - db_datawriter

- db_ddladmin
- db_executor

7. Select **OK**.

Related reference:

"Required user account information during installation and configuration" on page 22

During installation and configuration, various user accounts are used, each with specific permissions. The Service Account and the Local System User account can be a single account, with the same user name and password. However, if your organization requires a separation of duties, use the Local System User Account during installation and configuration, and then use the Service Account for maintaining SQL Server database access.

Preparing for security testing

Creating a server group

A server group is a group of items that can be tested as a unit; the same security tests will be applied to all the servers in the group. A server group can be any combination of domains and IP addresses.

About this task

User role: Product Administrator

Important: Changes as of 8.8.0.1

Server groups do not include URLs anymore.

Learn more about server groups:

You must create one or more server groups to define what can be tested. After a server group is created, you then assign it to a Job Administrator. That person then creates jobs that perform security tests on a specific group of servers.

For any given server you can enter its domain or IP address, but you do not need to enter all. Assume you want to scan all the servers within your building in Houston together. Because you know their IP addresses include 14.1.1.2 through 14.1.1.20, you only need to enter the IP address range; you do not need to enter each specific domain.

Note: If you added an open IP range (0.0.0.0 - 255.255.255.255) in the Module Licenses page so that AppScan Enterprise can scan unresolvable domains, make sure that the domain name is included in a server group. Add users to that specific server group so that they can send security tests to that domain. This gives you more flexibility when you assign user permissions for scanning.

The Default User can be assigned server groups and test policies to facilitate setting up users. If you know that all your users will be testing a particular set of servers, you can create a group with those servers and assign it to the Default User. All newly created users will be automatically given permission to test that server.

Procedure

1. Go to the Administration view.
2. On the Server Groups page, click **Create**.
3. On the Create Server Group page, enter a name for the server group and click **Create**.
4. On the Edit Server Group page, enter the domains or IP addresses of the servers that are included in this server group and click **Save**.
5. Next you will create a security test policy and assign the server group and security test policy to users.

Enabling and disabling IP addresses to scan

If you want to enable or disable your address ranges (which will affect the entire installation), you can do so. You might disable a range of addresses if you had servers that were in the process of being backed up. In this case, you can prevent anyone from running security tests on the servers by disabling the IP address range of the servers. Another method of restricting IP address testing is at the user level through the application of server groups.

About this task

Important: Changes as of 8.8.0.1

To configure AppScan Enterprise to scan specific unresolvable domains, add an open IP range (0.0.0.0 - 255.255.255.255) on the Module License page. On the Server Groups page, add the name of the specific domain or domain pattern to a server group, and add users to that server group so that they can send security tests to that domain. This gives you more flexibility when you assign user permissions for scanning.

Note: Your IP address changes will also affect AppScan if it uses AppScan Enterprise Server as its permissions server.

Procedure

1. Go to the Administration view and navigate to the Module Licenses page.
2. In the *Security IP Ranges* section, select the ranges you want to enable or clear the ranges you want to disable.

Creating and importing security test policies

Security test policies

A security test policy is a predefined set of security tests. Users must be assigned both a server group and a test policy before they can perform security scans.

Administrators do not need to be granted explicit access to a test policy, nor do they need to be assigned to a server group. There are two types of test policies available:

- A *Simple security test policy* defines tests at a high level. You can create and edit simple test policies in AppScan Enterprise Server and assign them to server groups.
- An *Advanced security test policy* defines tests at a more granular level. You can import advanced test policies from AppScan 7.7 (or higher) and assign them to server groups, but you cannot edit their properties:

- **Application only**: Includes all application level tests except invasive and port listener tests.
- **Complete**: Includes all AppScan tests.
- **Default**: Includes all tests except invasive and port listener tests.
- **Developer Essentials**: Includes a selection of application tests that have a high probability of success. This can be useful for evaluating a site when time is limited.
- **Infrastructure only**: Includes all infrastructure level tests except invasive and port listener tests.
- **Invasive**: Includes all invasive tests (tests which might affect the server's stability).
- **The Vital Few**: Includes a selection of tests that have a high probability of success. This can be useful for evaluating a site when time is limited.
- **Web Services**: Includes all SOAP related tests except invasive and port listener tests.
- **WebSphere Portal**: Includes a selection of tests that have a high probability of success on WebSphere Portal.

