

AppDetectivePro™

AppDetectivePro 7.3 User Guide

Last Modified February 2, 2011

Application Security, Inc.
www.AppSecInc.com
info@appsecinc.com
1-866-9APPSEC

Contents

AppDetectivePro Basics 5

- What is AppDetectivePro? 5
- Viewing Your Version of AppDetectivePro 6
- Minimum System Requirements 6
- AppDetectivePro Tasks 13
- Customer Support 15

Licensing 16

- What is the License File? 16
- Licensing FAQ 16

Installation 19

- Installing and Configuring AppDetectivePro and SHATTER Knowledgebase Components 19

Getting Started 42

- Understanding the AppDetectivePro Graphical User Interface (GUI) 42
- Navigating the Toolbar 43
- Navigating Page Views 44
- Navigating Menus 46

Administration and Maintenance 51

Performing an ASAP Update 51

Uninstalling AppDetectivePro (and the Database and SHATTER Knowledgebase Components), and Deleting the AppDetectivePro Back-End Database 56

AppDetectivePro Tasks 57

Sessions 57

Discovery 66

Policies 76

Pen Tests, Audits, and User Rights Reviews 102

Interviews, Questionnaires, and Work Plans 137

Reports 191

Edit and Tools Menu Tasks 219

Job Scheduler 235

Vulnerability Manager 246

User-Defined Checks 252

Fix Scripts 266

Viewing SCAP Information 268

Appendices 270

Appendix A: Command Line Reference 271

Appendix B: Viewing Check Descriptions 293

Appendix C: Troubleshooting 294

Appendix D: Using Default and Custom Dictionaries 297

Appendix E: Using NMAP 302

Appendix F: Clearing Sybase Application Logs 307

Appendix G: Audit and User Rights Review Privileges 307

Appendix H: Using Microsoft SQL Server with AppDetectivePro 361

Appendix I: Enabling SSL Encryption on AppDetectivePro 363

Appendix J: Default Ports 364

Appendix K: Fix Scripts (Detail) 366

Appendix L: Check Point Logging Properties Installation 407

Appendix M: Customizing Reports with Your Company Logo 413

Appendix N: Integrating a Custom Dictionary to Uncover Easily-Guessed Passwords 414

Appendix O: Oracle Critical Patch Update Detection 418

Appendix P: Migrating Your Back-End Database 423

Appendix Q: Understanding System Auditing 424

Appendix R: Updating Your Back-End Database from Microsoft SQL Server 2000 to Microsoft SQL Server 2005 or Microsoft SQL Server 2008 426

Appendix S: Dynamic Shell Prompt Handling 428

Appendix T: AppDetectivePro Application Log Files and Installation/Upgrade Log Files 429

Appendix U: Open Ports (on Computers Running Microsoft SQL Server) Required to Run Discoveries, Pen Tests, and Audits 432

Appendix V: Uploading Comma-Delimited Text Files, CSV Files, or NMAP Files Containing IP Addresses (or IP Addresses and Ports) to Discover 433

This section consists of the following topics:

- [What is AppDetectivePro?](#)
- [Viewing Your Version of AppDetectivePro](#)
- [Minimum System Requirements](#)
- [AppDetectivePro Tasks](#)
- [Customer Support](#)

What is AppDetectivePro?

AppDetectivePro™ is a network-based vulnerability assessment tool that rates the security strength of applications within your network. Armed with a revolutionary security methodology, together with an extensive knowledge base of application vulnerabilities, AppDetectivePro locates, examines, reports, and helps you fix security holes and mis-configurations.

AppDetectivePro helps you identify vulnerable applications residing upon your network, defines security holes on the applications, then helps you fix them. It has features designed to help you secure your applications, including:

- application detection and Pen Testing methodology/tactics
- non-intrusive application Denial of Service attack simulations and in-depth "agent-less" Audits
- automated inventory, information gathering, and analysis features
- reporting facilities to communicate application vulnerabilities and security holes for yourself, colleagues, and others up, down, and across your organization
- complimentary and compatible to existing security solutions
- an extensive and continuously updated library of vulnerabilities and misconfigurations.

After identifying all specified applications residing upon your network via performing a Discovery, you can Pen Test or Audit your applications for security holes. All Pen Tests are associated with Policies. You can add new Policies designed to reflect the level of security appropriate for your corporate network. Once you have

performed a Discovery and Pen Tests, the [Report Wizard](#) allows you to report your results in a formatted layout. (You can include your company name and logo.)

Viewing Your Version of AppDetectivePro

To view your version of AppDetectivePro, Choose [Help > About AppDetectivePro](#). The [About AppDetectivePro](#) pop-up shows your version information.

Minimum System Requirements

This topic consists of the following sub-topics:

- [AppDetectivePro Client Requirements](#)
- [Additional Requirements](#)
- [Supported Platforms](#)

AppDetectivePro Client Requirements

The following table lists AppDetectivePro client requirements:

System Requirement	Minimum
Operating System	<ul style="list-style-type: none"> • Microsoft Windows XP Professional SP2 or greater • Microsoft Windows Server 2003 Standard Edition • Microsoft Windows Server 2003 Enterprise Edition • Microsoft Windows Server 2003 Enterprise x64 • Microsoft Windows 7 • Microsoft Vista <p>To install (or ASAP Update to) AppDetectivePro 5.4.0 or greater on Microsoft Windows Server 2003 Enterprise x64, you must install Microsoft.NET Framework Version 2.0 (x64).</p> <p>WinPcap is only required if a non-administrative user will be using AppDetectivePro or if you are installing AppDetectivePro on Windows Vista. In the latter case, WinPcap is required even if the user belongs to the Administrators group, because the User Access Control—the security concept introduced in Windows Vista—requires the privileges to be explicitly elevated.</p>
Browser	Internet Explorer 6 or higher.
Rights	To install AppDetectivePro, perform an ASAP Update, and run a Discovery, you must have Administrative privileges on Windows.
Processor	750 MHz or 1 GHz processor.
RAM	512 MB (1 GB recommended).
Hard Drive	AppDetectivePro requires a minimum 200 MB of free disk space, with additional space required to store vulnerability information.
Program Files drive	AppDetectivePro requires 402MB of available space on the Program Files drive.
Networking	Network connection to the application.

System Requirement	Minimum
Back-End Database	<ul style="list-style-type: none">• Microsoft SQL Server 2000 SP4• Microsoft SQL Server 2005• Microsoft SQL Server 2005 Express Edition• Microsoft SQL Server 2008• Microsoft SQL Server 2008 Express Edition <p>For more information, see Appendix H: Using Microsoft SQL Server with AppDetectivePro.</p> <p>Microsoft SQL Server Desktop Engine 2000 SP4 (MSDE) supports a database size up to 2 GB. Microsoft SQL Server 2005 and 2008 Express Edition support a database size up to 4 GB. If your back-end database grows beyond these limits, clean out old data, or upgrade your to full version of Microsoft SQL Server. You can download MSDE 2000 SP4 from the Microsoft website for free at http://www.asp.net/msde/default.aspx. If you want to update your back-end database from Microsoft SQL Server 2000 to Microsoft SQL Server 2005 or Microsoft SQL Server 2008, see Appendix R: Updating Your Back-End Database from Microsoft SQL Server 2000 to Microsoft SQL Server 2005 or Microsoft SQL Server 2008.</p>

System Requirement	Minimum
Prerequisite Components	<p>When you install AppDetectivePro, the installer checks for the following prerequisite components.</p> <ul style="list-style-type: none">• Microsoft XML Core Services 4.0 SP2• Microsoft .NET Framework 2.0 SP1 (x86). Note that x86 will read x64 if you are installing AppDetectivePro on a 64-bit host machine.• Microsoft Visual Studio 2005 C++ Redistributable (x86)• SQL Server 2005 Backwards Compatibility (x86)• Backend Installer Component• Database Component• WinPcap. Note that WinPcap is only required if a non-admin user is going to use AppDetectivePro or if you are installing AppDetectivePro on Windows Vista. In the latter case, WinPcap is required even if the user belongs to the Administrators group because the UAC (User Access Control), the security concept introduced in Windows Vista, requires the privileges to be explicitly elevated. <p>If any of these prerequisite components are missing, the AppDetectivePro installer automatically installs them. For more information, see Installing and Configuring AppDetectivePro and SHATTER Knowledgebase Components.</p>

Additional Requirements

- **Microsoft .NET Framework Requirement on Microsoft Windows Server 2003 Enterprise x64.** If you want to install (or ASAP Update to) AppDetectivePro 5.4.0 or greater on Microsoft Windows Server 2003 Enterprise x64, you **must** install Microsoft .NET Framework Version 2.0 (x64).

In order to run AppDetectivePro, you must have the permission Full Control on the following items:

- The directory to which you installed AppDetectivePro.
- The registry key [HKEY_LOCAL_MACHINE\SOFTWARE\ODBC](#) and all sub-keys underneath.

Supported Platforms

The following table lists AppDetectivePro supported platforms.

Review [Appendix O: Oracle Critical Patch Update Detection](#) for a listing of all OS-specific, required Audit privileges.

Platform	Minimum
AppDetectivePro for Oracle Target Database Servers	<p>Oracle 11gR2, Oracle 11gR1, Oracle 10g, Oracle9i, and Oracle8i.</p> <p>You can perform User Rights Reviews against Discovered Oracle 8i-11g databases. For more information, see Pen Tests, Audits, and User Rights Reviews.</p> <p>Application Security, Inc. recommends that you disable <code>TCP.VALIDNODE_CHECKING</code> in order to Audit an Oracle target database. However, if you Audit an Oracle 10gR2 target with <code>TCP.VALIDNODE_CHECKING</code> enabled, and include the AppDetective host's IP address in the <code>TCP.INVITED_NODES</code> list, the Audit will work. Oracle reference: http://download.oracle.com/docs/cd/B19306_01/network.102/b14213/sqlnet.htm.</p>
AppDetectivePro for Microsoft SQL Server Target Database Servers	<p>Microsoft SQL Server Versions 2000, 2005, 2005 Express Edition, and 2008. MSDE 2000 SP4. Note that you can perform User Rights Reviews against Discovered Microsoft SQL Server 2000, Microsoft SQL Server 2005, and Microsoft SQL Server 2008 databases. For more information, see Pen Tests, Audits, and User Rights Reviews. In order to run a Discovery, Pen Test, or Audit against a Microsoft SQL Server database, certain ports on the machine running Microsoft SQL Server must be open. For more information, see Appendix U: Open Ports (on Computers Running Microsoft SQL Server) Required to Run Discoveries, Pen Tests, and Audits.</p>

Platform	Minimum
AppDetectivePro for Lotus Domino Target Servers	<p>Lotus Domino 6.0, 6.5, 7.0, 8.0, and 8.5. Note that AppDetectivePro performs Audits (but not Pen Tests) against Domino Groupware (Notes). AppDetectivePro performs Pen Tests (but not Audits) against Domino Web.</p> <p>In order to run AppDetectivePro's Lotus Domino features, you must have the Lotus Notes Client installed on your system. AppDetectivePro needs a valid <code>.id</code> file and password to function properly. If you are already a Lotus Notes user, you do not need to reload your Lotus Notes client. For more information, see Lotus Notes Client Driver Installation.</p>

Platform	Minimum
AppDetectivePro for Sybase Target Dataservers	<p>Sybase 11.9.2, 12.0, 12.5, 12.5.4, 15, and 15.5.</p> <p>An issue exists with the Sybase Adaptive Server Enterprise 15.x ODBC driver that results in an AppDetectivePro connection failure when a Sybase 15.0.2/3 ODBC driver is installed. This is a known issue with the Sybase ODBC driver, and not with AppDetectivePro. The current suggested solutions for this issue are to:</p> <ul style="list-style-type: none"> • use an older Sybase ODBC driver, even if you have Sybase 15.x installed (Sybase 15, for example) • use the new Sybase ASE ODBC driver 15.05.0000.1016, or newer <p>For more information on Sybase ODBC client driver installation, see Sybase Client/Client Driver/.NET Driver Installation. To run AppDetectivePro for Sybase Target Dataservers, you must have Full Control on the registry key:</p> <p><code>HKEY_LOCAL_MACHINE\SYBASE\Setup</code></p> <p>If you are using ODBC driver versions less than 3.7, you must also have read/write permissions on the following local system files on the client machine: <code>\${SYBASE_ROOT}\ini\sql.ini</code></p> <p>To run an Audit on a Sybase/Adaptive Server Enterprise, your workstation requires the appropriate client drivers installed. For more information, see Sybase Client/Client Driver/.NET Driver Installation.</p> <p>To Audit a Sybase ASE dataserver, you must have the Sybase ASE ODBC driver, the Sybase client, and a client-appropriate ADO.NET driver installed on your workstation. You must also copy some files to the [Common Files] folder so AppDetectivePro can retrieve them. In all cases, the .NET Framework 1.1 must be installed in order for the driver to work; for more information, see Sybase Client/Client Driver/.NET Driver Installation.</p>

Platform	Minimum
AppDetectivePro for IBM DB2 (LUW) Target Servers	IBM DB2 Version 8.1, IBM DB2 Version 8.2, IBM DB2 Version 9.1, and IBM DB2 Version 9.5. To run an Audit on IBM DB2, your workstation requires the appropriate client drivers installed. For more information, see IBM DB2 Client Driver Installation .
AppDetectivePro for MySQL Target Servers	MySQL 4.0, 4.1, 5.0, and 5.1. To run an Audit on MySQL, your workstation requires the appropriate MySQL ODBC driver installed. For more information, see MySQL Client Driver Installation .
AppDetectivePro for IBM DB2 Z Series Target Database Servers	IBM DB2 Version 8 and 9 (z/OS and OS/390). To run an Audit on IBM DB2 Z Series, you must install IBM DB2 Connect software on your scanning machine.

AppDetectivePro Tasks

This topic describes the tasks you can perform with AppDetectivePro.

- **Session.** Specifies the types of applications and range of ports on your network that you want to Pen Test and Audit. The Session is a prerequisite for most AppDetectivePro tasks. For more information, see [Sessions](#).
- **Discovery.** Locates network applications (and identifies their IP addresses), as well as the ports used to provide network services. You can run Pen Tests and Audits against discovered applications and ports. For more information, see [Discovery](#).
- **Policy.** Sets of security checks used when AppDetectivePro performs Pen Tests and Audits. AppDetectivePro contains several built-in Pen Test and Audit Policies. You can also create new Policies, modify Policies, and more. For more information, see [Policies](#).

- **Pen Tests, Audits, and User Rights Review.** Run from an “outside-in” perspective, **Pen Tests** assess the security of your applications by running security checks (based on a Policy you choose). Pen Tests give a good simulation of what a hacker or intruder might try in order to get past your application defenses, and commonly uncover mis-configuration errors in addition to well-known application vulnerabilities. An **Audit** tests the security of your application using an “inside out” approach. Audits require that you already have access to a system, such as Oracle. The Audit checks your Discovered applications for password configurations, table access, user roles, and other vulnerabilities. **User Rights Reviews** are supported for Discovered Oracle 8i-11g, Microsoft SQL Server 2000, Microsoft SQL Server 2005, and Microsoft SQL Server 2008 databases. A User Rights review is a comprehensive “inside-out” scan of users, roles, and their privileges within a database. Once you have run a User Rights Review, you can generate reports from the scan data. For more information, see [Pen Tests, Audits, and User Rights Reviews](#).
- **Reports.** Communicate vulnerabilities discovered by AppDetectivePro (and actions taken) to all levels of your organization. For more information, see [Reports](#).
- **Edit Menu Tasks.** Add applications for AppDetectivePro to Pen Test or Audit, modify the risk level of a built-in check, organize your AppDetectivePro export/purge data, and more. For more information, see [Edit and Tools Menu Tasks](#).
- **Job Scheduler.** Schedule the date and time to run an AppDetectivePro task, such as a Pen Test or Audit. For more information, see [Job Scheduler](#).
- **Vulnerability Manager.** Manage security vulnerabilities found in a Session, apply filters to help you assess the status of various application vulnerabilities, and more. For more information, see [Vulnerability Manager](#).
- **User-Defined Checks.** Define your own MS-SQL and Oracle checks to supplement the built-in AppDetectivePro security checks. For more information, see [User-Defined Checks](#).
- **Fix Scripts.** Generate SQL scripts designed to correct misconfigurations and address vulnerabilities identified by AppDetectivePro during an Audit. For more information, see [Fix Scripts](#).

Customer Support

Customer Support is available from 9 A.M. to 9 P.M. (GMT -5) Monday through Friday, except for company holidays. You may contact technical support for the list of company holidays.

Extended support of 24x7 is available as an added cost. You may contact sales@appsecinc.com if you require this service.

Telephone (in the U.S.): 1-866-927-7732

Telephone (outside the U.S.): 1-212-912-4100

Email: support@appsecinc.com

This section consists of the following topics:

- [What is the License File?](#)
- [Licensing FAQ](#)
- [Downloading the License File](#)
- [Viewing Your License File](#)

What is the License File?

The AppDetectivePro license file specifies whether your version of AppDetectivePro software is an evaluation or production version, as well as other important license details. If you have an evaluation version, the license file specifies when your evaluation period ends. The license file also specifies your machine ID number, the number of Pen Test and Audit licenses purchased, and more.

Licensing FAQ

Q. How is the license file generated?

A. RSA is used to sign and verify the license file. Do not edit it under any circumstances. Doing so will result in a non-functioning key. If you are having problems with a license key, email support@appsecinc.com.

Q. How do I know if my license has expired?

A. Choose View > Licensing Info to determine whether your license has expired. For more information, see [Viewing Your License File](#).

Q. What happens when my license expires?

A. If your AppDetectivePro license expires, you can't run tests using the software. Email support@appsecinc.com to renew your license file.

Q. My license key expired, how do I get a new one?

A. Email support@appsecinc.com or call 1-866-9APPSEC. More ways to reach us are available at www.appsecinc.com.

Q. Where do I put my new license key if I obtained a new one from your company?

A. In most cases, you download your new license file to the appropriate directory.

The directory for the AppDetectivePro license file is: `<installation directory>\AppSecInc\licenses` (for example, `C:\Program Files\AppSecInc\licenses` for 32-bit machine, or `C:\Program Files (x86)\AppSecInc\licenses` for 64-bit machine). For more information, see [Downloading the License File](#).

Downloading the License File

The license file is a separate download from Application Security, Inc. and should be placed in the `\licenses` folder located in the AppDetectivePro installation directory.

The directory for the AppDetectivePro license file is: `<installation directory>\AppSecInc\licenses` (for example, `C:\Program Files\AppSecInc\licenses` for 32-bit machine, or `C:\Program Files (x86)\AppSecInc\licenses` for 64-bit machine).

Viewing Your License File

To view your AppDetectivePro license file, choose **View > Licensing Info**. The **Licensing Info** dialog box displays your license file. The license file consists of the following parts:

- **License File: drop-down.** Allows you to choose an AppDetectivePro license on your computer (assuming you have multiple licenses).
- **Customer Name:** Displays the name of the customer who was originally issued the AppDetectivePro license.
- **License Type:** Specifies whether the license is a production or evaluation copy.
- **Product Version:** Specifies whether the license is an enterprise version.
- **Expiration Date:** Specifies the license expiration date.
- **ASAP Expiration:** Specifies when you can no longer perform an ASAP Update of AppDetectivePro.
- **Machine ID #:** Specifies the ID number of the machine where the AppDetectivePro license is installed. You can click the **Get Machine ID #** button to obtain the ID number of your machine (see below).
- **Application Type: drop-down.** Allows you to choose a license file specifically for applications that use a specific database (for example, **Oracle**).
- **Penetration Tests tab.** Click to display the number of licenses purchased for Pen Tests.

- **Security Audits tab.** Click to display the number of licenses purchased for Audits.
- **User Rights Review tab.** Click to display the number of licenses purchased for User Rights Reviews.
- **Get Machine ID # button.** Click to display the **Machine ID Number** pop up, which allows you to obtain the machine ID number of your machine. You can manually copy/paste the machine ID number into an email or document, or click the **Copy to Clipboard** button to copy the machine ID number to your computer's clipboard, then paste the machine ID number into an email or document.
- **Select License File button.** Click to display the **Open** dialog box and manually locate/open a license file on your computer or network

This section consists of the following topics:

- [Installing and Configuring AppDetectivePro and SHATTER Knowledgebase Components](#)

Installing and Configuring AppDetectivePro and SHATTER Knowledgebase Components

Caution!	Before you start installing AppDetectivePro, make sure you have thoroughly reviewed the Minimum System Requirements .
-----------------	---

This topic consists of the following sub-topics:

- [Installing AppDetectivePro](#)
- [Installing the Prerequisite Database Component](#)
- [Installing the Prerequisite SHATTER Knowledgebase Component](#)
- [IBM DB2 Client Driver Installation](#)
- [Supported and Non-Supported Client Configurations](#)
- [Downloading and Installing the IBM DB2 Client Drivers](#)
- [Microsoft .NET Framework 1.1 Prerequisite for IBM DB2 v8.x Client Drivers](#)
- [Lotus Notes Client Driver Installation](#)
- [Sybase Client/Client Driver/.NET Driver Installation](#)
- [MySQL Client Driver Installation](#)

Installing AppDetectivePro

To install/configure AppDetectivePro:

1. Locate the AppDetectivePro setup file on the Application Security, Inc.-provided CD, or download it from the Application Security, Inc. customer portal site.
 2. Save the file to a convenient location on your computer (for example, [C:\temp](#)).
 3. Double click the executable ([appdetectivepro_setup.exe](#)) file.
-

Installing the Prerequisite Database Component

If the AppDetectivePro installer determines you are missing the Database Component, the [Welcome to the Database Component Setup](#) dialog box appears, prompting you to complete the following Database Component installation steps:

Step	Action
1	When the Welcome to the Database Component Setup dialog box appears, click the Next button to display the Database Component's End-User License Agreement dialog box.
2	Read the License Agreement. If you accept the terms of the License Agreement, check I accept the terms of the license agreement to illuminate the Next button. Click the Next button to display the Destination Folder dialog box.
3	By default, the installer installs the Database Component in the <code>\Database</code> sub-folder located under <code><installation directory>\Program Files\AppSecInc</code> . You can click the Change... button to specify a different installation path for the Database Component.
4	Click the Next button to display the Database Component Repository dialog box, which prompts you to select the database server type . If you select: <ul style="list-style-type: none">• Microsoft Access, the Ready to Install Database Component dialog box appears. Go to Step 9.• Microsoft SQL Server (Express, 2000, 2005, or 2008), the Database Component Repository dialog box appears, prompting you to complete a few additional steps. Complete Steps 5-8.