Creating a simple security test policy

The Simple security test policy is the default test policy. It defines tests at a high level. You can create and edit simple test policies and assign them to server groups. Then you can assign server group/test policy combinations to users to use during security scanning.

Procedure

1. Go to the Administration view.
2. On the Security Test Policies page, click **Create**.
3. On the Create Simple Security Test Policy page, give the test policy a name and description and click **Create**.
4. On the Edit Simple Security Test Policy page, configure the tests that will be included in the test policy and click **Save**.

What to do next

Assign the test policy to one or more users.

Importing an advanced security test policy from AppScan Standard

Use Advanced security test policies to test down to the variant level of a vulnerability, giving you complete control over the test sent during a scan. You can import advanced security test policies from AppScan Standard Edition 7.5 (or higher) and assign them to server groups.

About this task

These test policies are exported from AppScan 7.5 (or higher) and are read-only. Any required modifications to the test policy must be performed in AppScan and re-imported.

Procedure

1. Go the Administration view.
2. On the Security Test Policies page, click **Import Advanced Security Test Policy**.

3. On the Import Advanced Security Test Policy page, give the policy a name.
4. Enter the location of the .policy file and click **Import**.

   Note: If you do not know the location of the .policy file, click **Browse** to locate it on your file system and then click **Import**. The Edit Advanced Test Policy page opens where you can view a read-only version of the tests the test policy contains.
5. On the Edit Advanced Security Test Policy page, edit the name and description of the test policy as required and click **Save**.
6. Verify that you have imported the correct test policy by checking its details.

What to do next

Assign the security test policy to one or more users.

Re-importing advanced security test policies

For those times when you must re-import a security test policy file from AppScan Standard, you can re-import it without affecting your workflow.

About this task

There might be times when you must re-import a security test policy file, including:

- you've assigned the test policy to users who are currently using it on scan jobs
- test policy rule versions have updated in AppScan Standard and you would like to use them in AppScan Enterprise

To avoid having to reassign security permissions on the test policy, and to avoid affecting jobs that are currently using the security test policy, you can re-import it from AppScan without affecting your workflow. Otherwise, you must delete the test policy in AppScan Enterprise and create a new one, compromising any job that references the deleted policy.

1. Apply updates in AppScan Standard and then close AppScan Standard.
2. Reopen AppScan and export the test policy as a .policy file.
3. Re-import the security test policy into AppScan Enterprise.

Defining the servers to test and the security tests to perform

Job Administrators are assigned security test policies and server groups by a Product Administrator. Security test policies define what tests they can perform; server groups define which applications/servers they can run those tests against.

Before you begin

Learn more:

- The test policies that are available depend on what the Product Administrator has assigned to you.
- Each test policy is associated with a certain server group, so changing the test policy changes the server group.

About this task

Your user properties list the security test policies and server groups that have been assigned to you. When a Job Administrator creates a job, its security test policies and server groups are predetermined. However, other Job Administrators can

change what tests the job can run and which applications it can test. Any other Job Administrator can "take ownership" of the job. When a Job Administrator takes ownership of a job, the available security test policies and server groups become those of the new Job Administrator.

Procedure

1. Go to the Folder Content Summary, select the job, and click **Edit**.
2. On the General Properties page, click **Select Job Owner**, and choose yourself as the new job owner.
3. Click **Select Job Owner** > **Save**.

What to do next

"Assigning security test policies and server groups to users"

Assigning security test policies and server groups to users

After you have created your server groups (what you want to test) and your security test policies (what tests you want to perform), you must assign them to users. Users can only run security tests on the server groups that you assign to them. If they do not have any test policies assigned to them, they cannot perform security scans.