Step	Action
5	<p>If you selected Microsoft SQL Server (Express, 2000, 2005, or 2008) as your database server type, the Database Component Repository dialog box appears, prompting you to complete a few additional steps.</p> <p>Specify the location of the Microsoft SQL Server instance, which can be local or remote. You can:</p> <ul style="list-style-type: none">• use the Database Instance drop-down to select an available instance for the Database Component• manually enter an instance name (in the editable Database Instance drop-down field) using the syntax <code>hostname\instance</code> (for example, <code>myserver\myinstance</code>) or <code>hostname:port</code> (for example, <code>myserver:1883</code>). If you enter <code>hostname:port</code>, you do not need to have the SQL Server browser service turned on. <p>You can also click the Browse... button to locate a different instance on your network. The Select Computer pop-up appears, allowing you to search for a database host.</p> <p>Click Next to display the Database Installation Credentials dialog box.</p>
6	<p>The Database Credentials dialog box has the default Windows Authentication database authentication type selected by default.</p> <p>The Database Installation Credentials screen allows you to select the authentication type to use to install the Database Component. AppDetectivePro will use this user to create/modify tables, views, and other objects in the Database Component. The Database Component installer automatically creates the database.</p> <p>Select one of the following authentication types for the database user:</p> <ul style="list-style-type: none">• Windows Authentication (default), and go to Step 7• SQL Authentication, and go to Step 8. <p>If you're not sure which authentication type to select, see your database administrator.</p>

Step	Action
7	<p>If you selected the default Windows Authentication database authentication type in Step 6, the Database Installation Credentials dialog box appears. The Windows Authentication (a/k/a <domain\user>) database authentication type uses the Windows credentials from the account with which you are currently logged in (for fresh installations).</p> <p>You must click the Test Connection button to test the database user credentials. If the connection is successful, a green checkmark icon appears, and the Next button is illuminated.</p> <p>You can click the:</p> <ul style="list-style-type: none">• Next button to display the Ready to Install Database Component screen and go to Step 9.• Modify Database Properties button to display the Database Properties dialog box, which allows you to modify your database data file and log file location. <p>If you click this button, the Database Properties dialog box appears. It enables you to modify your database data file and log file location. This is an advanced option; if you have no reason to force locations, Application Security, Inc. recommends you leave these fields blank.</p> <p>Specify the Database data file path and Database log file path. You can click the Recommend Path button to have the Database Component Setup Wizard populate the fields automatically.</p> <ul style="list-style-type: none">• Click the OK button to apply any changes you made to the database data file and/or log file locations, or the Cancel button to cancel any changes.• The Database Installation Credentials dialog box re-appears. <p>These credentials are used only for first-time installations in order to create the database. When you upgrade, the AppDetectivePro installer will attempt to use Windows Authentication (if possible). If Windows Authentication fails, this dialog box will display again during the upgrade.</p>

Step	Action
8	<p>If you selected the SQL Authentication database authentication type in Step 6, the Database Installation Credentials dialog box displays with the Login: and Password: fields illuminated.</p> <p>Make sure you have enabled SQL authentication on the database.</p> <ul style="list-style-type: none">• Enter a valid Login: and Password:• You must click the Test Connection button to test the database user credentials. If the connection is successful, a green checkmark icon appears, and the Next button is illuminated. You can check the Remember the database credentials for upgrades checkbox (unchecked by default) if you want to store this SQL authentication login/password combination to use when you upgrade to a newer version of AppDetectivePro in the future. This checkbox only displays if you select the SQL Authentication database authentication type. <p>Click:</p> <ul style="list-style-type: none">• Next to display the Ready to Install Database Component screen and go to Step 9.• Modify Database Properties to display the Database Properties dialog box, which allows you to modify your database data file and log file location. <p>If you click this button, the Database Properties dialog box appears, which allows you to modify your database data file and log file location. This is an advanced option, and if you have no reason to force locations, Application Security, Inc. recommends you leave these fields blank.</p>
9	<p>Specify the Database data file path and Database log file path. Click Recommend Path to have the Database Component Setup Wizard populate the fields automatically.</p>

Step	Action
10	<p>Click OK to apply any changes you made to the database data file and/or log file locations, or the Cancel button to cancel any changes. The Data-base Installation Credentials dialog box reappears. AppDetectivePro does not store the credentials provided in this step unless you check the Remember the database credentials for upgrades checkbox. These credentials are used only for first-time installations in order to create the database. If the credentials are missing during an upgrade (in other words, if you do not check the Remember the database credentials for upgrades checkbox), or if the stored credentials are wrong or have changed, this dialog box will display again during the upgrade, prompting you to provide the correct credentials.</p>
11	<p>Once you have selected and configured the database server type for the Database Component (Microsoft Access or Microsoft SQL Server), the Ready to Install Database Component dialog box appears. Click the Install button to install the Database Component. When the Database Component installation is complete, the Completed the Database Component Setup Wizard dialog box appears.</p>
12	<p>Click Finish to complete the Database Component installation. If you are still missing the SHATTER Knowledgebase Component component, the Welcome to the SHATTER Knowledgebase Component Setup dialog box appears, prompting you to complete a separate set of SHATTER Knowledgebase Component installation steps before installing AppDetectivePro. These steps are explained in Installing the Prerequisite SHATTER Knowledgebase Component.</p>

Installing the Prerequisite SHATTER Knowledgebase Component

If the AppDetectivePro installer determines you are missing the SHATTER Knowledgebase Component, then the [Welcome to the SHATTER Knowledgebase Component Setup](#) dialog box appears, prompting you to complete the following SHATTER Knowledgebase Component installation steps:

Step	Action
1	When the Welcome to the SHATTER Knowledgebase Component Setup dialog box appears, click the Next button to display the Ready to install SHATTER Knowledgebase Component dialog box.
2	Click the Install button to begin the SHATTER Knowledgebase Component installation.
3	Click the Finish button to complete the SHATTER Knowledgebase Component installation. If you are not missing any more prerequisite components, go to Step 6 Installing AppDetectivePro.

IBM DB2 Client Driver Installation

To perform an Audit on an IBM DB2 server, you must install the IBM DB2 run time client. If you do not have these drivers and privileges, AppDetectivePro cannot access tables that are critical for information gathering.

If you are already an IBM DB2 user, and you have the run time client installed, you do not need to reinstall the client drivers. You only need your login name and password.

This topic consists of the following sub-topics:

- Supported and Non-Supported Client Configurations
- Downloading and Installing the IBM DB2 Client Drivers
- Microsoft .NET Framework 1.1 Prerequisite for IBM DB2 v8.x Client Drivers
- DB2 Connect Installation for Mainframe.

Supported and Non-Supported Client Configurations

Your IBM DB2 servers and clients should be at the same version in order for AppDetectivePro to perform a successful Audit. For example, if you are Auditing an IBM DB2 v9.1 database, your IBM DB2 same client driver should also be version v9.1. This requirement applies to IBM DB2 databases on all supported platforms; for more information, see [Supported Platforms](#).

Detailed information on the IBM DB2 website describes the standard and gateway configuration support for IBM DB2 clients. For more information on:

- **version 8** refer to: <http://publib.boulder.ibm.com/infocenter/db2help/index.jsp?topic=/com.ibm.db2.udb.doc/start/r0009731.htm>

If you are installing an IBM DB2 v8.x driver, you **must** install the Microsoft .NET Framework 1.1 on your system first. For more information, see Microsoft .NET Framework 1.1 Prerequisite for IBM DB2 v8.x Client Drivers.

- **version 9.1** refer to: <http://publib.boulder.ibm.com/infocenter/db2luw/v9/index.jsp?topic=/com.ibm.db2.udb.uprun.doc/doc/r0009731.htm>
- **version 9.5** refer to: <http://publib.boulder.ibm.com/infocenter/db2luw/v9r5/index.jsp?topic=/com.ibm.db2.luw.qb.client.doc/doc/r0009731.html>

Audits of IBM DB2 databases on all platforms require you to download one or more of the following run-time clients (all of which are available at <http://www-01.ibm.com/support/docview.wss?rs=71&uid=swg27007053>):

- 'DB2 Run-Time Client' version 8.1 or 8.2

If you are installing an IBM DB2 v8.x driver, you **must** install the Microsoft .NET Framework 1.1 on your system first. For more information, see Microsoft .NET Framework 1.1 Prerequisite for IBM DB2 v8.x Client Drivers.

- 'DB2 Runtime Client' version 9.1 (any FP)
- 'IBM Data Server Runtime Client' version 9.5 (any FP).

Downloading and Installing the IBM DB2 Client Drivers

To download and install IBM DB2 client drivers:

Step	Action
1	<p>The client drivers needed are run time. You can do one of the following:</p> <ul style="list-style-type: none"> • Contact your system administrator, who can provide the IBM DB2 installation CD containing the client drivers. • Download the appropriate run time client. You can download the: <ul style="list-style-type: none"> -IBM DB2 run time client version 8.1 or 8.2 (any FP) from http://www-1.ibm.com/software/data/db2/udb/support/downloadv8.html. <p>If you are installing an IBM DB2 v8.x driver, you must install the Microsoft .NET Framework 1.1 on your system first. For more information, see Microsoft .NET Framework 1.1 Prerequisite for IBM DB2 v8.x Client Drivers.</p> <ul style="list-style-type: none"> -IBM DB2 run time client version 9.1 (any FP) from http://www-1.ibm.com/software/data/db2/udb/support/downloadv9.html or IBM Data Server run time client version 9.5 (any FP) from http://www.ibm.com/support/docview.wss?rs=71&uid=swg21287889 <p>Do the following:</p> <ul style="list-style-type: none"> -From the drop-down, select the appropriate version of Windows where AppDetectivePro is running. -Click the GO button. -Scroll down and download the DB2 Administration Client (language independent version). <ul style="list-style-type: none"> • Or, you can visit the IBM website (http://www-1.ibm.com/support/all_download_drivers.html) and search for an appropriate driver. <ul style="list-style-type: none"> -From the Category drop -down, select Information Management. -From the Sub-category drop -down, select DB2 for Linux, Unix, and Windows. -On the next page that displays, select Windows from the Operating System list. -From the list, select DB2 Vx.x Fix Packs and Client Downloads (for the appropriate version of Windows). -Select the Runtime Client Installable for the appropriate language. • As a final alternative, you can download an evaluation version of IBM DB2 from the IBM website, and install the client drivers which come with the installation package. For more information, see http://www-3.ibm.com/software/data/db2/
2	Locate the downloaded client driver on your hard drive (a <code>.zip</code> file).

Step	Action
3	Use a utility like Winzip to unzip the contents into a temporary install directory.
4	Once the files are extracted into the temporary install directory, double click the setup file (setup.exe) to begin the installation process.
5	Click the Next button to choose the IBM DB2 client.
6	Choose Typical .
7	Click the Next button.
8	Choose to install the client in the default location.
9	Click the Next button. A dialog box informs you if there is enough information to complete the installation.
10	Click the Next button.
11	Click the Finish button.
12	Reboot your system. The IBM DB2 client drivers are now installed. You can now perform Audits on an IBM DB2 server.

Microsoft .NET Framework 1.1 Prerequisite for IBM DB2 v8.x Client Drivers

If you are installing an IBM DB2 v8.x driver, you must install the Microsoft .NET Framework 1.1 on your system first. If the driver is already installed, install and configure Microsoft .NET Framework 1.1, then reinstall the IBM DB2 v8.x driver. You can download Microsoft .NET Framework 1.1 from the following location:

<http://www.microsoft.com/downloads/details.aspx?familyid=262D25E3-F589-4842-8157-034D1E7CF3A3&displaylang=en>

To download and install IBM DB2 client drivers:

Step	Action
1	<p>The client drivers needed are run time. Either contact your system administrator, who can provide the IBM DB2 installation CD containing the client drivers; or download the appropriate run time client. You can download the:</p> <ul style="list-style-type: none">• IBM DB2 run time client version 8.1 or 8.2 (any FP) from http://www-1.ibm.com/software/data/db2/udb/support/downloadv8.html. If you are installing an IBM DB2 v8.x driver, you must install the Microsoft .NET Framework 1.1 on your system first. For more information, see Microsoft .NET Framework 1.1 Prerequisite for IBM DB2 v8.x Client Drivers.• IBM DB2 run time client version 9.1 (any FP) from http://www-1.ibm.com/software/data/db2/udb/support/downloadv9.html or IBM Data Server run time client version 9.5 (any FP) from http://www.ibm.com/support/docview.wss?rs=71&uid=swg21287889

Step	Action
2	<p>Do the following:</p> <ul style="list-style-type: none">• From the drop-down, select the appropriate version of Windows where AppDetectivePro is running.• Click the GO button.• Scroll down and download the DB2 Administration Client (language independent version). <p>Or, visit the IBM website (http://www-1.ibm.com/support/all_download_drivers.html) and search for an appropriate driver.</p> <ul style="list-style-type: none">• From the Category drop -down, select Information Management.• From the Sub-category drop -down, select DB2 for Linux, Unix, and Windows.• On the next page that appears, select Windows from the Operating System list.• From the list, select DB2 Vx.x Fix Packs and Client Downloads (for the appropriate version of Windows).• Select the Runtime Client Installable for the appropriate language. <p>As a final alternative, you can download an evaluation version of IBM DB2 from the IBM website, and install the client drivers which come with the installation package. For more information, see http://www-3.ibm.com/software/data/db2/</p>
3	Locate the downloaded client driver on your hard drive (a .zip file).
4	Use a utility like Winzip to unzip the contents into a temporary install directory.
5	Once the files are extracted into the temporary install directory, double click the setup file (setup.exe) to begin the installation process.
6	Click the Next button to choose the IBM DB2 client.
7	Choose Typical .
8	Click the Next button.
9	Choose to install the client in the default location.

Step	Action
10	Click the Next button. A dialog box informs you if there is enough information to complete the installation.
11	Click the Next button.
12	Click the Finish button.
13	Reboot your system. The IBM DB2 client drivers are now installed. You can now perform Audits on an IBM DB2 server.

DB2 CONNECT INSTALLATION FOR MAINFRAME

There are certain requirements to Audit IBM DB2 for Mainframe (OS/390 and z/OS). You must have DB2 Connect installed on the same computer where AppDetectivePro is installed. AppDetectivePro does not support the use of a DB2 Connect in a gateway configuration. All DB2 Connect editions require you to obtain a proper license from IBM.

IBM DB2 OS/390 and z/OS Audits work when using:

- **DB2 Connect Personal Edition 8.1 or 8.2** (any FP), which you can obtain from: <http://www-1.ibm.com/software/data/db2/udb/support/downloadv8.html>

If you are installing an IBM DB2 v8.x driver, you must install the Microsoft .NET Framework 1.1 on your system first. For more information, see Microsoft .NET Framework 1.1 Prerequisite for IBM DB2 v8.x Client Drivers.

- **DB2 Connect Personal Edition 9.1** (any FP), which you can obtain from: <http://www-1.ibm.com/software/data/db2/udb/support/downloadv9.html>
- **DB2 Connect Personal Edition 9.5** (any FP), which you can obtain from: <http://www.ibm.com/support/docview.wss?rs=71&uid=swg21287889>

If you have a computer with an IBM Data Server Client installed, you can activate DB2 Connect Personal Edition by registering your DB2 Connect Personal Edition license to that computer.

Enterprise editions of DB2 Connect (at the versions listed above or higher) should also work, as long as they are not used in a gateway configuration.

Finally, there are certain requirements when accessing a host database at a lower level than the DB2 Connect installation.

- For **version 8**, refer to: <http://publib.boulder.ibm.com/infocenter/db2luw/v8/topic/com.ibm.db2.udb.doc/conn/r0011119.htm>
- For **version 9.1**, refer to: <http://publib.boulder.ibm.com/infocenter/db2luw/v9/topic/com.ibm.db2.udb.uprun.doc/doc/r0011119.htm>
- For **version 9.5**, refer to: <http://publib.boulder.ibm.com/infocenter/db2luw/v9r5/topic/com.ibm.db2.luw.qb.dbconn.doc/doc/r0011119.html>

Lotus Notes Client Driver Installation

To perform an Audit of a Lotus Notes-based Domino Mail Server, you must install the Lotus Notes client drivers. If you are already a Lotus Notes user, you do not need to re-install the client drivers. You only need to find your `.id` file, typically located in your `C:\Lotus\Notes\Data` folder. You must also know your password.

This topic consists of the following sub-topics:

- [Downloading and Installing Lotus Notes Client Software](#)
- [Starting Lotus Notes for the First Time](#)

DOWNLOADING AND INSTALLING LOTUS NOTES CLIENT SOFTWARE

To download and install Lotus Notes client software:

Step	Action
1	Open http://www.lotus.com in your browser.
2	Click the Downloads link.

Step	Action
3	Click the most appropriate Lotus Notes client software download link. You must register to access the download site.
4	Download the Lotus Notes client software setup file to a convenient location (for example, <code>C:\temp</code>).
5	Double click the setup file you downloaded from the Lotus website. The welcome dialog box appears.
6	Click the Next button. The license dialog box appears.
7	Read the License Agreement .
8	If you consent to the License Agreement , press the Yes button to continue. The name and company dialog box appears.
9	Enter your name and company name.
10	Click the Next button. The default installation directory dialog box appears.
11	Do not change the default installation directories.
12	Click the Next button. The setup dialog box appears.
13	Select Typical Setup .
14	Click the Next button. The Lotus Notes program icons dialog box appears.
15	Specify the folder where you want to install the Lotus Notes program icons. Lotus Notes is installed.

STARTING LOTUS NOTES FOR THE FIRST TIME

Your Domino administrator must set up a valid Lotus Notes account for you. He/she can provide you with a password as well as an .id file which you must copy to your C:\Lotus\Notes\Data folder. Contact your Domino administrator if you are unsure about the proper responses to give in the following procedure.

To start Lotus Notes for the first time:

Step	Action
1	Choose Start > Lotus Applications > Lotus Notes . The set up connections dialog box appears.
2	Click the Next button. The Connect to Domino Server dialog box appears.
3	Click the Next button.
4	Choose your desired method of connecting to the server. If you are in an office, select Connect through a LAN .
5	Click the Next button. The Server dialog box appears.
6	Enter your server name. (Ask your Domino administrator if you are unsure.)
7	Click the Next button. The Browse for Your ID File/Lotus Notes Name dialog box appears.
8	Browse for your .id file, or use your Lotus Notes name. (Ask your Domino administrator if you are unsure.)
9	Click the Next button. Setup is complete. You may or may not want to set up your email, news, directory server, and proxy servers. This is usually done by your Domino administrator. At this point, you have provided enough information to run AppDetectivePro for Lotus Domino.

Sybase Client/Client Driver/.NET Driver Installation

To perform an Audit on a Sybase ASE dataserer, you must have the following installed on your workstation:

- the **Sybase client**
- a **Sybase ASE ODBC driver**
- a client-appropriate **ADO.NET driver**

AppDetectivePro uses both the Sybase ASE ODBC and ADO.NET drivers to access your Sybase dataserer. For more information on supported Sybase client versions, see [Minimum System Requirements](#).

Note: An issue exists with the Sybase Adaptive Server Enterprise 15.x ODBC driver that results in an AppDetectivePro connection failure when a Sybase 15.0.2/3 ODBC driver is installed. This is a known issue with the Sybase ODBC driver, and **not** with AppDetectivePro.

The current suggested solutions for this issue are to:

- use an older Sybase ODBC driver, even if you have Sybase 15.x installed (Sybase 15, for example)
- use the new Sybase ASE ODBC driver 15.05.0000.1016, or newer

This topic consists of the following sub-topics:

- [Verifying That You Have the Proper Sybase ASE ODBC Drivers Installed](#)
- [Checking If You Have the ADO.NET Driver Installed](#)
- [Downloading and Installing Sybase ASE ODBC Drivers and the Sybase Client-Appropriate .NET Driver](#)

VERIFYING THAT YOU HAVE THE PROPER SYBASE ASE ODBC DRIVERS INSTALLED

To check if you have the proper Sybase ASE ODBC driver installed:

Step	Action
1	Choose Start > Settings > Control Panel .
2	Double click the Administrative Tools icon.

Step	Action
3	Double click the Data Sources (ODBC) icon.
4	Click the Drivers tab.
5	Scroll down and check if you have either the Sybase ASE ODBC Driver or the Adaptive Server Enterprise ODBC Driver installed (in the Name column).
6	<p>If you:</p> <ul style="list-style-type: none"> • have the drivers on your machine, you are ready to use AppDetectivePro's security Audit feature (assuming you have the proper ADO.NET driver installed, as explained in Checking If You Have the ADO.NET Driver Installed) • do not have the driver installed, go to Downloading and Installing Sybase ASE ODBC Drivers and the Sybase Client-Appropriate .NET Driver.

CHECKING IF YOU HAVE THE ADO.NET DRIVER INSTALLED

To check if you have the Sybase ADO.NET driver installed:

Step	Action
1	<p>For Sybase 12.5.x and 15.0.x, check the <code>[install dir]\ado.net\dll</code> directory for the dll files listed in Step 3-4 of Downloading and Installing Sybase ASE ODBC Drivers and the Sybase Client-Appropriate .NET Driver, respectively.</p> <p>For Sybase 15.5, check the <code>[install dir]\DataAccess\ADONET\dll</code> directory for the dll files listed in Step 5 of Downloading and Installing Sybase ASE ODBC Drivers and the Sybase Client-Appropriate .NET Driver.</p>
2	If the dlls are there, then the ADO.NET driver is installed and can be used after you copy the dlls to <code>[Common Files]</code> folder (as explained in Downloading and Installing Sybase ASE ODBC Drivers and the Sybase Client-Appropriate .NET Driver).