About this task

Each user can be assigned certain security test policies and server groups. However, if you want all new users to automatically have the same test policies and server groups, assign them to the Default User instead.

To assign security test policies and server groups to users:

1. Go to the Administration view.
2. On the Users and Groups page, select a user from the list of existing users or select the Default User, and click **Edit**.
3. In the Security Scan Permissions section of the Edit User page, select a test policy and a corresponding server group, and click **Add**.
4. Add additional combinations of test policies and server groups to the **Currently Assigned Security Test Policies and Server Groups** list, and click **Save**.

Creating scan templates

Overview of scan configuration differences in v9.0.2 and previous versions

Version 9.0.2 offers a new approach to create scans consistent with AppScan Standard, for both the security team who creates the templates and for the developers who create the scans.

The security team (whose members have Administrator privileges) creates templates by using scan configuration that they author in AppScan Standard. The scan template file is then available for use in AppScan Enterprise. Developers (with QuickScan user privileges) pick up the template when they create a scan, and use a wizard in the new AppScan Dynamic Analysis Client to finish the scan creation. They use the same Client when they need to amend the scan configuration.

This workflow provides many benefits: The security team uses a richer environment to select scan options in AppScan Standard. This method is a one-step process to provide these templates to developers in AppScan Enterprise. It produces more consistent results across the organization, and provides the same user experience during job configuration. It improves the configuration experience for developers, who often don't have much security knowledge, and provides them with the ability to configure action-based login and manual explore features.

There are some upgrade considerations to know about:

- The new method is accessed from both the Monitor and Scans views.
- Existing scan templates from v9.0.1.1 are kept after upgrade, and the old method of QuickScan template creation still exists. To take advantage of this new method, during upgrade you must run the Default Settings Wizard after the Configuration Wizard to install the templates for v9.0.2.
- To avoid any template name conflicts in the Templates directory in the Folder Explorer, (v9.0.2) is appended to the template name. If you install a new instance of AppScan Enterprise, you can still access the templates from v9.0.1.1. When you create a new content scan or template from the Scans view, select **Create using previously saved settings file** and go to `<install-dir>\AppScan Enterprise\Initializations\ASE\DefaultTemplates\Job\Version 9.0.1.1` to select the *.xml file.

Creating a QuickScan template using scan properties from AppScan Standard

Starting in v9.0.2, the security team can create a scan template based on scan configuration options in AppScan Standard. Developers modify these templates in the AppScan Dynamic Analysis Client to create scans. The AppScan Dynamic Analysis Client uses the same scan configuration options that are used in AppScan Standard, including action-based login and manual explore.

About this task

User role: Product Administrator

This task assumes that you have created a scan template file in AppScan Standard.

Procedure

1. In the Scans view, go to the Templates folder in the Folder list and click **Create** in the main content pane.
2. On the Create Folder Item page, select **Create Template for Content Scan** and give it a name.
3. Select **Create using properties from AppScan Standard scan template file (.scant file)** as the Method of Creation and **browse** to the file location of the *.scant file.

   Note: If you do not have a copy of AppScan Standard, click **Download**. After you install it and create a *.scant file, then you can upload it here.
4. Add the *.scant file that you located and click **Create** > **Done**.

   Note: If there are any issues during the upload process, they display in the Folder Item Created page as not supported.

5. Security test policies are ignored during upload. On the template's Security page, select a test policy. Or, to let developers pick their own security test policy, choose **Use the AppScan Dynamic Analysis Client to select**. Users can select their own policy when they create a scan in the Client.
6. Configure the remaining options for the template, such as Log Settings, Agent Server, Job Properties, and What to Scan.
7. To prevent users from accessing the advanced scan configuration pages, disable the check box on the Template Configuration page.
8. Click **Save**.

Chapter 5. Reference

License Server

Specify the Rational License Server to use for licenses.