Step	Action
3	<p>If the dlls are not present, then you must install the ADO.NET driver before you can Audit a Sybase database.</p> <p>In Sybase 12.5.x and 15.0.x the option to install the ADO.NET driver is not selected by default. Therefore you must perform a custom installation and select the driver manually.</p> <p>However, in Sybase 15.5, the driver is installed by default. Therefore, you do not need to perform a custom installation, but you still must copy the dlls to [Common Files] folder (as explained in Downloading and Installing Sybase ASE ODBC Drivers and the Sybase Client-Appropriate .NET Driver).</p>
4	<p>If you:</p> <ul style="list-style-type: none"> • have the drivers on your machine, you are ready to use AppDetectivePro's security Audit feature (assuming you have the proper Sybase ASE ODBC drivers installed, as explained in Verifying That You Have the Proper Sybase ASE ODBC Drivers Installed) • do not have the driver installed, go to Downloading and Installing Sybase ASE ODBC Drivers and the Sybase Client-Appropriate .NET Driver.

DOWNLOADING AND INSTALLING SYBASE ASE ODBC DRIVERS AND THE SYBASE CLIENT-APPROPRIATE .NET DRIVER

Refer to the Sybase installation CDs shipped with your database installation to obtain the correct Sybase ASE ODBC drivers and ADO.NET drivers.

Alternately, you can obtain the Sybase ASE ODBC drivers in the Sybase Software Developer Kit (SDK). This is not a free download. You need to select the following drivers in the custom installation option: [Sybase Open Client and ASE Data providers \(ODBC,OLEDB,ADODB.NET\)](#). For more information, see <http://www.sybase.com>.

You can try to download a free copy of the Sybase SDK. However, Application Security, Inc. is not responsible for when (and whether) Sybase is making this available.

To download and install Sybase ASE ODBC drivers and the Sybase client and a client-appropriate .NET driver:

Step	Action
1	Select Custom in your Sybase driver installer and make sure you select ODBC and ADO.NET .
2	<p>To Audit a Sybase database, you must install both the Sybase client and a client-appropriate ADO.NET driver (included in the Sybase client distribution). You must also copy some files to the [Common Files] folder so AppDetectivePro can retrieve them. In all cases, the .NET Framework 1.1 must be installed in order for the driver to work; for more information, see Minimum System Requirements.</p> <p>For more information on installing the Sybase client-appropriate .NET driver for:</p> <ul style="list-style-type: none">• Sybase 12.5, see Step 3• Sybase 15, see Step 4• Sybase 15.5, see Step 5
3	<p>Sybase 12.5</p> <p>The ADO.NET drivers are not installed by default. You must select the ADO.NET drivers manually when you install the 12.5 Sybase client. After the installation, the driver files will be located in the following folder:</p> <p>[client install dir]/ado.net/dll</p> <p>Copy the following files to the <installation folder>/AppSecInc/Common Files folder:</p> <ul style="list-style-type: none">• Sybase.Data.AseClient.dll• sybdrvado11.dll• sybdrvss1.dll

Step	Action
4	<p data-bbox="278 251 442 286">Sybase 15.0</p> <p data-bbox="278 303 1306 407">The ADO.NET drivers are not installed by default. You must select the ADO.NET drivers manually when you install the 15.0 Sybase client. After the installation, the driver files will be located in the following folder:</p> <p data-bbox="278 416 721 442"><code>[client install dir]/ado.net/dll</code></p> <p data-bbox="278 460 1256 529">Copy the following files to the <code><installation folder>/AppSecInc/Common Files</code> folder:</p> <ul data-bbox="278 546 956 841" style="list-style-type: none">• <code>Sybase.Data.AseClient.dll</code>• <code>sybdrvado115.dll</code>• <code>sybdrvkrb.dll</code>• <code>sybdrvssl.dll</code>• <code>sbgse2.dll</code>• <code>policy.1.15.Sybase.Data.AseClient</code>• <code>policy.1.15.Sybase.Data.AseClient.dll</code>

Step	Action
5	<p data-bbox="278 251 442 286">Sybase 15.5</p> <p data-bbox="278 303 1306 442">The ADO.NET drivers are installed by default, including both a .NET v.1.1 driver and a .NET v.2.0 driver. There is no need to perform a custom installation. AppDetectivePro cannot use the ADO.NET v2.0 driver, even if it's installed.</p> <p data-bbox="278 460 1306 633">After the installation, the driver files will be located in the following folder: <code>[installdir]\DataAccess\ADONET\dll</code>. However, AppDetectivePro cannot read these files in the default location. Therefore, in order to Audit a Sybase database, you must copy the following files to the <code><installation folder>/AppSecInc/Common Files</code> folder:</p> <ul data-bbox="278 659 956 980" style="list-style-type: none"> • <code>policy.1.15.Sybase.Data.AseClient</code> • <code>policy.1.15.Sybase.Data.AseClient.dll</code> • <code>sbgse2.dll</code> • <code>Sybase.Data.AseClient.dll</code> • <code>sybcsi_certicom_fips26.dll</code> • <code>sybcsi_core26.dll</code> • <code>sybdrvado115a.dll</code> • <code>sybdrvkrb.dll</code>

MySQL Client Driver Installation

To perform an Audit on MySQL, you must have the MySQL ODBC driver installed on your workstation. AppDetectivePro uses the MySQL ODBC driver to access your MySQL. For more information on supported MySQL ODBC driver client versions, see [Minimum System Requirements](#).

This topic consists of the following sub-topics:

- VERIFYING THAT You Have the Proper MySQL ODBC Drivers Installed
- Downloading and Installing MySQL ODBC Drivers.

VERIFYING THAT YOU HAVE THE PROPER MYSQL ODBC DRIVERS INSTALLED

To check if you have the proper MySQL ODBC driver installed:

Step	Action
1	Choose Start > Settings > Control Panel .
2	Double click the Administrative Tools icon.
3	Double click the Data Sources (ODBC) icon.
4	Click the Drivers tab.
5	Scroll down and check if you have either the MySQL ODBC 3.51 Driver or the MySQL ODBC 5.1 Driver installed (in the Name column).
6	<p>If you:</p> <ul style="list-style-type: none"> • have the drivers on your machine, you are ready to use AppDetectivePro's security Audit feature • do not have the driver installed, go to Downloading and Installing MySQL ODBC Drivers

DOWNLOADING AND INSTALLING MYSQL ODBC DRIVERS

To download and install MySQL ODBC drivers:

Step	Action
1	<p>You can download MySQL ODBC drivers at:</p> <p>http://dev.mysql.com/downloads/connector/odbc/5.1.html</p>

This section consists of the following topics:

- [Understanding the AppDetectivePro Graphical User Interface \(GUI\)](#)
- [Navigating the Toolbar](#)
- [Navigating Page Views](#)
- [Navigating Menus](#)

Understanding the AppDetectivePro Graphical User Interface (GUI)

To start AppDetectivePro, choose [Start > Programs > AppSecInc > AppDetective > AppDetectivePro](#) from the menu. The AppDetectivePro main page appears.

The graphical user interface (GUI) of the AppDetectivePro main page consists of the following parts:

- [Toolbar](#)
- [Page Views](#)
- [Menus](#)

Toolbar

The toolbar consists of menu shortcut buttons. You can click these buttons to perform AppDetectivePro tasks (for example, creating a Session, performing a Discovery, running a Pen Test or an Audit, and more). You can complete all toolbar tasks from the menu, as well. For more information, see [Navigating the Toolbar](#).

Page Views

Page views display information about your network, its applications (and their vulnerabilities), AppDetectivePro tasks, and more. For more information, see [Navigating Page Views](#).

Menus

The menus allow you to perform AppDetectivePro tasks (for example, creating a Session, performing a Discovery, running a Pen Test or an Audit, and more). You can

complete some menu tasks from the toolbar, as well. For more information, see [Navigating Menus](#).

Navigating the Toolbar

The toolbar consists of buttons that you click to perform AppDetectivePro tasks (for example, creating a Session, performing a Discovery, running a Pen Test or an Audit, and more). You can complete most of the toolbar tasks from the menu, too.

Click the:

- **New** button to create a new Session; for more information, see [Creating a Session](#).
- **Open** button to load a previous Session; for more information, see [Loading a Previous Session](#).
- **Discover** button to perform a Discovery; for more information, see [Running a Discovery](#).
- **Policy** button to configure Policies for Pen Tests or Audits; for more information, see [Viewing a Policy](#).
- **Pen Test** button to run a Pen Test, which tries to “break” the defenses of your application; for more information, see [Running a Pen Test](#).
- **Audit** button to audit your application’s configuration settings from the inside out; for more information, see [Running an Audit](#).
- **User Rights** button to run a User Rights Review of a supported Microsoft SQL Server or Oracle database; for more information, see [Running a User Rights Review](#).
- **Work Plan** button to display the Work Plan Manager, i.e., a tool that maps an imported, built-in Questionnaire to a completed Audit; for more information, see [Interviews, Questionnaires, and Work Plans](#).
- **Interview** button to conduct an Interview against a completed Audit, based on a Work Plan and an associated Questionnaire; for more information, see [Interviews, Questionnaires, and Work Plans](#).
- **Reports** button to generate different reports based on Sessions, Policies, Pen Tests, and Audits you have performed. For more information, see [Running Reports](#).

- **Update** button to run an ASAP Update, which upgrades your copy of AppDetectivePro with the latest checks and enhancements automatically via the Internet (available in v.2.5.22 and above); for more information, see [Performing an ASAP Update](#).
- **Schedule** button to run an AppDetectivePro task at a specified time on your machine; for more information, see [Scheduling a Job](#).
- **Fix** button to generate SQL scripts designed to correct mis-configurations and address vulnerabilities identified by AppDetectivePro during an Audit; for more information, see [Generating a Fix Script](#).

Navigating Page Views

The page views display information about your network, your vulnerabilities, AppDetectivePro tasks, and more. The AppDetectivePro GUI consists of the following page views:

- [Main View](#)
- [Network Tree View](#)
- [Vulnerability View](#)

Main View

The main view allows you to view information about detected Pen Test and Audit vulnerabilities, as well as completed User Rights Review scan data.

For detected Pen Test and Audit vulnerabilities, the main view (center) is comprised of three tabbed sub-windows:

- **Details.** Click the **Details** tab to display a list of information pertaining to the particular applications. Click the **+** icons to browse the information contained within this section.
- **Vulnerability Description.** Click the **Vulnerability Description** tab to display a description of the vulnerability found after a Pen Test or Audit is performed.
- **Graph View.** Click the **Graph View** tab to display a color-coded, graphical view of alerts by risk level (i.e., **High**, **Medium**, **Low**, and **Informational**) and category (i.e., **Mis-configurations**, **Denial of Services**, etc.).

For more information on Pen Tests and Audits, see [Pen Tests, Audits, and User Rights Reviews](#).

For completed User Rights Reviews, the main view (center) is comprised of one sub-window:

- **Details.** The **Details** sub-window displays a list of post-User Rights Review, high-level scan data, such as database parameters, number of users, number of roles, etc. Click the **+** icons to browse the scan data contained within this section.

For more information on User Rights Reviews, see Pen Tests, Audits, and User Rights Reviews.

The main view also contains useful links to AppDetectivePro documentation and the Application Security, Inc. website.

Network Tree View

The network tree view (left) displays the applications and machines found on your network after a Discovery has been loaded or performed. You can click the **+** icon to expand the branches, and the **-** icon to collapse branches. You can also organize the network by adding folders and subsequently moving IP addresses into the folders.

Click an application in the network tree view to display information collected during the Discovery process in the **Details** tab of the main view. Right click any item in the network tree view to display a list of related options.

Vulnerability View

The vulnerability view (bottom) displays vulnerabilities discovered after running a Pen Test and/or Audit. Columns provide the following details:

- **Risk Level**
- **Vulnerability**
- **IP Address**
- **Port Number**
- **Application Name**
- **Vulnerability Details**

You can double click a row to display a dialog box that contains general vulnerability information. Detailed vulnerability data also displays in the main view.

Navigating Menus

The menus allow you to perform AppDetectivePro tasks (for example, creating a Session, performing a Discovery, running a Pen Test or an Audit, and more). You can complete several of the tasks from the toolbar, too.

AppDetectivePro includes the following menus:

- [Session Menu](#)
- [Run Menu](#)
- [Edit Menu](#)
- [View Menu](#)
- [Tools Menu](#)
- [Help Menu](#)

Session Menu

From the [Session](#) menu, you can choose:

- [Session > New](#) to create a new Session (i.e., a logical grouping of applications and the Pen Tests/Audits run against them). For more information, see [Creating a Session](#).
- [Session > Open](#) to load a previous Session. For more information, see [Loading a Previous Session](#).
- [Session > Close](#) to close your current Session.
- [Session > Merge](#) to merge two Sessions. For more information, see [Merging Sessions](#).
- [Session > Exit](#) to close AppDetectivePro.

The [Session](#) menu also displays your ten most recent Sessions created. You can highlight and load any of these recent Sessions.

Run Menu

From the [Run](#) menu, you can choose:

- [Run > Discovery](#) to perform a Discovery, which locates applications on your network, and identifies the applications' IP addresses (as well as ports used to provide network services). For more information, see [What is Discovery?](#).

- **Run > Pen Test** to run a Pen Test, an "outside-in" simulation of what a hacker or intruder might try in order to get past your application defenses. For more information, see [What are Pen Tests, Audits, and User Rights Reviews?](#)
- **Run > Audit** to run an Audit, an "inside-out" assessment of discovered applications that checks password configurations, table access, user roles, and other potential vulnerabilities. For more information, see [What are Pen Tests, Audits, and User Rights Reviews?](#)
- **Run > Interview** to display the Interview tool, which allows you to conduct an Interview. During an Interview, you respond to questions from a Questionnaire in the Work Plan you select (which uses check result data derived from the Audit associated with the Interview). For more information, see [Interviews, Questionnaires, and Work Plans](#).
- **Run > User Rights** to run a User Rights Review, which allows you to conduct a comprehensive "inside-out" scan of users, roles, and their privileges within a Discovered, User Rights reviewable database. For more information, see [Running a User Rights Review](#).
- **Run > Fix Script** to generate an SQL script designed to correct mis-configurations and address vulnerabilities identified during an Audit. For more information, see [What are Fix Scripts?](#)
- **Run > ASAP Updater** to update your version of AppDetectivePro with the latest enhancements and additions.
- **Run > Job Scheduler** to schedule an AppDetectivePro task to run at a pre-set time. For more information, see [What is the Job Scheduler?](#)

Edit Menu

From the **Edit** menu, you can choose:

- **Edit > Add Application** to add an application to a Session manually. For more information, see [Adding an Application to a Session](#).
- **Edit > Vulnerability Management** to manage security vulnerabilities found in a Session with the **Vulnerability Manager**. For more information, see [What is the Vulnerability Manager?](#)
- **Edit > Policies** to rename Policies, create a new Policy, edit a selected Policy and set a selected Policy as current (default). For more information, see [What are Policies?](#)

- **Edit > User-Defined Checks** to create your own MS-SQL and Oracle checks in order to add depth to your existing corporate information security policies. For more information, see [What are User-Defined Checks?](#)
- **Edit > Work Plan** to display the Work Plan Manager, i.e., a tool that maps an imported, built-in Questionnaire to a completed Audit; for more information, see [Interviews, Questionnaires, and Work Plans](#).
- **Edit > Questionnaire** to display the **Questionnaire Editor**, which allows you to view all Questionnaires, Questionnaire details, and individual Questionnaire questions. The **Questionnaire Editor** also allows you to create your own custom Questionnaire. For more information, see [Interviews, Questionnaires, and Work Plans](#).
- **Edit > Questionnaire Type Settings** to display the **Questionnaire Type Settings** dialog box, which allows you to create a Questionnaire type, which you can associate with a custom Questionnaire. You can also revise certain parameters of a built-in Questionnaire (i.e., **DISA-STIG** or **General**). A Questionnaire type consists of question fields and response fields. For more information, see [Working with Questionnaire Types](#).
- **Edit > Interview > Copy** to display the **Copy Interview** dialog box which allows you to copy a completed Interview to use in other Audits; for more information, see [Copying a Completed Interview](#).
- **Edit > Properties** view and modify application properties, for example, page refresh time, report logos, password parameters, and more. For more information, see [Properties](#).

For more information, see [Edit and Tools Menu Tasks](#).

View Menu

From the **View** menu, you can choose:

- **View > Reports** to display the **Report Wizard** dialog box and run AppDetectivePro reports. For more information, see [What are AppDetectivePro Reports?](#)
- **View > Licensing Info** to view your AppDetectivePro license file, which specifies whether your version of AppDetectivePro software is an evaluation or production version, as well as other important license details.
- **View > Refresh** to refresh your AppDetectivePro page.

- **View > SCAP Info** to display the most current information about CPE, CCE, and CVE, including when each component was updated in the product and when last updated by the National Institute of Standards and Technology (NIST); for more information, see Viewing SCAP Information in AppDetectivePro
- **View > Log Files** to display the **AppDetectivePro - Log Viewer** window and collect/open **application log files** and **installation/upgrade log files**. For detailed information on the AppDetectivePro application and installation/upgrade log files, including the locations of the default log file directories, see Appendix T: AppDetectivePro Application Log Files and Installation/Upgrade Log Files.

When you select the **Application Log Files** tab or the **Installation/Upgrade Log Files** tab on the **AppDetectivePro - Log Viewer** window, you can specify a destination folder and collect available application and installation/upgrade log files, respectively. You can also double-click any individual log file to view its contents in Notepad.

Click the:

- **Browse** button on the **AppDetectivePro - Log Viewer** to specify a non-default directory for log file collection. **This is the recommended method of application log file collection.** AppDetectivePro **must** have required privileges to be able to copy the collected log files in the specified location.
- **Collect Log Files** button to collect all available log files.

To maximize the number of generated log files and data to send to Application Security, Inc. Support for troubleshooting, you should run a Discovery, Pen Test, Audit, or User Rights Review before collecting log files.

You can also check the **Show full paths of files** checkbox (unchecked by default) to display the (often very long) full paths of the collected application log files and installation/upgrade log files in the **AppDetectivePro - Log Viewer** window.

Tools Menu

From the **Tools** menu, you can choose:

- **Tools > Export/Purge Data** to export data to a Microsoft Access database file other than the one used by AppDetectivePro, or to purge data from the default database. For more information, see Exporting/Purging Data.

- **Tools > Import Data** to import data from a database, which is useful for transferring Sessions between machines, or when you have a Sessions you want to use from a prior installation. For more information, see Importing Data.
- **Tools > Import Questionnaire** to import a built-in Questionnaire (in XML format). For more information, see Interview Work Flow Step 2: Importing a Built-In Questionnaire/Creating a Custom Questionnaire.

For more information, see Edit and Tools Menu Tasks.

Help Menu

From the **Help** menu, you can choose:

- **Help > Contents** to display the AppDetectivePro online help.
- **Help > Feedback/Product Enhancements** to display an online feedback form and provide feedback and suggest future product enhancements to Application Security, Inc.
- **Help > About AppDetectivePro** to display a pop-up that provides information about your version of AppDetectivePro.

This section consists of the following topics:

- [Performing an ASAP Update](#)
- [Configuring Proxy Settings for the ASAP Updater](#)
- [Uninstalling AppDetectivePro \(and the Database and SHATTER Knowledgebase Components\), and Deleting the AppDetectivePro Back-End Database](#)

Performing an ASAP Update

The ASAP Update feature allows you to update AppDetectivePro and/or SHATTER Knowledgebase to the latest version. Updates generally contain new security checks for Pen Tests and Audits, as well as performance enhancements and new features.

Important!

If you have modified the built-in dictionary files or added any custom dictionary files, you **must** back up these files to a separate temp file. After you successfully complete the ASAP update, you can replace your built-in dictionary and/or custom dictionary files with the ones you backed up.

ASAP Updates can be performed in two ways: either by downloading the executable file and running it locally on the machine where AppDetectivePro is installed, or by clicking 'Update' from the main menu in AppDetectivePro (if access to internet is available).

Using the Update Button:

Step	Action
1	Click Update on the main menu of AppDetectivePro.
2	This will close the AppDetectivePro application, open the AppDetectivePro ASAP Updater dialog box, and display the current Installed Version and available Update Version of both AppDetectivePro and SHATTER Knowledgebase.