1. If you installed a local license server during installation, <localhost> will be pre-populated in the field.
2. If you are using a single license server and a port in the default port range (27000-27009), enter the license server name in the License server box. Otherwise, click the **Advanced** button to display the advanced license server view.
3. In the advanced license server view, enter the license server name in the Server box. If you are using redundant license servers, you can enter up to three redundant server names, separated by a comma (for example, server1,server2,server3).

   Note:

   - The port number is not needed if the license server(s) in the Server box are using a port in the default port range. Otherwise, enter the port number used by the license server(s).
   - Licenses are searched for on the license servers in the order in which they appear in the 'License server search order' list.
   - The license servers you choose during configuration apply to all instances configured on this Server.

Product and user licenses

This topic on AppScan Enterprise licenses opens a technote in a separate browser.

Read this technote: Licensing for AppScan Enterprise.

Server Components

Select the components you want to configure. The components available to you depend on the license.

Table 17. Server Components

Component	Description
User Administration	User administration for LDAP authentication.
Enterprise Console	Enterprise reporting, collaboration, and the ability to conduct dynamic analysis assessments. Select this component for AppScan Enterprise and for AppScan Source distributed deployments that only require Windows authentication.
Dynamic Analysis Scanner	Scanning and testing web applications. Select this component for an AppScan Enterprise deployment.

Instance Name

Specify the name of the instance you want to configure.

1. If you are installing only one instance on this computer, select the **Select or create a default instance** check box and then click **Next**.
2. If you are installing more than one instance on this computer, clear the **Select or create a default instance** check box, enter a name for the instance, and then click **Next**. You will be given the option to configure another instance at the end of the wizard.

Related tasks:

"Uninstalling an instance of the Enterprise Console" on page 100
Remove instances that are no longer needed on a single server.

Database Connection

Enter the SQL Server name, port number, and the name of the database you are connecting to. You can click **Test Connection** to make sure you can connect to the SQL Server. The configuration wizard does not proceed until the connection is successful.

Note:

1. The syntax for the SQL Server name has changed with the introduction of Liberty support. *".\SQL_SERVER_NAME"* no longer works. Use *"HOSTNAME\SQL_SERVER_NAME"* instead.
2. If your environment uses a named SQL Server instance for the AppScan Enterprise database or SQL Server Express, make sure that TCP/IP is enabled in the SQL Server configuration manager, and restart the SQL services for SQL Server. Use the port number of the named SQL Server instance instead of the default port number (1443).
3. If you have multiple instances and want to remove an instance that is no longer required:
   - Clear the **Use default name** check box.
   - Select the name of the relevant instance, click **Remove**, confirm the removal when prompted, and finish the wizard.

Database encryption changes

AppScan Enterprise no longer uses proprietary encryption mechanisms to prevent unauthorized transfers of its database because there are other third-party mechanisms that are designed to specifically perform physical layer encryption with less impact on performance. This type of encryption is usually applied at the database server level; for example, SQL Server Enterprise Edition has a built-in encryption TDE mechanism (Transparent Data Encryption). TDE encrypts the data residing in the database or in backups on physical media. SQL Server Standard Edition uses Windows Encrypting File System.

Related concepts:

"Data protection through encryption" on page 85
Data that is stored on a physical media can be a target of unauthorized access attack. The physical media might be stolen, or the data might be accessed remotely. While you can use physical and computer security methods to protect your data from these types of attacks, encrypting the data offers more protection by preventing an attacker from reading the stolen files.

Related tasks:

"Enabling Transparent Data Encryption on SQL Server databases" on page 86
SQL Server has a built-in encryption TDE mechanism (Transparent Data Encryption) encrypts the data residing in the database or in backups on physical media.

"Encrypting, backing up, and restoring a SQL Server database with EFS" on page 89
The Encrypting File System (EFS) is a feature of Microsoft Windows that lets you store information on your hard disk in an encrypted format. EFS enables transparent encryption and decryption of files by using advanced, standard cryptographic algorithms. Use this method to encrypt the database file if you have SQL Server Standard Edition 2008, 2008 SP3, 2008 R2 SP2, 2012, and 2014.