Step	Action
3	<p>If a version of either is available, the Download and install updates button will be available to click. Click on the button to continue.</p> <p>Note: It is always best practice to be on the latest version of each component.</p>
4	<p>During the update you will see the process statuses of 'Downloading', 'Verifying', 'Installing' etc.</p> <p>If the Installed Version of AppDetectivePro is not the most current version, then the ASAP updater will download and run AppDetectivePro installer, which also contains the latest SHATTER Knowledgebase.</p> <p>If the Installed Version of the SHATTER Knowledgebase is not the most current version, then the ASAP updater will download and run SHATTER Knowledgebase installer to perform the update.</p> <p>If the Installed Version of AppDetectivePro is not a compatible version with the most current SHATTER Knowledgebase, then the ASAP Updater will also download and run AppDetectivePro installer to update it before updating SHATTER Knowledgebase.</p> <p>The update logs are written to a new log file AsapUpdater_<PID>.log which is located in user's local app date directory like other AppDetectivePro log files.</p>
5	<p>Follow the Update wizard through until the update is complete.</p>

Performing the local update:

Step	Action
1	<p>Log into the AppSecInc Customer Support Portal at http://www.appsecinc.com/support/customer_portal/. Click on the latest 'AppDetectivePro <version> Software and Documentation' link or 'AppDetectivePro ASAP Update Download links' link available in the Top 5 Solutions listing. If you do not have access, contact support@appsecinc.com to set up an account.</p>
2	<p>If updating the AppDetectivePro software use the latest 'AppDetectivePro <version> Software and Documentation link':</p> <p>Download the AppDetectivePro_Setup_<version>_en-US.exe file to a temporary directory.</p> <p>Note: If you are an AppDetectivePro Japanese customer, you should not use this ASAP Update file. For the AppDetectivePro Japanese ASAP Update file and instructions, open http://www.appsecinc.com/update/AppDetective/jp/local_update_instructions.shtml in your web browser.</p> <p>If updating the SHATTER Knowledgebase use the latest 'AppDetectivePro ASAP Update Download links' link:</p> <p>Download the ShatterKnowledgebase_Setup_<version>_en-US.msi file to a temporary directory.</p>
3	<p>Run the AppDetectivePro_Setup_<version>_en-US.exe file or the ShatterKnowledgebase_Setup_<version>_en-US.msi depending on which update you are performing.</p>

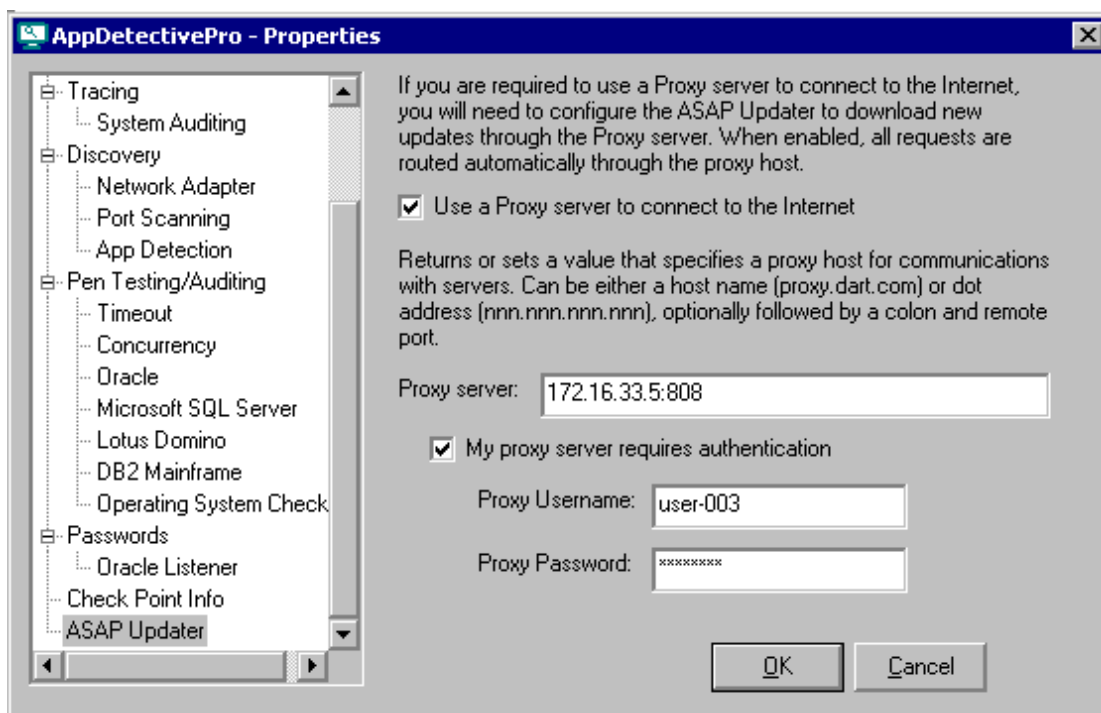
Step	Action
4	<p data-bbox="297 249 1282 322">During the update you will see the process statuses of 'Downloading', 'Verifying', 'Installing' etc.</p> <p data-bbox="297 385 1239 531">If the Installed Version of AppDetectivePro is not the most current version, then the ASAP updater will download and run AppDetectivePro installer, which also contains the latest SHATTER Knowledgebase.</p> <p data-bbox="297 593 1302 704">If the Installed Version of the SHATTER Knowledgebase is not the most current version, then the ASAP updater will download and run SHATTER Knowledgebase installer to perform the update.</p> <p data-bbox="297 767 1288 913">If the Installed Version of AppDetectivePro is not a compatible version with the most current SHATTER Knowledgebase, then the ASAP Updater will also download and run AppDetectivePro installer to update it before updating SHATTER Knowledgebase.</p> <p data-bbox="297 975 1273 1086">The update logs are written to a new log file AsapUpdater_<PID>.log which is located in user's local app date directory like other AppDetectivePro log files.</p> <p data-bbox="297 1149 1208 1218">Note: ASAP Updates for both the AppDetectivePro software and SHATTER Knowledgebase are cumulative.</p>

Configuring Proxy Settings for the ASAP Updater

You can configure proxy server settings for the ASAP Updater under the "ASAP Updater" branch in the Properties dialog box. From this branch:

1. Set the proxy server address and port.

2. Set the proxy server address, port, and authentication information (user name/ password).



Uninstalling AppDetectivePro (and the Database and SHATTER Knowledgebase Components), and Deleting the AppDetectivePro Back-End Database

You can uninstall AppDetectivePro -- as well as the Database Component and the SHATTER Knowledgebase Component -- using the uninstaller tool on the Start Menu. However, you must use SQL Server Enterprise Manager to manually delete the AppDetectivePro SQL Server back-end database, or delete the [AppDetective.mdb](#) file if you have a AppDetectivePro Access back-end database installed.

To uninstall AppDetectivePro—as well as the AppDetectivePro Database Component and the SHATTER Knowledgebase Component—and to delete the AppDetectivePro back-end database:

1. Choose **Start > AppSecInc > AppDetectivePro > Uninstall AppDetectivePro** to display the uninstallation wizard.
2. Follow the prompts. The order of the uninstallation process is the exact opposite of the AppDetectivePro installation process; for more information, see [Installing and Configuring AppDetectivePro and SHATTER Knowledgebase Components](#). The AppDetectivePro uninstallation process does **not** delete your back-end database. You **must** use SQL Server Enterprise Manager to manually delete the AppDetectivePro SQL Server back-end database, or delete the [AppDetective.mdb](#) file if you have a AppDetectivePro Access back-end database installed.
3. A message informs you when the uninstallation is complete. Click **Finish**.

This section describes tasks you perform with AppDetectivePro. It consists of the following topics:

- Sessions
- Discovery
- Policies
- Pen Tests, Audits, and User Rights Reviews
- Interviews, Questionnaires, and Work Plans
- Reports
- Edit and Tools Menu Tasks
- Job Scheduler
- Vulnerability Manager
- User-Defined Checks
- Fix Scripts
- Viewing SCAP Information

Sessions

This section consists of the following topics:

- What is a Session?
- Creating a Session
- Loading a Previous Session
- Renaming a Session
- Merging Sessions
- Importing Sessions

What is a Session?

A Session is a logical grouping of applications and the Pen Tests/Audits run against them. It is a prerequisite to performing a Discovery, and running Pen Tests and Audits.

When you create a Session, AppDetectivePro automatically performs a Discovery of applications on your network. You can then run Pen Tests and Audits against the Discovered applications.

Note:	AppDetectivePro allows you to perform multiple Discoveries in a single Session, by appending each Discovery to the Session -- without overwriting any previous Discoveries. AppDetectivePro also allows you to uniquely name each Session so you can distinguish between them.
--------------	--

Creating a Session

To create a Session:

Step	Action
1	<p>Do one of the following: Choose Session > New from the menu. Click the New button on the toolbar. Press <CTRL>+N. The Session wizard appears. You can also create a new Session, or open an existing Session, by doing one of the following: choose Run > Discover from the menu bar. Click the Discover button on the toolbar. The Session wizard appears, prompting you to create a new Session.</p>
2	<p>Click the Next button. The next page of the Session wizard appears.</p>
3	<p>If you select: Enter ranges on which to Discover applications, and click then Next button, then the Set IP Addresses to Discover page of the Session wizard appears. Go to Step 4. Load list of live network IPs and ports from a file, and click then Next button, then the Which file would you like to use? page of the Session wizard appears. Go to Step 5. Regardless of your selection, if you check Check responses to ports even if the IP address is not responsive, then AppDetectivePro probes all ports (including firewalled ports) to detect whether the IP address is alive.</p>

Step	Action
4	<p>Using the Set IP Addresses to Discover page of the Session wizard, you can specify the IP addresses you want to include (and exclude) in your Discovery. To specify IP addresses to:</p> <p>include in your Discovery, in the upper portion of the page: Manually enter or use the drop-down to specify the Hostname: and the Starting IP: and Ending IP: addresses to include in the Discovery. Click Next and go to Step 6.</p> <p>exclude from your Discovery, then in the lower portion of the page: Manually enter or use the drop-down to specify the Hostname: and the Starting IP: and Ending IP: addresses to exclude from the Discovery. Click Next and go to Step 6.</p> <p>Or, you can click the Load File button to display a pop-up which allows you to load a text or CSV file containing ranges of IP addresses to include/exclude in your Discovery. You must use the following format:</p> <pre><ip address> <ip address> <ip address></pre> <p>For example: 192.168.1.1 192.168.1.100 192.168.1.255</p> <p>For more information, see Appendix V: Uploading Comma-Delimited Text Files, CSV Files, or NMAP Files Containing IP Addresses (or IP Addresses and Ports) to Discover.</p> <p>Optionally, in either portion of the page, you can highlight one or more individual ranges of IP addresses from your include/exclude in a Discovery list, and click the Remove Selected button to remove them. Click <CTRL> to highlight non-sequential IP address ranges. Click Remove All to remove all IP address ranges from an include/exclude in a Discovery list.</p>

Step	Action
5	<p>The Which file would you like to use? page of the Session wizard allows you upload a standard, comma-delimited text file or NMAP file containing the IP addresses you want to Discover.</p> <p>Use the drop-down in the bottom portion of the page to select the file type, i.e., Default (a standard, comma-delimited text file) or NMAP. Manually enter (or click the Browse button to select) the comma-delimited text file or NMAP file containing the IP addresses you want to Discover.</p> <p>When running a Discovery for IBM DB2 (using either file identification method described above), you must include the DB2 Administration Server (DAS) port (523 by default) to ensure AppDetectivePro will Discover all databases. Otherwise, AppDetectivePro will only Discover the default databases (i.e. SAMPLE).</p> <p>AppDetectivePro only supports NMAP normal output files. For more information on NMAP files, see Appendix E: Using NMAP. If you select Default (i.e., a standard, comma-delimited text file), you must use the following format:</p> <pre><ip address>,<port> <ip address>,<port> <ip address>,<port></pre> <p>For example:</p> <pre>192.168.1.1,1024 192.168.1.1,1052 192.168.1.1,1072</pre> <p>For more information, see Appendix V: Uploading Comma-Delimited Text Files, CSV Files, or NMAP Files Containing IP Addresses (or IP Addresses and Ports) to Discover.</p> <p>Click Next and go to Step 6.</p>

Step	Action
6	<p>Check one or more of the following application types to Discover:</p> <ul style="list-style-type: none"> IBM DB2 z/OS IBM DB2 Lotus Domino Microsoft SQL Server MySQL Oracle Sybase Advance Server Enterprise
7	<p>Click Next.</p> <p>The next page of the Session wizard appears.</p>
8	<p>If you select:</p> <ul style="list-style-type: none"> • Discover applications on Default Ports, then AppDetectivePro will Discover applications on known default ports (for each application type chosen in Step 6). Click Next. The next page of the Session wizard appears. Go to Step 9. • Session wizard, then AppDetectivePro will Discover applications on a range of ports that you specify (for each application type chosen in Step 6). You can: <ul style="list-style-type: none"> -Click Next to display the Enter ports on which to discover page of the Session wizard. -Enter a Starting Port: and an Ending Port: -Click Add. Your range of ports appears in the text box. AppDetectivePro will Discover applications on this range of ports. <p>Next, you can specify as many port ranges as you want. Optionally you can highlight one or more individual port ranges, and click the Remove Selected button to remove them. Or, click the Remove All button to remove all port ranges from the text box.</p> <p>Click <CTRL> to highlight non-sequential port ranges.</p> <p>When you're done, click Next. The next page of the Session wizard appears.</p>

Step	Action
9	Enter the: Session name (required) Session description (optional). The next page of the Session wizard appears.
10	Click Next . The next page of the Session wizard displays your Session summary information.
11	Click Next . A Discovery runs, and your Session is saved.

Loading a Previous Session

AppDetectivePro allows you to load a previous Session—useful if you prefer to use NMAP for Discovery, or if you do not wish to create a new Session before running a Pen Test or Audit. For more information on using NMAP files, see [Appendix E: Using NMAP](#).

To load a previous Session:

Step	Action
1	Do one of the following: Choose Session > Open from the menu bar. Click the Open button on the toolbar. Press <CTRL>+O. The Open dialog box appears.
2	Select the Session you want to load.
3	Click the Load Session button. AppDetectivePro loads your selected Session.

Renaming a Session

AppDetectivePro allows you to rename a Session any time.

To rename a Session:

Step	Action
1	Do one of the following: Choose Session > Open from the menu bar. Click the Open button on the toolbar. Press <CTRL>+O. The Open dialog box appears.
2	Select the Session you want to rename.
3	Click Rename .
4	Highlight the old Session name.
5	Enter a new Session name.
6	Click OK .
7	Click Yes to confirm.

Merging Sessions

AppDetectivePro allows you to merge two Sessions into a single unified Session.

Caution!	When merging two Sessions, AppDetectivePro deletes the two original (source) Sessions and creates a single new (merged) Session. If you want to retain the source Sessions, you must export them (for more information, see Exporting/Purging Data), then import them when the merge is finished (for more information, see Importing Data).
-----------------	--

To merge Sessions:

Step	Action
1	Choose Session > Merge from the menu bar. The Merge sessions dialog box appears.
2	Highlight the first Session you want to merge. (To see the Session data, check Show Applications .)
3	Click the Next button. The next Merge sessions dialog box appears.
4	Highlight the Session you want to merge with the first Session selected, in Step 2. (To see the Session data, check Show Applications .)
5	Click the Next button. The Merge sessions dialog box warns you that AppDetectivePro will delete the two original (source) Sessions to create a single new (merged) Session. If you want to retain the source Sessions, export them (for more information, see Exporting/Purging Data), then import them when the merge is finished (for more information, see Importing Data).
6	Click the Next button. The next Merge sessions dialog box informs you when the merge is complete.
7	Click the Finish button.

Importing Sessions

AppDetectivePro allows you to import Session data from a database. This is useful if you want to transfer Sessions between machines, or use Sessions from a prior installation.

To import a Session:

Step	Action
1	Choose Edit > Import Data from the menu bar. The Import/Export/Purge Data dialog box appears.
2	Click the Import Session tab.
3	Click the Set Import File button. The Set Import File dialog box appears.
4	Specify the path and file name of the AppDetectivePro database file (.adb). You can preview the Session by checking Preview session selected above .
5	Click the Import button. A pop-up appears, notifying you AppDetectivePro has exported your Session data as an AppDetectivePro database file (.adb). The imported Session is now available.

Discovery

This section consists of the following topics:

- [What is Discovery?](#)
- [Pre-Discovery: Adding an IBM DB2 Instance](#)
- [Pre-Discovery: Working With Oracle SIDs](#)
- [Known Discovery Limitations for Oracle 10gR1 and Greater on Linux](#)
- [Running a Discovery](#)
- [Post-Discovery](#)

What is Discovery?

When AppDetectivePro performs a Discovery, it:

- locates applications on your network
- identifies the applications' IP addresses (as well as ports used to provide network services)
- automatically creates a **Session** (a prerequisite to the Pen Test or Audit).

Note:	Discovery does not identify vulnerabilities. Discovering vulnerabilities is the function of Pen Tests and Audits.
--------------	--

Pre-Discovery: Adding an IBM DB2 Instance

If there is no Administrator Server it is impossible to locate DB2 databases without additional information. However, AppDetectivePro allows you to add an IBM DB2 instance.

To add an IBM DB2 instance, choose [Edit > Add Application](#) from the menu bar and add the application; for more information, see [Adding an Application to a Session](#).

Pre-Discovery: Working With Oracle SIDs

This section consists of the following topics:

- [SID Enhancements](#)
- [Adding an Oracle SID](#)
- [Brute-Forcing Oracle SIDs](#)
- [Detecting Oracle SIDs with a Listener Password](#)

SID ENHANCEMENTS

AppDetectivePro includes the following Oracle System Identifier (SID) enhancements:

- **Add an Oracle SID.** When you set a listener password, Oracle does not provide information on SIDs. However, AppDetectivePro allows you to add an SID manually.
- **Brute-force Oracle SIDs.** Allows you to determine whether it is possible to brute-force an SID name by attempting all possible combinations of a set length of letters.
- **Detect Oracle SIDs with a listener password.** When you set a listener password, Oracle does not provide information on SIDs. However, AppDetectivePro allows you to specify a listener password that can gather SID information from a specified listener with a set password.

ADDING AN ORACLE SID

To add an Oracle SID:

Step	Action
1	In the network tree view, right click a listener.
2	Select Add SID .
3	Enter the name of the instance you want to add.
4	Click the Verify button.
5	Click the Add button.

BRUTE-FORCING ORACLE SIDS

To brute-force Oracle SIDs:

Step	Action
1	In the network tree view, right click a listener.
2	Select Brute Force SIDs .

Step	Action
3	Enter the number of letters you want to brute force.
4	Click the Run button.

DETECTING ORACLE SIDS WITH A LISTENER PASSWORD

To detect Oracle SIDs with a listener password:

Step	Action
1	In the network tree view, right click a listener.
2	Select Detect SIDS with Listener Password .
3	Enter the password.
4	Click the Detect SIDs button.

Pre-Discovery: Required Open Ports on Machines Running Microsoft SQL Server

In order to run a Discovery against a Microsoft SQL Server database, certain ports on the machine running Microsoft SQL Server must be open. For more information, see [Open Ports \(on Computers Running Microsoft SQL Server\) Required to Run a Discovery](#).

Known Discovery Limitations for Oracle 10gR1 and Greater on Linux

Discoveries performed against Oracle 10gR1 and greater databases on Linux may not work 100% of the time -- even if you supply a correct `LISTENER` password. In some cases, versions of Oracle 10gR1 and greater on the Linux platform respond to the `STATUS` command by abruptly closing the connection as soon as it has sent data from its side. This can cause the client (in this case, the AppDetectivePro machine) to potentially lose incoming data containing results from the `STATUS` command. AppDetectivePro can still obtain some of this data using blocking sockets, but this is not guaranteed (especially over slow networks).

The same limitation applies to the Oracle Pen Test check `ADMIN_RESTRICTIONS flag not set`. The only difference is the use of `LOG_STATUS` command as opposed to `STATUS` command. Both commands may fail against Oracle 10gR1 and greater on Linux (only).

Running a Discovery

When you perform a Discovery, the results are added to your open Session; for more information, see [What is a Session?](#)

Caution! Before you can run a Discovery, you **must** select the network adapter in the **Discovery** branch of the **Properties** dialog box. If you do not, AppDetectivePro will **not** let you run a Discovery.

To run a Discovery:

Step	Action
1	<p>Do one of the following:</p> <ul style="list-style-type: none">• Choose Run > Discover from the menu bar.• Click the Discover button on the toolbar. <p>If you do not have a Session open, the Discovery wizard prompts you to create a new Session; for more information, see Creating a Session.</p>
2	<p>Click the Next button.</p> <p>The next page of the Discovery wizard appears.</p>

Step	Action
3	<p>If you select:</p> <ul style="list-style-type: none">• Enter ranges on which to Discover applications, and click the Next button, then the Set IP Addresses to Discover page of the Discovery wizard appears. Go to Step 4.• Load list of live network IPs and ports from a file, and click the Next button, then the Which file would you like to use? page of the Discovery wizard appears. Go to Step 5. <p>Regardless of your selection, if you check Check responses to ports even if the IP address is not responsive, then AppDetectivePro probes all ports (including firewalled ports) to detect whether the IP address is alive.</p>

Step	Action
4	<p>The Set IP Addresses to Discover page of the Discovery wizard allows you specify the IP addresses you want to include (and exclude) in your Discovery.</p> <p>To specify IP addresses to Include in your Discovery, in the upper portion of the page:</p> <ul style="list-style-type: none">• Manually enter or use the drop-down to specify the Hostname: and the Starting IP: and Ending IP: addresses to include in the Discovery.• Click Next and go to Step 6. <p>To specify IP addresses to Exclude from your Discovery, in the lower portion of the page:</p> <ul style="list-style-type: none">• Manually enter or use the drop-down to specify the Hostname: and the Starting IP: and Ending IP: addresses to exclude from the Discovery.• Click Next and go to Step 6. <p>Or, you can click the Load File button to display a pop-up which allows you to load a text or CSV file containing ranges of IP addresses to include/exclude in your Discovery. You must use the following format:</p> <pre><ip address> <ip address> <ip address></pre> <p>For example:</p> <pre>192.168.1.1 192.168.1.100 192.168.1.255</pre> <p>For more information, see Appendix V: Uploading Comma-Delimited Text Files, CSV Files, or NMAP Files Containing IP Addresses (or IP Addresses and Ports) to Discover.</p> <p>Optionally, in either portion of the page, you can:</p> <ul style="list-style-type: none">• highlight one or more individual ranges of IP addresses from your include/exclude in a Discovery list, and click the Remove Selected button to remove them. Click <CTRL> to highlight non-sequential IP address ranges.• click the Remove All button to remove all IP address ranges from an include/exclude in a Discovery list.

Step	Action
5	<p>The Which file would you like to use? page of the Session wizard allows you upload a standard, comma-delimited text file or NMAP file containing the IP addresses you want to Discover. Do the following:</p> <ul style="list-style-type: none">• Use the drop-down in the bottom portion of the page to select the file type, i.e., Default (a standard, comma-delimited text file) or NMAP.• Manually enter (or click the Browse button to select) the comma-delimited text file or NMAP file containing the IP addresses you want to Discover. <p>Be aware that when you run a Discovery for IBM DB2 (using either file identification method described above), you must include the DB2 Administration Server (DAS) port (523 by default) to ensure AppDetectivePro will Discover all databases. Otherwise, AppDetectivePro will only Discover the default databases (i.e. SAMPLE).</p> <p>AppDetectivePro only supports NMAP normal output files.</p> <p>If you select Default (i.e., a standard, comma-delimited text file), you must use the following format:</p> <pre><ip address>,<port> <ip address>,<port> <ip address>,<port></pre> <p>For example:</p> <pre>192.168.1.1,1024 192.168.1.1,1052 192.168.1.1,1072</pre> <ul style="list-style-type: none">• Click Next.
6	<p>Check one or more of the following application types to Discover:</p> <ul style="list-style-type: none">• IBM DB2 z/OS• IBM DB2• Lotus Domino• Microsoft SQL Server• MySQL• Oracle• Sybase Advance Server Enterprise

Step	Action
7	Click Next . The next page of the Discovery wizard appears.
8	<p>If you select:</p> <ul style="list-style-type: none"> • Discover applications on Default Ports, then AppDetectivePro will Discover applications on known default ports (for each application type chosen in Step 6). Click the Next button. <p>The next page of the Discovery wizard appears. Go to Step 9.</p> <ul style="list-style-type: none"> • Discover applications on a list of ports, then AppDetectivePro will Discover applications on a range of ports that you specify (for each application type chosen in Step 6). You can: <ul style="list-style-type: none"> -Click the Next button to display the Enter ports on which to discover page of the Discovery wizard. -Enter a Starting Port: and an Ending Port: -Click the Add button - <p>When running a Discovery for IBM DB2 (using either file identification method described above), you must include the DB2 Administration Server (DAS) port (523 by default) to ensure AppDetectivePro will Discover all databases. Otherwise, AppDetectivePro will only Discover the default databases (i.e. SAMPLE).</p> <p>Your range of ports displays in the text box. AppDetectivePro will Discover applications on this range of ports.</p> <p>You can specify as many port ranges as you want. Optionally you can highlight one or more individual port ranges, and click the Remove Selected button to remove them. Or, click the Remove All button to remove all port ranges from the text box.</p> <p>Click <CTRL> to highlight non-sequential port ranges.</p> <p>When you're done, click Next.</p> <p>The next page of the Discovery Wizard appears. Go to Step 9.</p>

Step	Action
9	Enter the: <ul style="list-style-type: none">• Session name (required)• Session description (optional). The next page of the Discovery wizard appears.
10	Click the Next button. The next page of the Discovery wizard displays your Session summary information.
11	Click the Next button. The Discovery runs, and your Session is saved.

Post-Discovery

This section consists of the following topics:

- [Displaying/Hiding Discovered Applications in the Network Tree View](#)
- [Running Pen Tests/Audits/User Rights Reviews/Reports From the Network Tree View \(Shortcuts\)](#)
- [Displaying, Printing, and Saving Discovered Application Information](#)

DISPLAYING/HIDING DISCOVERED APPLICATIONS IN THE NETWORK TREE VIEW

After creating a Session, or loading a previous Session, the network tree view displays all Discovered applications. You can click the:

- + icons to expand tree branches and display Discovered applications
- - icons to collapse tree branches and hide Discovered applications.

For more information on:

- creating a Session, see [Creating a Session](#)
- loading a previous Session, see [Loading a Previous Session](#)
- working with the network tree view, see [Navigating Page Views](#).

RUNNING PEN TESTS/AUDITS/USER RIGHTS REVIEWS/REPORTS FROM THE NETWORK TREE VIEW (SHORTCUTS)

To run a Pen Test, Audit, User Rights Review, or Report from the network tree view:

Step	Action
1	Right click an application.
2	<p>You can select:</p> <ul style="list-style-type: none"> • Pen Test with... to Pen Test a Discovered application • Audit with... to Audit a Discovered application • User Rights Review... run a User Rights Review against a Discovered application • Generate Pen Test Reports or Generate Audit Reports to run Reports on Pen Tested and Audited applications, respectively.

For more information on running:

- Pen Tests, see [Running a Pen Test](#)
- Audits, see [Running an Audit](#)
- User Rights Reviews, see [Running a User Rights Review](#)
- Reports, see [Running Reports](#)

DISPLAYING, PRINTING, AND SAVING DISCOVERED APPLICATION INFORMATION

To display Discovered application information:

Step	Action
1	<p>In the network tree view, click a Discovered application. Click the + icons in the network tree view to display all Discovered applications.</p> <p>The main view (Details tab) displays detailed information on Discovered applications. AppDetectivePro gathers this information by querying the ports of the Discovered applications. This information differs from application to application.</p>

To print Discovered application information:

Step	Action
1	Right click Application Info and choose Print Tree . AppDetectivePro prints Discovered application information for the branches of the tree you have expanded.

To save a Discovered application information grid to a file:

Step	Action
1	Right click the grid and choose Export .

Policies

This section consists of the following topics:

- [What are Policies?](#)
- [Built-In Audit Policies](#)
- [Built-In Pen Test Policies](#)
- [Viewing a Policy](#)
- [Creating a Policy](#)
- [Editing a Policy](#)
- [Modifying the Risk Level of Checks Associated With Custom Policies](#)
- [Renaming a Policy](#)
- [Importing a Policy](#)
- [Activating/Deactivating a Policy](#)
- [Exporting a Policy](#)
- [Purging a Policy](#)
- [Searching Policies](#)
- [Specifying the Current Policy for a Pen Test or Audit](#)
- [Specifying Exceptions](#)
- [Running a Policy Report](#)
- [Advanced Policy Editor Features](#)

What are Policies?

Policies are sets of security checks used by AppDetectivePro to perform Pen Tests and Audits. AppDetectivePro includes built-in Policies which can be used "out of the box." For more information, see [Built-In Audit Policies](#) and [Built-In Pen Test Policies](#).

Built-In Audit Policies

AppDetectivePro includes the following built-in Audit Policies.

Note:	Built-in Policies cannot be modified. However, you can edit a built-in Policy and perform a "save as" to save the edited Policy under a different name. For more information, see Editing a Policy .
--------------	--

- **Base Line.** Provides an adequate level of security for most applications in the government, financial services, and healthcare industries. Provides maximum security without sacrificing performance and functionality.
- **FISMA.** This Policy is structured following NIST standards and is recommended for use in a FISMA compliance assessment.
- **Basel II.** This Policy is structured for use in a Basel II compliance assessment.
- **Integrity.** This Policy is used to Audit the integrity of an application and the underlying operating system.
- **Best Practices for Federal Government.** Based on CIS, NSA SNAC, DISA Database STIG, NIST 800-53, and Best Practices defined by Application Security's Team SHATTER.
- **Operating System.** A Policy that checks the service, registry, and file portions of a database. It requires an authenticated account to the physical machine running the database.
- **Download.** A default Policy that allows an evaluator the chance to test specific checks.
- **MITs.** This Policy is structured following CoBIT, ISO, and NIST standards and is recommended for use in a MITs compliance assessment.
- **Passwords.** This Policy is used to Audit password strength and settings.

- **DISA-STIG Database Security Configuration.** This policy has been created with guidance of the configuration parameters outlined by the DISA-STIG for SQL Server and Oracle only.

Note:	Starting with version 6.0, AppDetectivePro uses Windows Management Instrumentation (WMI) technology on certain DISA checks when you Audit a Microsoft SQL Server application on a remote WMI server; for more information, see DISA Check Requirements and Understanding the Connection Details Dialog Box .
--------------	--

- **Authorization.** This Policy is used to Audit permissions and access controls.
- **PCI Data Security Standard.** This Policy is structured following the PCI Data Security Standard and is recommended for use in a compliance assessment.
- **Sarbanes-Oxley.** This policy is structured following CoBIT and ISO 17799 standards and is recommended for use in a Sarbanes-Oxley compliance assessment.
- **Strict.** Provides a maximum level of security with a significant impact on functionality. This Policy is much more restrictive than required by most applications. Usually used by only the most top secret applications.
- **Massachusetts 201 CMR.** Standards for the protection of personal information of residents of the Commonwealth.
- **MiFID.** This Policy is structured for use in a Markets in Financial Instruments Directive (MiFID) compliance assessment.
- **EU Data Protection Directive.** This Policy is structured following EU 95/46/EC standards and is recommend for use in a EU Data Protection Directive compliance assessment.
- **Gramm-Leach-Bliley Act.** This Policy is structured following Gramm-Leach-Bliley Act (GLBA) standards and is recommened for use in a GLBA compliance assessment.
- **HIPAA.** This Policy is structured following NIST standards and best practices for database security and is recommended for use in a HIPAA compliance assessment.

Built-In Pen Test Policies

AppDetectivePro includes the following built-in Pen Test Policies. Built-in Policies **cannot** be modified. However, you can edit a built-in Policy and perform a "save as" to save the edited Policy under a different name. For more information, see [Editing a Policy](#).

- **HIPAA.** This Policy is structured following NIST standards and best practices for database security and is recommended for use in a HIPAA compliance assessment.
- **PCI Data Security Standard.** This Policy is structured following the PCI Data Security Standard and is recommended for use in a compliance assessment.
- **Gramm-Leach-Bliley Act.** This Policy is structured following Gramm-Leach-Bliley Act (GLBA) standards and is recommended for use in a GLBA compliance assessment.
- **Demo.** Runs a demonstration of DbProtect Vulnerability Management features. This demo runs quickly, returning a maximum number of vulnerabilities in a short period of time.
- **Sarbanes-Oxley.** This Policy is structured following CoBIT and ISO 17799 standards and is recommended for use in a Sarbanes-Oxley compliance assessment.
- **Evaluation.** Performs a Penetration Test using basic checks, allowing you to evaluate DbProtect Vulnerability Management.
- **FISMA.** This Policy is structured following NIST standards and is recommended for use in a FISMA compliance assessment.
- **Safe.** Runs safe checks only. This Policy does not perform Brute Force or Denial of Service checks that cannot be run safely.
- **Basel II.** This Policy is structured for use in a Basel II compliance assessment.
- **Full.** Performs a complete Penetration Test of your application using all available checks.
- **EU Data Protection Directive.** This Policy is structured following EU 95/46/EC standards and is recommended for use in a EU Data Protection Directive compliance assessment.
- **Brute Force.** Performs a Penetration Test designed to test the strength of your applications' passwords as well as other mechanisms that may be breached by brute force methods.

- **Heavy.** Performs a detail-level Penetration Test on your applications. Adds a heavy amount of usage. May take more than one hour to run.
- **Download.** A default Policy that allows you to test specific checks.
- **MiFID.** This Policy is structured for use in a Markets in Financial Instruments Directive (MiFID) compliance assessment.
- **Light.** Performs a first-level Penetration Test on your application. Adds a minimal amount of usage. Should take less than one minute to run.
- **Medium.** Performs a second level Penetration Test on an application. Adds a moderate amount of usage on the application. Should take less than 15 minutes to run.
- **Denial of Service.** This Policy checks if your applications are vulnerable to any Denial of Service (DoS) attacks by looking at the version and platform of the database or listener.

Viewing a Policy

AppDetectivePro allows you to view a Policy (for either a Pen Test or an Audit), including what security checks it contains. You can view inactive Policies. For more information, see [Activating/Deactivating a Policy](#).

To view a Policy:

Step	Action
1	Do one of the following: <ul style="list-style-type: none"> • Choose Edit > Policies from the menu bar. • Click the Policy button on the toolbar • Press <CTRL>+L. The Policies dialog box appears.
2	Click the Pen Test Policies or Audit Test Policies tab.
3	Select a Policy.
4	Click the View Policy button. The Policy Editor appears.

Step	Action
5	View which security checks are active within the chosen Policy. (Security checks with check marks next to them are active .) Some Policies have advanced features in the Policy Editor ; for more information, see Advanced Policy Editor Features .
6	Click an individual security check to display its detailed description.

Creating a Policy

AppDetectivePro allows you to create a Policy (for either a Pen Test or an Audit), including what security checks it contains.

To create a Policy:

Step	Action
1	<p>Do one of the following:</p> <ul style="list-style-type: none"> • Choose Edit > Policies from the menu bar. • Click the Policy button on the toolbar. • Press <CTRL>+L. <p>The Policies dialog box appears.</p>
2	Click the Pen Test Policies or Audit Test Policies tab.

Step	Action
3	<p>Click the New Policy button or the Edit Policy button to display the Policy Editor page.</p> <p>If you click the:</p> <ul style="list-style-type: none"> • New Policy button, the Save As button is deactivated, and the Save button is activated • Edit Policy button (for a built-in Policy), the Save As button is activated, and the Save button is deactivated. Optionally, you can select an existing Policy to serve as a template for your new Policy. If you decide to do this, make sure to click the Edit Policy button. Your new Policy automatically inherits the activated checks from the selected template Policy (which you can edit). If you click the New Policy button instead, you will not automatically inherit the activated checks.
4	<p>Activate/deactivate security checks by checking/unchecking the corresponding checkboxes. Some Policies have advanced features in the Policy Editor; for more information, see Advanced Policy Editor Features.</p>
5	<p>Some checks allow you to click an Exceptions button and specify your own dictionary. Do the following:</p> <ul style="list-style-type: none"> • Click the Exceptions button to display the Create Exception pop up. • Click the Save button on the Create Exception pop up to save the exception to the currently-opened Policy (which you may then edit).
6	<p>If you clicked the:</p> <ul style="list-style-type: none"> • New Policy button in Step 3, the Save As button is deactivated, and the Save button is activated. Click the Save button to display the Save New Policy pop-up and go to Step 7. • Edit Policy button (for a built-in Policy) in Step 3, the Save As button is activated, and the Save button is deactivated. Click the Save As button to display the Save New Policy pop-up and go to Step 7.
7	<p>Enter the new Policy name in the Policy Name field (required).</p>
8	<p>Enter the new Policy description in the Policy Description field (optional).</p>

Step	Action
9	Click the OK button. AppDetectivePro saves your new Policy.

Editing a Policy

AppDetectivePro allows you to edit a Policy. Built-in Policies **cannot** be edited. However, you **can** edit a built-in Policy and perform a "save as" to save the edited Policy under a different name.

Step	Action
1	Do one of the following: <ul style="list-style-type: none"> • Choose Edit > Policies from the menu bar. • Click the Policy button on the toolbar. • Press <CTRL>+L. The Policies dialog box appears.
2	Click the Pen Test Policies or Audit Test Policies tab.
3	Select a Policy.
4	Click the View Policy button. The Policy Editor appears.
5	You can activate/deactivate: <ul style="list-style-type: none"> • individual security checks within the chosen Policy by checking/unchecking the checkboxes, respectively • an entire non-built in Policy (including all of its security checks); for more information, see <i>Activating/Deactivating a Policy</i>. Some Policies also have advanced features in the Policy Editor; for more information, see <i>Advanced Policy Editor Features</i>.

Step	Action
6	<p>Some checks allow you to click an Exceptions button and specify your own dictionary. Do the following:</p> <ul style="list-style-type: none"> • Click the Exceptions button to display the Create Exception pop up. • Click the Save button on the Create Exception pop up to save the exception to the currently-opened Policy (which you may then edit).
7	<p>Save the edited Policy. If the Policy is a:</p> <ul style="list-style-type: none"> • non-built-in Policy, then click the Save button to save the edited Policy • built-in Policy, then click the Save As button to save the edited Policy under a different name.

Modifying the Risk Level of Checks Associated With Custom Policies

AppDetectivePro allows you to use the **Policy Editor** to modify the risk level (i.e., **High, Medium, Low, Informational**) of a Penetration Test or Audit security check in association with any custom Policy. AppDetectivePro allows you to modify the risk level of both built-in checks and user-defined checks (for more information, see *User-Defined Checks*). You can only modify the risk levels in checks associated with custom Policies. However, AppDetectivePro allows you to modify the risk levels in checks associated with built-in Policies, then click the **Save As** button in the **Policy Editor** to save a built-in Policy as a custom Policy.

The **Policy Editor** allows you to modify a check's risk level parameters at a highly-granular level. You can specify the risk level for a specific built-in or user-defined check in association with an individual custom (not built-in) **Policy**. (In other words, different risk levels can exist for the **same check** in association with **different Policies**.)

You can also modify the risk level of a check in association with a particular **test type** (i.e., **Penetration Test** or **Audit**), and a particular **application** (for example, **Microsoft SQL Server**).

Example: A **high** risk level is applied only to the **Agent jobs privilege escalation** check for **Penetration Tests** run against **Microsoft SQL Server** using the custom Policy **<MY COMPANY POLICY>**.

To modify the risk level of a check:

Step	Action
1	Do one of the following: <ul style="list-style-type: none"> • Choose Edit > Policies from the menu bar. • Click the Policy button on the toolbar. • Press <CTRL>+L. The Policies dialog box appears.
2	Click the Pen Test Policies or Audit Test Policies tab.
3	Select a Policy (custom or built-in).
4	Click the View Policy button. The Policy Editor appears.
5	Select a check in the right section of the Policy Editor .
6	Use the Risk Level: drop-down to modify the risk level of the built-in or user-defined check selected in Step 5, in association with the selected custom Policy. You can change the risk level to: High, Medium, Low, or Informational). You can only modify the risk level of enabled checks. In other words, if the Check Enabled checkbox is not checked, you cannot modify the risk level of the built-in or user-defined check.
7	Click: <ul style="list-style-type: none"> • Save to save the built-in or user-defined check with the modified risk level (if the associated Policy is a custom Policy). • Save As to save a Policy under a different name (which is especially useful if you want to save a built-in Policy as a custom Policy). • Reset to reset the built-in or user-defined check to its default risk level. <p>Clicking Reset does not save the risk level of the built-in or user-defined check. You must click the Save button to save a check's reset value.</p>

Renaming a Policy

AppDetectivePro allows you to rename a Policy. Built-in and inactive Policies **cannot** be renamed.

To rename a Policy:

Step	Action
1	Do one of the following: <ul style="list-style-type: none">• Choose Edit > Policies from the menu.• Click the Policy button on the toolbar.• Press <CTRL>+L. The Policies dialog box appears.
2	Click the Pen Test Policies or Audit Test Policies tab.
3	Select the Policy you want to rename.
4	Click the Rename button. The Rename button is disabled if you select an inactive Policy. For more information on activating/deactivating Policies, see Activating/Deactivating a Policy . The Rename Policy pop-up appears.
5	Enter the new Policy name.
6	Click the OK button. A pop-up displays and informs you if the rename was successful.
7	Click the OK button.

Importing a Policy

AppDetectivePro allows you to import Policy data from a database. This is useful if you want to transfer Policies between machines.

Note: Imported Policies include any user-defined checks that are part of the Policy. In addition, you can import inactive Policies. For more information, see [Activating/Deactivating a Policy](#).

To import a Policy:

Step	Action
1	<p>Do one of the following:</p> <ul style="list-style-type: none"> • Choose Edit > Policies from the menu bar. • Click the Policy button on the toolbar. • Press <CTRL>+L. <p>The Policies dialog box appears.</p>
2	Click the Import Policy tab.
3	<p>Click the Set Import File button.</p> <p>The Set Import File dialog box appears.</p>
4	Specify the path and file name of the AppDetectivePro database file (.adb).
5	<p>Click the Import button.</p> <p>A pop-up appears, notifying you AppDetectivePro has imported your Policy data as an AppDetectivePro database file (.adb). The imported Policy is now available.</p>

Activating/Deactivating a Policy

AppDetectivePro allows you to activate an inactive Policy and vice-versa. You cannot set inactive Policies as current Pen Testing and Auditing Policies (for more information, see [Specifying the Current Policy for a Pen Test or Audit](#)), nor can you rename inactive Policies (for more information, see [Renaming a Policy](#)).

You can, however, do the following:

- generate a [Policy](#) report on inactive Policies; for more information, see [Reports](#)
- view inactive Policies; for more information, see [Viewing a Policy](#)
- purge inactive Policies; for more information, see [Purging a Policy](#)
- import inactive Policies; for more information, see [Importing a Policy](#).

Note:	Built-in Policies cannot be deactivated. Their status is always active.
--------------	--

The [Policies](#) dialog box includes a [Show inactive policies](#) checkbox. You can check this checkbox to display all inactive Policies. Or, you can uncheck this checkbox to hide all inactive Policies.

To activate an inactive Policy:

Step	Action
1	Do one of the following: <ul style="list-style-type: none"> • Choose Edit > Policies from the menu bar. • Click the Policy button on the toolbar. • Press <CTRL>+L. The Policies dialog box appears.
2	Click the Pen Test Policies or Audit Test Policies tab. The Policies dialog box includes a Show inactive policies checkbox. Make sure you check this checkbox to display all inactive Policies.
3	Highlight the inactive Policy you want to activate.
4	Click the View Policy button. The Policy Editor appears.

Step	Action
5	Click the Activate Policy button.

To deactivate an active Policy:

Step	Action
1	Do one of the following: <ul style="list-style-type: none"> • Choose Edit > Policies from the menu bar. • Click the Policy button on the toolbar. • Press <CTRL>+L. The Policies dialog box appears.
2	Click the Pen Test Policies or Audit Test Policies tab.
3	Highlight the non-built in Policy you want to deactivate.
4	Click the Edit Policy button. The Policy Editor appears.
5	Click the Deactivate Policy button.
6	AppDetectivePro prompts you to confirm that you want to remove (deactivate) the Policy. Click the Yes button. AppDetectivePro deactivates the Policy. The Policies dialog box will not display deactivated Policies if the Show inactive policies checkbox is checked.

Exporting a Policy

AppDetectivePro allows you to export Policy data from a database. This is useful if you want to transfer Policies between machines.

Note: Exported Policies include any user-defined checks that are part of the Policy.

To export a Policy:

Step	Action
1	Do one of the following: <ul style="list-style-type: none"> • Choose Edit > Policies from the menu bar. • Click the Policy button on the toolbar. • Press <CTRL>+L. The Policies dialog box appears.
2	Click the Export/Purge Policy tab.
3	Check the Policies you want to export.
4	Click the Export button. A pop-up appears, notifying you AppDetectivePro has exported your Policy data as an AppDetectivePro database file (.adb). The exported Policy is now available.

Purging a Policy

AppDetectivePro allows you to purge Policy data from a database.

Note: You can purge active/inactive custom Policies, but **not** built-in Policies. For more information, see [Activating/Deactivating a Policy](#).

To purge a Policy:

Step	Action
1	Do one of the following: <ul style="list-style-type: none"> • Choose Edit > Policies from the menu bar. • Click the Policy button on the toolbar. • Press <CTRL>+L. The Policies dialog box appears.
2	Click the Export/Purge Policy tab.
3	Check the Policy you want to purge.
4	Click the Purge button. A pop-up appears, notifying you AppDetectivePro has purged your Policy data from the database.

Searching Policies

AppDetectivePro allows you to search Policies for checks that match a specified criteria. It also allows you to search for specific checks' CVE numbers.

To search Policies:

Step	Action
1	Do one of the following: <ul style="list-style-type: none"> • Choose Edit > Policies from the menu bar. • Click the Policy button on the toolbar. • Press <CTRL>+L. The Policies dialog box appears.
2	Click the Pen Test Policies or Audit Test Policies tab.
3	Select a Policy.

Step	Action
4	Click the New Policy or View Selected button. The Policy Editor appears.
5	Click the Search button in the toolbar. The Policy Search dialog box appears.
6	Enter text to search for. If you have a specific CVE number, enter it as the target string. AppDetectivePro displays your search results in the Policy Search dialog box (sorted by Check Name and Application Type).
7	Click a Policy to display the full Policy (and its checks, on the left) in the Policy Editor .

Specifying the Current Policy for a Pen Test or Audit

AppDetectivePro allows you to specify the current Policy for a Pen Test or Audit. The "current" Policy is your default Policy when you run the associated Pen Test or Audit (although this can be changed).