Service Account

Specify the service account that will be used by the services.

During the configuration of the components you install, you must enter service account information. This service account allows the agents to access the database server. Individual users do not require any form of database permissions. The service accounts used for the agents and the database should have passwords that do not expire. If, however, the passwords must change at regular intervals, you can rerun the Configuration wizard on all the AppScan Enterprise Server and Dynamic Analysis Scanner computers and enter the new password.

The Local System User account and the Service Account can be a single account, with the same user name and password.

The service account is granted db_owner rights to the database and must have permissions that allow it to create a database and tables, add users, run stored procedures, and grant rights.

If granting db_owner rights to the service account contravenes your organization's security policies, you can create a role to run stored procedures. See "Creating a wizard user account to run stored procedures" on page 138.

With a SQL Server database, you can use a single service account or multiple service accounts, depending on how you decide to install.

File and folder permissions

The service account must have the following permissions on `Drive:\\YourInstallFolder\IBM\product name\` and all of its subfolders:

- Read and Execute
- Write
- Delete
- Delete files and subfolders
- Create files and subfolders

Note: These permissions enable the service account to write to the log files. They also enable the scan agents to write temp files, without which the scans would not function. The Configuration wizard creates these permissions for you - do not change them.

Local security policies

The service account must have permission to log on locally on the target machine so that it can impersonate the user's logon credentials. It also must have permission to log on as a service.

Registry permissions

The service account must have the following permissions:

- Read and Execute
- Write
- Delete

Related reference:

"Required user account information during installation and configuration" on page 22

During installation and configuration, various user accounts are used, each with specific permissions. The Service Account and the Local System User account can be a single account, with the same user name and password. However, if your organization requires a separation of duties, use the Local System User Account during installation and configuration, and then use the Service Account for maintaining SQL Server database access.

Server Certificate

For security reasons, HTTPS is enabled for Enterprise Console. Choose a certificate from the list of certificates that are installed in IIS. Taking these actions will help you deploy a secure AppScan Enterprise in your environment.

Server Keystore

If you choose to use a keystore that contains a trusted certificate chain for this host, complete the available fields.

- If you exported a certificate .pfx file, select **Public key cryptography standards #12 (PKCS #12)** as the Keystore Type.
- Browse to the location where you exported the certificate .pfx file.
- Enter the keystore password that you created when you exported the .pfx file.

Authentication Mechanism

Select an **Authentication Mechanism** to use to log into the Enterprise Console. If you choose Windows, you must be part of a domain.

LDAP authentication

If your LDAP server supports SSL, select the **Connect to LDAP server using SSL** check box. Some of the LDAP configuration fields are pre-populated for you. Check that they are correct for your environment.

When you select an **LDAP Server Type**, default settings for the **LDAP Server Port**, **User Filter**, and **User ID Map** fields are automatically filled in for you. However, you must understand the syntax required for each field so that the connection to Liberty works successfully. Contact your LDAP administrator to get the settings for your environment, especially for filtering users.

Related information:

Configuring a basic user registry for the Liberty profile

Configuring LDAP user registries with the Liberty profile

Product Administrator

This user is licensed separately; if you want to reassign the Product Administrator license, you must rerun the configuration wizard.

- For Windows authentication, provide your user name and full name.
- For LDAP authentication, provide your User ID, name and password.

Server Group Changes

A server group is a group of items that can be tested as a unit; the same security tests will be applied to all the servers in the group. A server group can be any combination of domains and IP addresses. You must create one or more server groups to define what can be tested. Once a server group is created, you then assign it to a Job Administrator. That person then creates jobs that perform security tests on a specific group of servers. As of version 9.0, Server Groups are no longer defined by URL. Any existing URL definitions are removed from existing Server Groups and listed in the WFCfigWiz.log.

Index

T

U

W