Note:	You can set two current Policies at once, i.e., one for Pen Testing and one or Auditing. However, you cannot set inactive Policies as current Pen Testing and Auditing Policies (the Set as Current button is grayed-out). For more information on activating/deactivating Policies, see <i>Activating/Deactivating a Policy</i> .
-------	--

To specify the current Policy for a Pen Test or Audit:

Step	Action
1	Do one of the following: <ul style="list-style-type: none"> • Choose Edit > Policies from the menu bar. • Click the Policy button on the toolbar. • Press <CTRL>+L. The Policies dialog box appears.
2	Click the Pen Test Policies or Audit Test Policies tab.
3	Select the Policy that you want to set as your current Pen Test or Audit Policy.
4	Click the Set as Current button. You cannot set inactive Policies as current Pen Testing and Auditing Policies (the Set as Current button is grayed-out). For more information on activating/deactivating Policies, see Activating/Deactivating a Policy. The Policy is set as current for the associated Pen Test or Audit (specified in Step 2). The current Policy is your default Policy when you run the associated Pen Test or Audit (although this can be changed). For more information, see Running a Pen Test and Running an Audit , respectively.

Specifying Exceptions

AppDetectivePro allows you to include check exceptions to any custom, user-created Policies. Check exceptions allow you to exclude parameter value(s) as being flagged as a violation if found during a Pen Test or Audit. This section consists of the following topics:

- [Exception Examples](#)
- [Risk Acceptance](#)
- [Adding an Exception](#)
- [Viewing an Exception](#)
- [Editing an Exception](#)

EXCEPTION EXAMPLES

Exceptions are a way of filtering out possible finding violations at scan time. Applying exceptions will result in these possible finding violations not showing up in the results of the scan. Exceptions are generally applied when running Access Control checks since many of these checks will result in providing a list of all possible access, even if acceptable or required for an application to function.

Below are some examples of Exceptions.

Oracle check "Role granted WITH ADMIN Option“:

- Exception: `Role=DBA`
- This will produce in AppDetectivePro not reporting a violation found for the DBA role.

Oracle check "Easily-guessed database password“:

- Exception: `Username=John`
- This will produce in AppDetectivePro not reporting a violation found for Username: John
- Exceptions: `Username=John` or `Password=12345`
- This will produce in AppDetectivePro not reporting a violation found for Username: John or any username with the password as `'12345'`.

RISK ACCEPTANCE

Since exceptions are suppressing possible finding violations at scan time, it is good security practice to capture information on why exceptions are being applied up front. This is known as Risk Acceptance in AppDetectivePro; meaning that you are accepting any possible risk by suppressing any possible issue at scan time. Adding risk acceptance information for exceptions is optional. Additionally optional, is including the risk acceptance information in a Policy or Vulnerability Details report.

For more information see, Pen Test and Audit ReportsFor more information see, Pen Test and Audit Reports

ADDING AN EXCEPTION

There are two ways to add an exception to a custom, user-created Policy. You can:

- manually create an exception
- load a file of exceptions (from a `.txt` or `.csv` file).

To add an exception:

Step	Action
1	On the Policy Editor , click the enabled check where you want to add an exception.
2	Click the Exceptions button to display the Exceptions dialog box.
3	If you want to: manually create an exception, go to Step 4 load a file of exceptions (from a <code>.txt</code> or <code>.csv</code> file), go to Step 5.

Step	Action
4	<p data-bbox="264 251 699 286">Manually create an exception.</p> <p data-bbox="264 286 1285 355">Click the Add button on the Exceptions dialog box to display the Create Exception pop up, which allows you to add:</p> <p data-bbox="264 399 735 468"><code>exceptions</code> <code>risk acceptance information</code></p> <p data-bbox="264 512 556 546">To add an exception:</p> <ul data-bbox="307 546 1306 1380" style="list-style-type: none"><li data-bbox="307 546 1306 737">• A list of all possible Parameter Names is displayed in the dialog box. Mark the checkbox to the left of each Parameter Name you want included as exceptions and enter value(s) in the Parameter Value field, for example DBA (example for 'Granted To' Parameter Name). You must repeat this step for each Parameter Value you wish to include in the exception<li data-bbox="307 746 464 781">• Click OK.<li data-bbox="307 789 1306 894">• To optionally add risk acceptance information, mark the checkbox for 'Optionally, enter risk acceptance information for the exception.' This will allow you to enter in Risk Acceptance information.<li data-bbox="307 902 1256 980">• Enter in a value in the Creator field, for example Joseph White. This is a mandatory field.<li data-bbox="307 989 1306 1058">• Enter in a value in the Authorizer field, for example James Delaney. This is an optional field.<li data-bbox="307 1067 1306 1180">• Optionally add Name and Value pairs as Change Control fields. Click in the Name field, and enter in a value. Click on the Value field, and enter a value, for example RAC (Name field) and 854 (Value field)<li data-bbox="307 1189 1306 1258">• Mark the checkbox to include an Expiration Date. Change the value to your desired date and time. This is an optional setting.<li data-bbox="307 1267 1306 1336">• Enter in text in Comments field text box. This is an optional field. The Last Updated Date field is auto-generated and not modifiable.<li data-bbox="307 1345 464 1380">• Click OK.

Step	Action
5	<p>Load a file of exceptions (from a .txt or .csv file).</p> <p>Click the Load From File button on the Exceptions dialog box to display the Load Exceptions from file pop up, which allows you to select a valid .txt or .csv file of exceptions.</p> <p>The content of the file, line by line, must adhere to the following syntax and rules:</p> <p>For exceptions only: <ParamName>=<ParamValue></p> <p>Note:</p> <ul style="list-style-type: none"> • <ParamName>: must be an available parameter in the Parameter Names table for the check • <ParamValue>: cannot be empty. <p>for example Granted To=DBA</p> <p>For exceptions and risk acceptance information: <ParamName>=<ParamValue>;Creator=<CreatorValue>,Authorize=<Auth Value>,Comments=<CommentsValue>,Expiration Date=2011-08-30 23:59:22;<ChangeControlName>=<ChangeControlValue></p> <p>Note that:</p> <ul style="list-style-type: none"> • <ParamName>: must be an available parameter in the Parameter Names table for the check • <ParamValue>: cannot be empty. • <CreatorValue>: cannot be empty • Multiple pairs of <ChangeControlName>=<ChangeControlValue> can be added, separated by a comma, for example name1=value1, name2=value2 <p>for example Granted To=DBA;Creator=S. Green,Authorizer=J. Olzewski,Comments=Insert Comments,Expiration Date=2011-12-31 23:59:22;name1=value1,name2=value2</p> <p>Click OK and go to Step 6.</p>

Step	Action
6	Click OK on the Exceptions dialog box.

VIEWING AN EXCEPTION

To view an exception:

Step	Action
1	Click the enabled check where you want to view an exception.
2	Click Exceptions .
3	The Exceptions dialog box will display and you will see a list of Exceptions in a tree view. Click on the '+' sign to expand the details of each exception where applicable. Any exception with a '+' contains risk acceptance information that can be viewed.
4	Click OK to close the Exceptions dialog box.

EDITING AN EXCEPTION

To edit an exception:

Step	Action
1	Click the enabled check where you want to edit an exception.
2	Click the Exceptions button.
3	The Exceptions dialog box will display and you will see a list of Exceptions in a tree view. Click on the exception you want to edit, for example Granted To=DBA
4	Click Edit .

Step	Action
5	This will open the dialog box to edit the existing exception you selected. Edit the exception and click the OK button.
6	Click OK to close the Exceptions dialog box. Your edits will automatically be saved.

DELETING AN EXCEPTION

To delete an exception:

Step	Action
1	Click the enabled check where you want to delete an exception.
2	Click Exceptions .
3	Select the exception you want to delete.
4	Click Delete .
5	Click the Yes button to verify the delete. This will delete the exception and any risk acceptance information you included for the selected exception.
6	Click OK to close the Exceptions dialog box. Your edits will automatically be saved.

Running a Policy Report

AppDetectivePro allows you to run a [Policy Report](#), which provides information about your Policies in an easy-to-read, formatted manner. For more information on AppDetectivePro reports, see Reports.

To run a [Policy Report](#):

Step	Action
1	Do one of the following: <ul style="list-style-type: none"> • Choose View > Reports from the menu bar. • Click the Reports button on the toolbar. The report wizard appears.
2	In the Report Name box, select Policy .
3	Click the Next button. The next page of the report wizard appears.
4	Select the Policy for which you want to generate the Policy Report .
5	Click Next . The next page of the report wizard appears.
6	Verify AppDetectivePro is about to generate the correct report.
7	Click Next . AppDetectivePro generates your Policy Report .

Advanced Policy Editor Features

Some Policies have advanced features in the Policy Editor. This section consists of the following topics:

- [“Logon Hours Validation” Advanced Feature](#)
- [“Audit Trail Location” Advanced Feature](#)
- [“Auditing of Commands” Advanced Feature](#)
- [“Password Checking” Advanced Feature](#)

“LOGON HOURS VALIDATION” ADVANCED FEATURE

The [Logon Hours Validation](#) Audit Policy check (displayed in the [Policy Editor](#) by choosing the [Oracle](#) tab > [Access Control](#) checkbox > [Logon Hours Validation](#) checkbox) includes an advanced feature.

Specifically, you can use the hours/week calendar tool to check *exactly* which days of the week -- and which hours (in military time, 0-23) on those days -- you allow users to log on to your Oracle database. If this check is enabled, and if someone logs on to your Oracle database outside a checked day/hour -- then AppDetectivePro reports the unauthorized logon as a vulnerability when you run an Audit.

"AUDIT TRAIL LOCATION" ADVANCED FEATURE

The [Audit Trail Location](#) Audit Policy check (displayed in the [Policy Editor](#) by choosing the [Oracle](#) tab > [Application Integrity](#) checkbox > [Audit Trail Location](#) checkbox) includes an advanced feature.

Specifically, an Oracle database can write an audit trail for every action performed on the database that you want audited. The [Audit Trail Location](#) advanced feature allows you to ensure the audit trail location is where you intend it to be, i.e., on the [Database](#) or in an [OS Logfile](#). If this check is enabled, and if the audit file is written to the database when you want it to be written to an operating system log file, or vice-versa -- then AppDetectivePro reports the wrong audit file location as a vulnerability when you run an Audit.

"AUDITING OF COMMANDS" ADVANCED FEATURE

The [Auditing of Commands](#) Audit Policy check (displayed in the [Policy Editor](#) by choosing the [Oracle](#) tab > [Application Integrity](#) checkbox > [Auditing of Commands](#) checkbox) includes an advanced feature.

Specifically, you enter any SQL command that you want to flag as a vulnerability when you run an Audit. You can:

- Enter the SQL command in the field at the top of the [Policy Editor](#) when this Audit Policy check is selected.
- Click the [Add](#) button to add the SQL command to the list.
- Check the SQL command(s) you want to Audit.

If this check is enabled, and if someone executes a specified/checked SQL command on your Oracle database -- then AppDetectivePro reports the unauthorized logon as a vulnerability when you run an Audit.

"PASSWORD CHECKING" ADVANCED FEATURE

Some password checks in the [Policy Editor](#) include a [Run check even if it might lock out accounts](#) checkbox. If you disable/uncheck this checkbox, AppDetectivePro will

skip this check and display the message: [Could not run check because accounts may become locked.](#)

If you encounter this error message, and you want to run the password check, you must edit the Policy that includes this check and make sure to check the [Run check even if it might lock out accounts](#) checkbox; for more information on editing a Policy, see [Editing a Policy](#). After you check this option, and run a new Audit or Pen Test, the check should run even though it *may*, potentially, lock out accounts.

Pen Tests, Audits, and User Rights Reviews

This section consists of the following topics:

- [What are Pen Tests, Audits, and User Rights Reviews?](#)
- [Understanding the ASIEngine](#)
- [Pre-Pen Test: Operating System and Database Considerations](#)
- [Running a Pen Test](#)
- [Post-Pen Test](#)
- [Pre-Audit: Operating System and Database Considerations](#)
- [Running an Audit](#)
- [Post-Audit](#)
- [Running a User Rights Review](#)
- [Post-User Rights Review](#)

What are Pen Tests, Audits, and User Rights Reviews?

This section consists of the following topics:

- [What is a Pen Test?](#)
- [What is an Audit?](#)
- [What is a User Rights Review?](#)

WHAT IS A PEN TEST?

A Pen Test assesses the security of your applications by running security checks (based on a Policy you choose). Pen Tests:

- are run from an “outside-in” perspective
- give a good simulation of what a hacker or intruder might try in order to get past your application defenses

- commonly uncover mis-configuration errors in addition to well-known application vulnerabilities.

This section explains how to perform a Pen Test using AppDetectivePro. Pen Tests may only be performed after a new Discovery has been performed or a prior Session has been loaded.

WHAT DOES A PEN TEST DO TO MY SYSTEM?

A Pen Test externally probes your database. Inherent to this activity is anonymous querying of network services for a variety of information. The administrator running AppDetectivePro does not provide a username or password, so nothing is used to actually connect to -- or authenticate to -- your system.

During the course of a Pen Test, AppDetectivePro can run tests which may result in acquiring a valid username and password that attackers can potentially use to authenticate to the application. In such cases, AppDetectivePro performs the authentication in order to gather additional information from the application. It may connect to the database and gather username and password hashes, or configuration values. The Pen Test does not make any updates or changes to your database. It may, however, read data such as the password hashes from the system.

WHAT IS AN AUDIT?

An Audit tests the security of your application using an “inside out” approach. Audits require that you already have access to a system, such as Oracle. The Audit checks your Discovered applications for password configurations, table access, user roles, and other vulnerabilities.

Note:	In order to perform a Security Audit for Lotus Domino, IBM DB2, or Sybase, you must have a working client installed. For more information, see Minimum System Requirements .
--------------	--

WHAT IS A USER RIGHTS REVIEW?

The User Rights Review utility allows you to conduct a comprehensive "inside-out" scan of users, roles, and their privileges within a Discovered, User Rights reviewable database.

Note:	User Rights reviewable applications are currently limited to Discovered Oracle 8i-11g, Microsoft SQL Server 2000, Microsoft SQL Server 2005, Microsoft SQL Server 2008, and Sybase (versions 12.5, 15.0, and 15.5) databases.
--------------	---

Once you have completed a User Rights Review, you can generate User Rights Review Reports -- specifically, an [All Effective Privileges for a User Report](#) and/or an [All Users in a Database Instance Report](#) -- from your scan data. For more information, see [User Rights Review Reports](#).

Understanding the ASIEngine

The **ASIEngine** is a dialog box that displays when you run a Discovery, Pen Test, Audit, or User Rights Review. The **ASIEngine**:

- provides detail about the progress of your particular task(s)
- allows you to pause or **cancel** the task.

The **ASIEngine** consists of the following parts:

- **Status bars.** Two status bars display:
 - The **top** status bar displays the overall progress of the task(s) being performed.
 - The **bottom** status bar displays the progress of the check selected. Whatever application is highlighted in the **Tasks** tab is displayed.

- **Close window when task is done** checkbox. You can:
 - check **Close window when task is done** to close the **ASIEngine** dialog box after the Discovery, Pen Test, Audit, or User Rights Review is complete
 - uncheck **Close window when task is done** to keep the **ASIEngine** dialog box open after the Discovery, Pen Test, Audit, or User Rights Review is complete.
- **Buttons.** You can click the:
 - Pause** button to pause the Discovery, Pen Test, or Audit.
 - Resume** button to resume a paused Discovery, Pen Test, or Audit.
 - Stop** button to cancel the Discovery, Pen Test, Audit, or User Rights Review and close the **ASIEngine**.
 - Close** button to close the **ASIEngine** dialog box. (The **Close** button only displays after the Discovery, Pen Test, Audit, or User Rights Review is complete.)
- **Tabs.** You can click the:
 - Tasks** tab to display the current task being performed. In addition, you can select an application in the **ASIEngine** dialog box to display its status in the bottom status bar (see above).
 - Errors** tab to display any errors that occur while running the Discovery, Pen Test, Audit, or User Rights Review.

Pre-Pen Test: Operating System and Database Considerations

This section consists of the following topics:

- [Prerequisite](#)
- [Warning: Pen Testing Microsoft SQL Server Instances Which Use Named Pipes for Connection NOT Supported](#)
- [Pre-Pen Test: Required Open Ports on Machines Running Microsoft SQL Server](#)

PREREQUISITE

Before running a Pen Test you must create a new Session, or load a previous Session. For more information, see [Creating a Session or Loading a Previous Session](#), respectively. If you want to Pen Test:

- **multiple applications**, you must create/load a Session that contains multiple applications. If no Session is loaded, AppDetectivePro will prompt you to load a previous Session during the Pen Set setup.
- **a single application**, you must create/load a Session that contains only a single application, or you can select only a single application in Step 3 of Pen Testing a Single Application. Also, you must create/load a Session before starting the Pen Test.

WARNING: PEN TESTING MICROSOFT SQL SERVER INSTANCES WHICH USE NAMED PIPES FOR CONNECTION NOT SUPPORTED

AppDetectivePro does not support Pen Testing any Microsoft SQL Server instances which use named pipes for connection.

PRE-PEN TEST: REQUIRED OPEN PORTS ON MACHINES RUNNING MICROSOFT SQL SERVER

In order to run a Pen Test against a Microsoft SQL Server database, certain ports on the machine running Microsoft SQL Server must be open. For more information, see [Open Ports \(on Computers Running Microsoft SQL Server\) Required to Run a Pen Test](#).

Running a Pen Test

This section consists of the following topics:

- [Pen Testing Multiple Applications](#)
- [Pen Testing a Single Application](#)

PEN TESTING MULTIPLE APPLICATIONS

To Pen Test multiple applications:

Step	Action
1	<p>Do one of the following:</p> <ul style="list-style-type: none">• Choose Run > Pen Test from the menu bar.• Click the Pen Test button on the toolbar. <p>If you do not have a Session open, AppDetectivePro prompts you to load a previous Session; for more information, see Loading a Previous Session. The Run Penetration Test dialog box appears.</p>
2	<p>Check the multiple applications you want to Pen Test.</p>
3	<p>Use the Policy to use drop-down to select a Pen Test Policy. The default (or current) Pen Test Policy; for more information, see Specifying the Current Policy for a Pen Test or Audit.</p>
4	<p>Click the Run Pen Test button.</p> <p>Be aware that AppDetectivePro may display warning pop-ups, explaining how the Pen Test may affect your system. You can click OK to continue or Cancel to cancel the Pen Test. (You can check Do not ask me this again to suppress these warnings).</p> <p>The ASISEngine dialog box appears, and the Pen Test runs. You can monitor Pen Test progress on the ASISEngine. You can also pause or stop the Pen Test by clicking the Pause or Stop button, respectively. For more information, see Understanding the ASISEngine.</p>

PEN TESTING A SINGLE APPLICATION

To Pen Test a single application:

Step	Action
1	Load a previous Session, or create a new Session; for more information, see Creating a Session or Loading a Previous Session , respectively.
2	In the network tree view of AppDetectivePro (for more information, see Navigating Page Views), click the + icons to expand the nodes and display all the applications.
3	Right click the application you want to Pen Test. A drop-down list appears.
4	<p>You can Pen Test your application with:</p> <ul style="list-style-type: none"> • the default Pen Test Policy by selecting Pen Test With Policy - <CURRENT> (where <CURRENT> is your default Pen Test Policy); for more information, see Specifying the Current Policy for a Pen Test or Audit • any other Pen Test Policy by choosing Pen Test With... and choosing another Pen Test. <p>The ASIEngine dialog box appears, and the Pen Test runs. You can monitor Pen Test progress on the ASIEngine. You can also pause or stop the Audit by clicking the Pause or Stop button, respectively; for more information, see Understanding the ASIEngine.</p> <p>When the Pen Test is complete, the detected vulnerabilities display in the vulnerability view of the AppDetectivePro main page; for more information, see Understanding the AppDetectivePro Graphical User Interface (GUI).</p>

Post-Pen Test

This section consists of the following topics:

- [This section consists of the following topics:](#)

DISPLAYING THE DESCRIPTION AND DETAILS OF A VULNERABILITY

After running a Pen Test, AppDetectivePro displays information about detected vulnerabilities in the vulnerability view.

To display the description of a vulnerability:

Step	Action
1	Click the vulnerability in the vulnerability view. The vulnerability description displays in the main view (with the Vulnerability Description tab selected). You must click the Vulnerability Description tab if you have a different tab selected.

To display the details of a vulnerability:

Step	Action
1	Double click the vulnerability description in the vulnerability view. The Vulnerability Info pop up displays the vulnerability details.

DISPLAYING, PRINTING, AND SAVING COMPLETED PEN TEST INFORMATION

In the network tree view, yellow magnifying glass icons represent completed Pen Tests.

To display completed Pen Test information:

Step	Action
1	<p>You can click the:</p> <ul style="list-style-type: none"> • + icons to expand tree branches and display completed Pen Tests • - icons to collapse tree branches and hide completed Pen Tests • yellow icon to display the Pen Tested applications. <p>If a Pen Test detects useful account information -- such as valid account information -- then AppDetectivePro displays this information in the main window (Details tab). Account information includes login name and password pairs.</p>
2	<p>You can click the:</p> <ul style="list-style-type: none"> • + icons to expand tree branches and display account information • - icons to collapse tree branches and hide account information.

To print completed Pen Test information:

Step	Action
1	<p>Right click Pen Test of (Application Name), then choose Print Tree. AppDetectivePro prints the branches of the tree you expanded.</p>

To save a completed Pen Test information grid to a file:

Step	Action
1	<p>Right click the grid and choose Export.</p>

Pre-Audit: Operating System and Database Considerations

This section consists of the following topics:

- [Windows OS Audit Check Requirements](#)
- [UNIX OS Audit Check Requirements](#)
- [IBM DB2 z/OS Considerations](#)
- [Running an Audit Using Currently Logged-On Windows User Credentials \(Instead of Oracle Database User Credentials\)](#)
- [DISA Check Requirements](#)
- [Required Open Ports on Machines Running Microsoft SQL Server](#)
- [Manually Setting the Oracle OS Platform Before Running an Audit with OS Checks \(For Oracle 11gR2 Only\)](#)
- [Disabling TCP.VALIDNODE_CHECKING When Auditing an Oracle Target Database](#)

WINDOWS OS AUDIT CHECK REQUIREMENTS

AppDetectivePro performs Windows OS checks via Windows authentication. Make sure the account and computer you are running AppDetectivePro from has the appropriate permissions for the corresponding checks:

- **Not Using NTFS Partition.** Permission to read the installation disk type.
- **Registry Permissions.** Remote registry access.
- **Service Runs as Local System.** Permission to list the system services.
- **Permissions on Files.** Permission to read files in the installation directory of the database.

UNIX OS AUDIT CHECK REQUIREMENTS

AppDetectivePro performs Unix OS checks via a Telnet or SSH account. Your account must have the appropriate read and directory listing permissions activated on the database installation and running directories.

If you run the following checks:

Permissions on Files
Setgid Bit Enabled
Setuid Bit Enabled

Then you must have permission to:

List files in the installation directories of the database.

PROPERLY-CONFIGURED ENVIRONMENT VARIABLES

AppDetectivePro can Audit platforms that use system variables to specify the location of the database instances. In UNIX, you must set the environment variables correctly in order to use SSH or Telnet to access the accounts. Specific requirements follow.

If you want to Audit the following platform:	Then you must:
Oracle	Make sure the <code>\$ORACLE_HOME</code> variable is correct.
Sybase	Make sure the <code>\$SYBASE</code> variable is correct.
MySQL	Define a <code>datadir</code> or <code>basedir</code> variable to point to the database root.

SYBASE AND LOTUS CONSIDERATIONS

When you run an Audit on Lotus or Sybase:

If the OS credentials fail at "Test Connect," your OS platform type may be set to "Unknown." If this is the case, select the correct OS platform from the **OS Platform** drop-down menu in the **Details** tab. After you have set the OS Platform type, try connecting again.

IBM DB2 z/OS CONSIDERATIONS

When you run an Audit with password checks against an IBM DB2 z/OS database, accounts can be locked out. The **Properties** dialog box allows you to select which security option AppDetectivePro should use to authenticate an IBM DB2 z/OS application. You can select:

- **Use authentication value in server's DBM configuration**
- **Client authentication**
- **Server authentication**
- **Server authentication with encryption**
- **DDCS authentication**
- **DDCS authentication with encryption.**

For more information, see Properties.

In addition, you must enable `sysproc.dsnwzp` on your target server or the following IBM DB2 z/OS Audit checks fail:

- **Dual logging not enabled**
- **Audit Trace is not set to start automatically**
- **SMF accounting is not set to start automatically**
- **Dual archiving not enabled**

The `sysproc.dsnwzp` stored procedure is not enabled by default when you install IBM DB2 z/OS, but it should be enabled if you properly performed maintenance hold data actions.

RUNNING AN AUDIT USING CURRENTLY LOGGED-ON WINDOWS USER CREDENTIALS (INSTEAD OF ORACLE DATABASE USER CREDENTIALS)

To perform an audit using currently logged-on Windows user credentials (instead of Oracle database user credentials) make sure:

- your target Oracle server is configured for NTS authentication (check the server file `sqlnet.ora` to verify)
- the local user on AppDetectivePro machine has the same user name and password as the one on the target machine
- the user on remote machine is member of local `ORA_DBA` Windows group (required to connect as `SYSDBA`)
- create file `\network\admin\sqlnet.ora` under AppDetectivePro's installation directory contains the following line: `sqlnet.authentication_services=(NTS)`.

If you have an Oracle client or database installed on your AppDetectivePro machine, make sure the `ORACLE_HOME` environment variable used to start AppDetectivePro points to AppDetective's installation directory so the correct `sqlnet.ora` file is used. To do so, manually unset the `ORACLE_HOME` environment before you launch `AppDetective.exe`.

To use currently logged-on Windows account to run your Audit, leave the **User Name** field empty in the **Connection Details** dialog box.

DISA CHECK REQUIREMENTS

Starting with version 6.0, AppDetectivePro uses Windows Management Instrumentation (WMI) technology on the following DISA checks when you Audit a Microsoft SQL Server application.

- [SQL Server service account user rights](#)
- [SQL Server component service account user rights](#)
- [Integration Services OS account least privileges](#)
- [SQL Server Agent account user rights](#)

Note:	For more information on WMI, see http://msdn.microsoft.com/en-us/library/aa389290(vS.85).aspx .
--------------	--

AppDetectivePro uses WMI to connect to remote WMI servers in order to obtain the service account or group of Microsoft SQL Server services (i.e., the Microsoft SQL Server service, Microsoft SQL Server Agent, Integration Service, Analysis Server, Report Server, Full Text Search and Microsoft SQL Server Browser).

Subsequently, if you are Auditing a Microsoft SQL Server database on a remote WMI server, and you have any of the DISA checks listed above enabled in your Policy, you can do either of the following:

- Enter a valid Windows account user name/password pair in the **User Name** and **Password** fields in the **Operating System Connection** section of the **Connection Details** dialog box. You can enter a user name (i.e., `jsmith`) or a domain \username (`wmiserver-10\jsmith`). The user name should only be valid with connections to **remote** WMI servers. If you enter a user name for a **local** WMI connection, the connection attempt will fail.
- Leave the **User Name** and **Password** fields blank if you want to log in as the currently logged-on user.

In the following scenarios you can leave the **User Name** and **Password** fields blank to log in as the current logged-on Windows user:

- You are **not** Auditing a Microsoft SQL Server database.
- You are Auditing a Microsoft SQL Server database on a remote WMI server on a Windows host, but **none** of the DISA checks listed above are enabled in your Policy.

- You are Auditing a Microsoft SQL Server database on a remote WMI server on a Windows host, and you want to log in as the current logged-on Windows user.
- You are Auditing a Microsoft SQL Server database on a **local** WMI server.

For more information, see [Understanding the Connection Details Dialog Box](#).

REQUIRED OPEN PORTS ON MACHINES RUNNING MICROSOFT SQL SERVER

In order to run an Audit against a Microsoft SQL Server database, certain ports on the machine running Microsoft SQL Server must be open. For more information, see [Open Ports \(on Computers Running Microsoft SQL Server\) Required to Run an Audit](#).

MANUALLY SETTING THE ORACLE OS PLATFORM BEFORE RUNNING AN AUDIT WITH OS CHECKS (FOR ORACLE 11GR2 ONLY)

Changes to the default listener configuration in Oracle 11gR2 make it impossible for AppDetectivePro to determine the OS platform properly. Consequently, you must manually set the OS platform before you can run an Audit with OS checks.

To manually set the Oracle OS platform before running an Audit with OS checks:

Step	Action
1	Run a Discovery; for more information, see Running a Discovery .
2	Select the Discovered Oracle 11gR2 Listener.
3	Click the Details tab in the AppDetectivePro main view.
4	Use the OS Platform: <OS Platform Name> drop-down to select the OS platform where your Discovered Oracle 11gR2 Listener is installed.
5	Unless it's already added, you should manually add Oracle SIDs by right clicking the Oracle listener and selecting Add SID . You can now run an Audit with OS checks against the Oracle SID.

DISABLING TCP.VALIDNODE_CHECKING WHEN AUDITING AN ORACLE TARGET DATABASE

Application Security, Inc. recommends that you disable `TCP.VALIDNODE_CHECKING` in order to Audit an Oracle target database.

However, if you Audit an Oracle 10gR2 target with `TCP.VALIDNODE_CHECKING` enabled, and include the AppDetective host's IP address in the `TCP.INVITED_NODES` list, the Audit will work. Oracle reference: http://download.oracle.com/docs/cd/B19306_01/network.102/b14213/sqlnet.htm.

Running an Audit

AppDetectivePro allows you to run an Audit on:

- multiple applications
- a single application

This section consists of the following topics:

- [Prerequisites](#)
- [Auditing Multiple Applications](#)
- [Auditing a Single Application](#)
- [Understanding the Connection Details Dialog Box](#)
- [Determining Your SSH Private Key Version and Creating OpenSSH Keys](#)
- [Auditing Microsoft SQL Server \(Using Windows Authentication\) Against a Machine on a Different or Untrusted Domain](#)
- [Scanning a Database that is part of an Oracle Real Application Cluster \(RAC\)](#)

PREREQUISITES

In order to Audit Lotus Domino, IBM DB2, or Sybase applications, you must have a working client installed. For more information, see [Minimum System Requirements](#).

AUDITING MULTIPLE APPLICATIONS

To Audit multiple applications:

Step	Action
1	Do one of the following: <ul style="list-style-type: none">• Choose Run > Audit from the menu bar.• Click the Audit button on the toolbar. If you do not have a Session open, AppDetectivePro prompts you to load a previous Session; for more information, see Loading a Previous Session. The Choose Applications to Audit dialog box appears.
2	Check the applications you want to Audit.
3	Click the Audit Applications button. The Run Audit dialog box appears.
4	Use the Policy to use drop-down to select an Audit Policy.

Step	Action
5	<p>Highlight a row of information in the Run Audit dialog box (consisting of an IP Address, Port, Application, and Audit Information, i.e., the application username, password, etc.).</p> <p>If you have:</p> <ul style="list-style-type: none"> • not already run a Pen Test or Audit, then the Connection Details dialog box appears, prompting you to configure connection details about the account which will run the Audit, i.e., user name, password, permissions, port number (if required), etc.; for more information, see Understanding the Connection Details Dialog Box. You can choose not to configure the connection details. • already run a Pen Test or Audit, then AppDetectivePro selects your previous configuration details (displayed in the Audit Information column of the Run Audit dialog box), and a pop-up prompts you to continue with these settings. <p>You can click the:</p> <ul style="list-style-type: none"> • Yes button to continue with these settings • No button to close the pop-up. <p>Then, click the Change Info button to display the Connection Details dialog box.</p> <p>Then, re-configure connection details about the account which will run the Audit, i.e., user name, password, permissions, port number (if required), etc.; for more information, see Understanding the Connection Details Dialog Box.</p> <p>Starting with version 6.0, AppDetectivePro uses Windows Management Instrumentation (WMI) technology on certain DISA checks when you Audit a Microsoft SQL Server application on a remote WMI server; for more information, see DISA Check Requirements and Understanding the Connection Details Dialog Box.</p>

Step	Action
6	<p>Click the Run Audit button.</p> <p>A pop up notifies you if you did not enter a username or password (in Step 5) for some of the applications you are Auditing. Click the Yes button to continue with the current settings, or click the No button and go back to Step 5 to configure connection details.</p> <p>The ASIShield dialog box appears, and the Audit runs. You can monitor Audit progress on the ASIShield. You can also pause or stop the Audit by clicking the Pause or Stop button, respectively. For more information, see Understanding the ASIShield.</p>
7	<p>When the Audit is complete, the detected vulnerabilities display in the vulnerability view of the AppDetectivePro main page; for more information, see Understanding the AppDetectivePro Graphical User Interface (GUI).</p>

AUDITING A SINGLE APPLICATION

To Audit a single application:

Step	Action
1	<p>Load a previous Session, or create a new Session; for more information, see Creating a Session or Loading a Previous Session, respectively.</p>
2	<p>In the network tree view of AppDetectivePro (for more information, see Navigating Page Views), click the + icons to expand the nodes and display all the applications.</p>
3	<p>Right click the application you want to Audit.</p> <p>A drop-down list appears.</p>

Step	Action
4	<p>You can Audit your application with:</p> <ul style="list-style-type: none">• the default Audit Policy by selecting Audit With Policy - <CURRENT> (where <CURRENT> is your default Audit Policy); for more information, see Specifying the Current Policy for a Pen Test or Audit• any other Audit Policy by choosing Audit With... and choosing another Audit. <p>The Run Audit dialog box appears.</p>
5	<p>Use from the Policy to use drop-down if you want to change the Audit Policy.</p>

Step	Action
6	<p>Highlight a row of information in the Run Audit dialog box (consisting of an IP Address, Port, Application, and Audit Information, i.e., the application username, password, etc.).</p> <p>If you have:</p> <ul style="list-style-type: none"> • not already run a Pen Test or Audit, then the Connection Details dialog box appears, prompting you to configure connection details about the account which will run the Audit, i.e., user name, password, permissions, port number (if required), etc.; for more information, see Understanding the Connection Details Dialog Box. You can choose not to configure the connection details. • already run a Pen Test or Audit, then AppDetectivePro selects your previous configuration details (displayed in the Audit Information column of the Run Audit dialog box), and a pop-up prompts you to continue with these settings. <p>You can click the:</p> <ul style="list-style-type: none"> • Yes button to continue with these settings • No button to close the pop-up. <p>Then, click the Change Info button to display the Connection Details dialog box.</p> <p>Then, re-configure connection details about the account which will run the Audit, i.e., user name, password, permissions, port number (if required), etc.; for more information, see Understanding the Connection Details Dialog Box.</p> <p>Starting with version 6.0, AppDetectivePro uses Windows Management Instrumentation (WMI) technology on certain DISA checks when you Audit a Microsoft SQL Server application on a remote WMI server; for more information, see DISA Check Requirements and Understanding the Connection Details Dialog Box.</p>

Step	Action
7	<p>Click the Run Audit button.</p> <p>A pop up notifies you if you did not enter a username or password (in Step 6) for some of the applications you are Auditing. Click the Yes button to continue with the current settings, or click the No button and go back to Step 6 to configure connection details.</p> <p>The ASIEngine dialog box appears, and the Audit runs. You can monitor Audit progress on the ASIEngine. You can also pause or stop the Audit by clicking the Pause or Stop button, respectively. For more information, see Understanding the ASIEngine.</p>
8	<p>When the Audit is complete, the detected vulnerabilities display in the vulnerability view of the AppDetectivePro main page; for more information, see Understanding the AppDetectivePro Graphical User Interface (GUI).</p>

UNDERSTANDING THE **CONNECTION DETAILS** DIALOG BOX

You can display the [Connection Details](#) dialog box when you Audit either a single or multiple applications. The [Connection Details](#) dialog box allows you to configure connection details about the account which will run the Audit, for example, user name, password, permissions, port number (if required), etc.

The [Connection Details](#) dialog box consists of the two section: [Database Connection](#) and [Operating System Connection](#).

The [Database Connection](#) section of the [Connection Details](#) dialog box consists of the:

- **User Name** field, which allows you to enter your database audit account user name.
- **Password** field, which allows you to enter your database audit account password.
- **Privileges** drop-down, which -- depending on your database type -- allows you to select the privilege associated with your database audit account.

Note:	You can click the Test DB Connect button to test the connection between AppDetectivePro and your host database.
--------------	--

The appearance of the [Operating System Connection](#) section of the [Connection Details](#) dialog box depends on whether the database you are Auditing is installed on Unix or Windows.

On Unix:

If the database you are Auditing is installed on Unix, the [Operating System Connection](#) section of the [Connection Details](#) dialog box allows you to do the following:

- Use the [SSH/Telnet](#) drop-down to select [SSH](#) or [Telnet](#).
- Enter the port number of your SSH/Telnet service in the [SSH/Telnet port](#) field.
- Check the [Use the application user name and password for operating system](#) checkbox to instruct AppDetectivePro to use the user name and password entered above.
- Enter your Unix operating system audit account information in the [SSH/Telnet account](#) field,
- Enter your operating system audit password in the [SSH/Telnet password](#) field.
- Enter your SSH private key file or private key string in the [SSH Private Key](#) field. You can, optionally, copy/paste a private key in its entirety into this field. You can click the [Browse](#) button to select a different SSH private key. The SSH private key is the half of the key pair that you keep on your computer. The public key is the part that you upload to the remote server. For more information on how the SSH Private Key works with AppDetectivePro, see [Determining Your SSH Private Key Version and Creating OpenSSH Keys](#).
- Click the [Test Login](#) button to test your connection and login to the server's Unix operating system for Telnet and SSH connections. The connection timeout (specified below) affects the test login differently for Telnet and SSH, due to the protocols used. For Telnet, the connection timeout is the *maximum time* AppDetectivePro will wait for a response. For SSH, the connection timeout specifies how much time AppDetectivePro will wait for a response before assuming the received response contains a full prompt, which AppDetectivePro uses for the test login.
- Enter a pass phrase for your password-protected private key in the [Pass Phrase](#) field.
- Use the [Cipher Type](#) drop-down to select the supported [RSA](#) or [DSA](#) cipher type.

- Enter the Telnet/SSH connection time out interval (in seconds) in the **Connection Time Out** field. The connection timeout affects the test login differently for Telnet and SSH, due to the protocols used; see above. You set the default value in the **Pen Testing/Auditing** branch of the **Properties** dialog box; for more information, see Understanding the Properties Branches.
- Enter the Session prompt in the **Session Prompt** field, i.e., the prompt AppDetectivePro should use when connecting via Telnet/SSH (rather than relying on AppDetectivePro to locate the Session prompt automatically in the login banner after connecting). For more information, see Appendix S: Dynamic Shell Prompt Handling.

On Windows:

Starting with version 6.0, AppDetectivePro uses Windows Management Instrumentation (WMI) technology on the following DISA checks when you Audit a Microsoft SQL Server application.

- **SQL Server service account user rights**
- **SQL Server component service account user rights**
- **Integration Services OS account least privileges**
- **SQL Server Agent account user rights**

Note:	For more information on WMI, see http://msdn.microsoft.com/en-us/library/aa389290(vb.85).aspx .
--------------	--

AppDetectivePro uses WMI to connect to remote WMI servers in order to obtain the service account or group of Microsoft SQL Server services (i.e., the Microsoft SQL Server service, Microsoft SQL Server Agent, Integration Service, Analysis Server, Report Server, Full Text Search and Microsoft SQL Server Browser).

Subsequently, if you are Auditing a Microsoft SQL Server database on a remote WMI server, and you have any of the DISA checks listed above enabled in your Policy, you can do either of the following:

- Enter a valid Windows account user name/password pair in the **User Name** and **Password** fields in the **Operating System Connection** section of the **Connection Details** dialog box. You can enter a user name (i.e., `jsmith`) or a domain \username (`wmiserver-10\jsmith`). The user name should only be valid

with connections to **remote** WMI servers. If you enter a user name for a **local** WMI connection, the connection attempt will fail. When you are done, click the **Test Login** button to test your connection and login to the remote WMI server.

- Leave the **User Name** and **Password** fields blank if you want to log in as the currently logged-on user. Click the **Test Login** button to test your connection and login to the remote WMI server.

In the following scenarios you can leave the **User Name** and **Password** fields blank to log in as the current logged-on Windows user:

- You are **not** Auditing a Microsoft SQL Server database.
- You are Auditing a Microsoft SQL Server database on a remote WMI server on a Windows host, but **none** of the DISA checks listed above are enabled in your Policy.
- You are Auditing a Microsoft SQL Server database on a remote WMI server on a Windows host, and you want to log in as the current logged-on Windows user.
- You are Auditing a Microsoft SQL Server database on a **local** WMI server.

DETERMINING YOUR SSH PRIVATE KEY VERSION AND CREATING OPENSSH KEYS

AppDetectivePro only supports OpenSSH SSH2 RSA encrypted keys, without a pass phrase. Complete the following steps to determine your SSH version and protocol, and create an OpenSSH key pair:

Step	Action
1	<p>To run the Windows telnet program, enter the following at the command prompt:</p> <pre>C:\>telnet <server> 22 SSH_1.99 OpenSSH_3.5p1</pre>
2	<p>Login with the user account you intend to create the public/private key connection. At the prompt, enter the following command:</p> <pre>>ssh-keygen -t rsa</pre> <p>This action creates an SSH2 pair of key using RSA encryption in the <code>\$HOME/.ssh</code> directory. By default the names are: <code>id_rsa</code> (private key) <code>id_rsa.pub</code> (public key).</p>

Step	Action
3	You may have to rename the public key to: <code>\$HOME/.ssh/authorized_keys2</code> . To do so, copy the private to the machine running AppDetectivePro and store it in a text file.

AUDITING MICROSOFT SQL SERVER (USING WINDOWS AUTHENTICATION) AGAINST A MACHINE ON A DIFFERENT OR UNTRUSTED DOMAIN

If you attempt to Audit a Microsoft SQL Server database (using Windows Authentication) against a machine on a different or untrusted domain, the following error message may display:

```
SQLSTATE: 28000, Native error: 18452, Message: [Microsoft][ODBC SQL Server Driver][SQL Server]Login failed for user ''. The user is not associated with a trusted SQL Server connection..
```

To Audit a Microsoft SQL Server database (using Windows Authentication) against a machine on a different or untrusted domain:

Step	Action
1	Establish a connection to the target server. Enter the appropriate <code>net use</code> syntax. For a remote host that is a: <ul style="list-style-type: none"> • member of domain, enter: <code>net use \\ip /user:domain\username</code> • workgroup member (standalone computer), enter: <code>net use \\ip /user:username</code> or <code>net use \\ip /user:computername\username</code>

Step	Action
2	<p>Use named pipes to connect to an untrusted domain. Select the Properties branch option Connect to Microsoft SQL Servers via Named Pipes. You must check this option when Auditing a Microsoft SQL Server database in an untrusted domain. For more information on:</p> <ul style="list-style-type: none">• displaying the Properties branch, see Displaying the Properties Branches• the Properties branch options, see Understanding the Properties Branches <p>You must enable the named pipes protocol on <i>both</i> the AppDetectivePro host and the Microsoft SQL Server target server when using this option.</p> <p>AppDetectivePro does not support Pen Testing any Microsoft SQL Server instances which use named pipes for connection.</p>
3	<p>Make sure of the following:</p> <ul style="list-style-type: none">• That the Server and Remote Registry services on your remote host are running• That the net use set of credentials file being used is a member of either the domain hosting the target server, or a domain that is trusted by that domain• The login provides remote registry access and read-only file access to the remote machine. To check this, do the following:<ul style="list-style-type: none">-Enter net use \\server with your credentials, and expand HKEY_LOCAL_MACHINE on the target server.-Enter net use \\server\c\$ to verify you can access files on the target server.• That access to the remote host can be restricted by firewall, which is common on Windows 2003/XP/Vista. You can verify this on the remote host by looking into the firewall settings/logs for rejects packets. This means there should be connectivity on port 445 or 139 on the target host.

Step	Action
4	<p>Do the following to create and test a DSN connection to the target host:</p> <ul style="list-style-type: none"> • Choose Control Panel > Administrative Tools > Data Sources (ODBC). • Open the System DSN tab and click the Add button. • Choose Microsoft SQL Server from the list. • Click the Finish button. • Enter a Name and Description for this data source entry. • In the Server field, enter the IP address and listening port of the target server, for example, <code>172.27.190.58,1756</code>. • Click the Next button. • Select SQL Server Authentication and enter your database credentials in the Login ID and Password fields. • Click the Next button. • Follow the steps in the wizard. <p>You should be able to test the connection to the data source. If this test is successful, you should also be able to perform the Audit with AppDetectivePro. If you are unable to connect, try using the other IP address, or use Windows Authentication rather than the SQL credentials (after connecting with Net Use). If you test the operating system connection, then you must run the <code>net use</code> command after testing the connection (even if it was executed already).</p>

SCANNING A DATABASE THAT IS PART OF AN ORACLE REAL APPLICATION CLUSTER (RAC)

An Oracle Real Application Cluster (RAC) allows multiple computers to run Oracle RDBMS software simultaneously while accessing a single database, thus providing a clustered database. In an Oracle RAC environment, two or more computers (each with an instance) concurrently access a single database. This allows an application or user to connect to either computer and have access to a single coordinated set of data.

For example, imagine a two-node RAC setup. This RAC consists of two computers, ORA1 and ORA2, with corresponding instances DEVB1 and DEVB2 (which access a single database, DEVB). For each node, there is a public IP Address and a virtual IP Address. The database can be accessed from any public IP or virtual IP.

By supplying any public IP or virtual IP, the AppDetectivePro Scan Engine should find the Oracle listener, and possibly the instance(s). If the instance(s) are not detected, you must manually add Oracle SIDs to any listener tree. For details, see [Adding an Oracle SID](#).

Post-Audit

This section consists of the following topics:

- Displaying the Description and Details of a Vulnerability
- Displaying, Printing, and Saving Completed Audit Information
- Generating Fix Scripts.

DISPLAYING THE DESCRIPTION AND DETAILS OF A VULNERABILITY

After running an Audit, AppDetectivePro displays information about detected vulnerabilities in the vulnerability view.

To display the description of a given vulnerability:

Step	Action
1	Click the vulnerability in the vulnerability view. The vulnerability description displays in the main view (Vulnerability Description tab).

To display the details of a given vulnerability:

Step	Action
1	Click the vulnerability description in the vulnerability view (Vulnerability Description tab). The Vulnerability Info pop up displays the vulnerability details.

DISPLAYING, PRINTING, AND SAVING COMPLETED AUDIT INFORMATION

In the network tree view, yellow magnifying glass icons represent completed Audits.

To display completed Audit information:

Step	Action
1	<p>You can click the:</p> <ul style="list-style-type: none"> • + icons to expand tree branches and display completed Audits • - icons to collapse tree branches and hide completed Audits • application icon to display the Audited applications. <p>If an Audit detects useful account information -- such as valid account information -- then AppDetectivePro displays this information in the main window (Details tab). Account information includes login name and password pairs.</p>
2	<p>You can click the:</p> <ul style="list-style-type: none"> • + icons to expand tree branches and display account information • - icons to collapse tree branches and hide account information.

To print completed Audit information:

Step	Action
1	<p>Right click Audit of (Application Name) and choose Print Tree. AppDetectivePro prints the branches of the tree you expanded.</p>

To save a completed Audit information grid to a file:

Step	Action
1	<p>Right click the grid and choose Export.</p>

GENERATING FIX SCRIPTS

In addition, the Fix Scripts utility generates SQL scripts designed to correct misconfigurations and address vulnerabilities identified by AppDetectivePro during an Audit. The Fix Scripts utility allows you to:

- review a Fix Script

- customize the Fix Script
- voluntarily (not automatically) deploy the Fix Script on to your database.

For more information, see [Generating a Fix Script](#).

Running a User Rights Review

The User Rights Review utility allows you to conduct a comprehensive "inside-out" scan of users, roles, and their privileges within a Discovered, User Rights reviewable database.

Note:	User Rights reviewable applications are currently limited to Discovered Oracle 8i-11g, Microsoft SQL Server 2000, Microsoft SQL Server 2005, and Microsoft SQL Server 2008 databases.
--------------	---

Once you have completed a User Rights Review, you can generate User Rights Review Reports -- specifically, an [All Effective Privileges for a User Report](#), [All Users in a Database Instance Report](#), and/or an [All Effective Members of a Role](#) ---- from your scan data. For more information, see [User Rights Review Reports](#).

AppDetectivePro allows you to a User Rights Review against:

- multiple applications
- a single application.

Note:	Currently, AppDetectivePro does not allow you to re-use connection information if a User Rights Review was already run once. In other words, you must re-enter connection information every time you run a User Rights Review.
--------------	---

This section consists of the following topics:

- [Running a User Rights Review Against Multiple Applications](#)
- [Running a User Rights Review Against a Single Application](#)
- [Understanding the Connection Details Dialog Box](#).

RUNNING A USER RIGHTS REVIEW AGAINST MULTIPLE APPLICATIONS

To run a User Rights Review against multiple applications:

Step	Action
1	<p>Do one of the following:</p> <ul style="list-style-type: none">• Choose Run > User Rights from the menu bar.• Click the User Rights button on the toolbar. If you do not have a Session open, AppDetectivePro prompts you to load a previous Session; for more information, see Loading a Previous Session. <p>The Choose Applications to Run User Review Rights On dialog box appears.</p>
2	<p>The Choose Applications to Run User Review Rights On dialog box allows you to select multiple User Rights reviewable applications. User Rights reviewable applications are currently limited to Discovered Oracle 8i-11g, Microsoft SQL Server 2000, Microsoft SQL Server 2005, and Microsoft SQL Server 2008 databases.</p>
3	<p>Click the Run Review button.</p>

Step	Action
4	<p>The Run User Entitlement Review dialog box appears.</p> <p>Highlight a row of information in the Run User Entitlement Review dialog box (consisting of an IP Address, Port, Application, and User Rights Review Parameters, i.e., the application username, password, etc.).</p> <p>You can click the Change Info button to display the Connection Details dialog box appears, which allows you to configure connection details about the account which will run the User Rights Review, i.e., user name, password, permissions, port number (if required), etc.</p> <p>Currently, AppDetectivePro does not allow you to re-use connection information if a User Rights Review was already run once. In other words, you must re-enter connection information every time you run a User Rights Review.</p> <p>You can also click the Test DB Connect button (on the Connection Details dialog box) to test whether the specified credentials have the proper privileges to perform a User Rights Review. If the credentials specified do not have the proper privileges to perform a User Rights Review, AppDetectivePro displays a list of tables and stored procedures it needs access to.</p>
5	<p>Click the Run Review button.</p> <p>A pop up notifies you if you did not enter a username or password (in Step 4) for some of your selected User Rights reviewable applications.</p> <p>Click the:</p> <ul style="list-style-type: none">• Yes button to continue with the current settings• No button and go back to Step 4 to configure connection details. <p>The ASISEngine dialog box appears, and the User Rights Review runs. You can monitor Audit progress on the ASISEngine. You can stop the User Rights Review by clicking Stop button. For more information, see Understanding the ASISEngine.</p>

RUNNING A USER RIGHTS REVIEW AGAINST A SINGLE APPLICATION

To run a User Rights Review against a single application:

Step	Action
1	Load a previous Session, or create a new Session; for more information, see Creating a Session or Loading a Previous Session , respectively.
2	In the network tree view of AppDetectivePro, click the + icons to expand the nodes and display all the applications.
3	Right click a User Rights reviewable application and select User Rights Review... User Rights reviewable applications are currently limited to Discovered Oracle 8i-11g, Microsoft SQL Server 2000, Microsoft SQL Server 2005, and Microsoft SQL Server 2008 databases.

Step	Action
4	<p>The Run User Entitlement Review dialog box appears.</p> <p>Highlight a row of information in the Run User Entitlement Review dialog box (consisting of an IP Address, Port, Application, and User Rights Review Parameters, i.e., the application username, password, etc.).</p> <p>You can click the Change Info button to display the Connection Details dialog box appears, which allows you to configure connection details about the account which will run the User Rights Review, i.e., user name, password, permissions, port number (if required), etc.</p> <p>Currently, AppDetectivePro does not allow you to re-use connection information if a User Rights Review was already run once. In other words, you must re-enter connection information every time you run a User Rights Review.</p> <p>You can also click the Test DB Connect button (on the Connection Details dialog box) to test whether the specified credentials have the proper privileges to perform a User Rights Review. If the credentials specified do not have the proper privileges to perform a User Rights Review, AppDetectivePro displays a list of tables and stored procedures it needs access to.</p>
5	<p>Click the Run Review button.</p> <p>A pop up notifies you if you did not enter a username or password (in Step 4) for some of your selected User Rights reviewable applications.</p> <p>Click the:</p> <ul style="list-style-type: none"> • Yes button to continue with the current settings • No button and go back to Step 4 to configure connection details. <p>The ASISengine dialog box appears, and the User Rights Review runs. You can monitor Audit progress on the ASISengine. You can stop the User Rights Review by clicking Stop button. For more information, see Understanding the ASISengine.</p>

UNDERSTANDING THE **CONNECTION DETAILS** DIALOG BOX

You can display the **Connection Details** dialog box when you run a User Rights Review against either a single or multiple applications. The **Connection Details** dialog box allows you to configure connection details about the account which will run the User Rights Review, for example, user name, password, permissions, port number (if required), etc.

The **Connection Details** dialog box consists of the following parts:

- **User Name** field, which allows you to enter your database audit account user name.
- **Password** field, which allows you to enter your database audit account password.
- **Privileges** drop-down, which -- depending on your database type -- allows you to select the privilege associated with your database audit account.

Note:	You can click the Test DB Connect button to test the connection between AppDetectivePro and your host database.
--------------	--

Post-User Rights Review

After you run a User Rights Review, AppDetectivePro allows you to review high-level scan data, such as database parameters, number of users, number of roles, etc.

Note:	Application Security, Inc. recommends you generate User Rights Review reports (upon completion of a review) in order to better assess the resulting scan data of users, roles, and their privileges within your reviewed databases. For more information, see User Rights Review Reports.
--------------	---

In the network tree view, yellow magnifying glass icons represent completed User Rights Reviews.

To display completed User Rights Review information:

Step	Action
1	Click the completed User Rights Review yellow magnifying glass icon in the network view. User Rights Review scan data displays in the main view (Details tab).
2	The main view displays high-level scan data, such as database parameters, number of users, number of roles. In the main view, you can click the: <ul style="list-style-type: none">• + icons in the main view to expand tree branches and display completed User Rights Review scan data• - icons to collapse tree branches and hide data.

Interviews, Questionnaires, and Work Plans

This section consists of the following topics:

- [Understanding Interviews, Questionnaires, and Work Plans](#)
- [Built-In Questionnaires and Built-In Work Plans](#)
- [Displaying and Understanding the Questionnaire Editor](#)
- [Displaying and Understanding the Work Plan Manager](#)
- [Displaying and Understanding the Interview Tool](#)
- [Interview Work Flow](#)
- [Interview Work Flow Step 1: Running a Discovery](#)
- [Interview Work Flow Step 2: Importing a Built-In Questionnaire/Creating a Custom Questionnaire](#)
- [Interview Work Flow Step 3: Running an Audit](#)
- [Interview Work Flow Step 4: Conducting the Interview](#)
- [Interview Work Flow Step 5: Generating an Interview Questionnaire Report](#)
- [Viewing the Results of a Completed Interview](#)
- [Copying a Completed Interview](#)
- [Purging an Interview](#)
- [Working with Questionnaire Types](#)
- [Deleting a Questionnaire](#)
- [Creating a Work Plan](#)

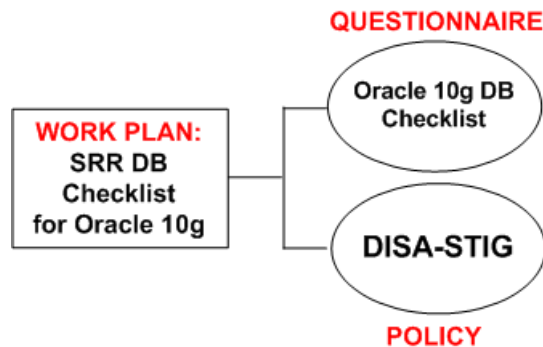
- [Editing a Work Plan](#)
- [Activating/Inactivating a Work Plan](#)
- [Deleting a Work Plan](#)
- [Interview Troubleshooting](#)

Understanding Interviews, Questionnaires, and Work Plans

AppDetectivePro allows you to conduct Interviews using questions derived from Questionnaires and data derived from completed Audits that use a compatible Audit Policy.

AppDetectivePro maps Audit check result data to certain questions (known as Check Associated Questions) in order to support Questionnaire responses with solid evidence. AppDetectivePro supports the use of the Built-in DISA-STIG Questionnaires and custom created Questionnaires; for more information, see Built-In Questionnaires and Built-In Work Plans.

Before you conduct an Interview, you must generate Audit result data for all checks associated with the Questionnaire. As noted earlier, AppDetectivePro uses this Audit data to support Questionnaire responses. In order to generate Audit result data for all checks associated with a Questionnaire, you must run an Audit using a compatible Audit Policy, which contains, at a minimum, all checks associated with the Questionnaire. Using a compatible Audit Policy ensures that your Questionnaire is populated with matching check results during the Interview. Questionnaires and compatible Audit Policies are unified in AppDetectivePro under a feature called a Work Plan.



Specifically, every Work Plan consists of:

- a **Questionnaire**
- one or more compatible Audit Policies (each of which can be used to Audit a target database in order to obtain Audit check result data for all checks associated with a Questionnaire).

After you run an Audit, AppDetectivePro maps the Audit result data to the checks in the associated Questionnaire questions. The mapped Audit check result data displays as part of the question information during the Interview. These Audit check result data provides support data for the Questionnaire responses, if applicable to the specific question. During the Interview, you respond to the questions in a Questionnaire. Once the Interview is finished, you can generate a report that contains Interview responses, applicable Audit check results, and other information; for more information, see Interview Work Flow Step 5: Generating an Interview Questionnaire Report.

Built-In Questionnaires and Built-In Work Plans

AppDetectivePro come with pre-configured built-in DISA-STIG Questionnaires and built-in Work Plans associated with these Questionnaires. Questionnaires are in XML format, as explained in the table below. AppDetectivePro automatically imports a built-in Work Plan (defined in the Questionnaire XML file) when you import a built-in Questionnaire.

You can also create a Questionnaire; for more information, see [Interview Work Flow Step 2: Importing a Built-In Questionnaire/Creating a Custom Questionnaire](#).

The built-in Questionnaires are located, by default, in the following location:
<installation folder>\AppSecInc\AppDetective\Questionnaire\Import.

After update to AppDetectivePro 7.2, the already imported questionnaires are not removed from AppDetective database but old Questionnaire xml files get deleted to only allow importing new/updated Questionnaires. User can decide if to continue using old Questionnaires or clean them up by deleting them from the system.

DISA-STIG Questionnaire source data is derived from the Database Security Checklist published by the Defense Information System Agency (DISA) Field Security Office (FSO), which is frequently updated based on the release of new checklists from DISA FSO.

The following table lists:

- each built-in Questionnaire
- a brief description of the built-in Questionnaire
- its compatible Audit Policy
- its compatible built-in Work Plan.

Currently, these built-in Questionnaires are only available for Microsoft SQL Server and Oracle databases.

The **ASI Security Compliance Workplan** listed below is a general Questionnaire XML import example file. It is **not** database-specific.

Built-In Questionnaire	Description.	Compatible Audit Policy	Compatible Built-In Work Plan
Sample Questionnaire for AppDetectivePro	A sample Questionnaire	Download Audit	ASI Security Compliance Workplan
SQL Server 9 INS Checklist	The DISA STIG checklist for Microsoft SQL Server 2005 installations.	DISA-STIG Database Security - Audit	SRR INS Checklist for SQL Server 9
SQL Server 8 INS Checklist	The DISA STIG checklist for Microsoft SQL Server 2000 installations.	DISA-STIG Database Security - Audit	SRR INS Checklist for SQL Server 8
Oracle 11g INS Checklist	The DISA STIG checklist for Oracle 11g installations.	DISA-STIG Database Security - Audit	SRR INS Checklist for Oracle 11g
Oracle 10g INS Checklist	The DISA STIG checklist for Oracle 10g installations.	DISA-STIG Database Security - Audit	SRR INS Checklist for Oracle 10g

Built-In Questionnaire	Description.	Compatible Audit Policy	Compatible Built-In Work Plan
Oracle 9i INS Checklist	The DISA STIG checklist for Oracle 9i installations.	DISA-STIG Database Security - Audit	SRR INS Checklist for Oracle 9i
SQL Server 9 DB Checklist	The DISA STIG checklist for the Microsoft SQL Server 2005 database.	DISA-STIG Database Security - Audit	SRR DB Checklist for SQL Server 9
SQL Server 8 DB Checklist	The DISA STIG checklist for the Microsoft SQL Server 2000 database.	DISA-STIG Database Security - Audit	SRR DB Checklist for SQL Server 8
Oracle 11g DB Checklist	The DISA STIG checklist for the Oracle 11g database.	DISA-STIG Database Security - Audit	SRR DB Checklist for Oracle 11g
Oracle 10g DB Checklist	The DISA STIG checklist for the Oracle 10g database.	DISA-STIG Database Security - Audit	SRR DB Checklist for Oracle 10g
Oracle 9i DB Checklist	The DISA STIG checklist for the Oracle 9i database.	DISA-STIG Database Security - Audit	SRR DB Checklist for Oracle 9i

Displaying and Understanding the Questionnaire Editor

Questionnaires contain the actual Interview questions themselves. Without a Questionnaire, you cannot conduct an Interview. The [Questionnaire Editor](#) allows you to view all Questionnaires, Questionnaire details, and individual Questionnaire questions.

AppDetectivePro comes pre-configured with some built-in Questionnaires, and associated built-in Work Plans (which contain a compatible Audit Policy for the built-in Questionnaire). AppDetectivePro uses the compatible Audit Policy during an Audit to obtain check result data (which is used to support responses during the Interview). For more information on built-in Questionnaires and compatible Audit Policies, see Built-In Questionnaires and Built-In Work Plans.

Note:	Starting in version 7.2, AppDetectivePro also allows you to create a custom Questionnaire; for more information, see Interview Work Flow Step 2: Importing a Built-In Questionnaire/Creating a Custom Questionnaire.
--------------	--

To display the [Questionnaire Editor](#):

Step	Action
1	Do one of the following: <ul style="list-style-type: none"> Choose Edit > Questionnaire from the main AppDetectivePro menu bar. Choose an available Work Plan from the left-side column of the Work Plan Manager, then select the Questionnaire and click on the blue right arrow to view; for more information, see Displaying and Understanding the Work Plan Manager.

The following table describes the components of the [Questionnaire Editor](#):

Component	Questionnaire Editor Location	Description
Questionnaire/question node	Left	This portion of the Questionnaire Editor displays: <ul style="list-style-type: none"> all Questionnaires

Component	Questionnaire Editor Location	Description
Questionnaire	Top right	<p>This portion of the Questionnaire Editor displays detailed information about the Questionnaire. Specifically, it consists of the following fields:</p> <ul style="list-style-type: none"> • Name, i.e., the name of the Questionnaire selected in the Questionnaire/question node. • Description, i.e., a description of the Questionnaire selected in the Questionnaire/question node. • Application Type, i.e., the database type to which a Questionnaire applies. • Questionnaire type, i.e., the type of Questionnaire. <p>AppDetectivePro has two built-in Questionnaire types, the DISA-STIG and General Questionnaire type. You can also create your own Questionnaire type; for more information, see Working with Questionnaire Types.</p> <ul style="list-style-type: none"> • Date modified, i.e., the last date a Questionnaire was imported or modified.
Question	Bottom right	<p>This portion of the Questionnaire Editor displays a list of all the questions (Name and Description) in the questionnaire. To view the details of each question, select a question and click on the blue right arrow. This will open the Question Editor in view-mode.</p>

Displaying and Understanding the Work Plan Manager

Questionnaires and compatible Audit Policies are unified in AppDetectivePro under a Work Plan, a feature that establishes relationships between a Questionnaire (used for Interview) and its compatible Audit Policy (used to run an Audit, which, in turn, generates check result data used to support responses in a Questionnaire). Work Plan allows you to manage Questionnaires and their compatible Audit Policies in a

convenient way. It allows you to bring context to your Audit scan results by mapping checks to questions or control objectives. For example, PCI DSS requirement 2 states “Do not use vendor-supplied defaults for system passwords and other security parameters”. You can create a PCI DSS work plan to manage your PCI DSS database audit component. Simply create a questionnaire with questions that contain the sub-requirements of PCI DSS and map any check, like Default database password, to sub-requirement 2.2.

This section consists of the following topics:

- Work Plan Manager Features
- Displaying the Work Plan Manager
- Using the Work Plan Manager.

WORK PLAN MANAGER FEATURES

The [Work Plan Manager](#) allows you to do the following:

- View a list of all Work Plans; for more information, see the **Work Plan list** row in the Using the Work Plan Manager table.
- View the details of a Work Plan, including Work Plan information, its Questionnaire, and its compatible Audit Policies; for more information, see [Work Plan, Questionnaire](#), and [Audit Policy](#) rows in the Using the Work Plan Manager table.
- Create a new Work Plan by selecting a Questionnaire to be used for an Interview, as well as a compatible Audit Policy to be used for running an Audit (and obtaining check results for an Interview); for more information, see [Creating a Work Plan](#).
- Edit a Work Plan to change a Work Plan name and description, and select a different Questionnaire and compatible Audit Polices; for more information, see [Editing a Work Plan](#).
- Activate/inactivate Work Plans.
 - Inactivating a Work Plan sets its status to **inactive**, which means the Work Plan **cannot** be used for a new Interview, but can be viewed in previously-run Interviews that used the Work Plan (before it is modified).
 - Activating a Work Plan sets an inactivated Work Plan back to **active** status, which means you can use it in an Interview.

- Delete a Work Plan, which permanently deletes a Work Plan from your system. Once deleted, you will **not** be able to view the Work Plan information in any Interview that used the deleted Work Plan; for more information, see [Deleting a Work Plan](#).

The [Work Plan Manager](#) also allows you to open the:

- Questionnaire Editor to view the associated Questionnaire in detail; for more information, see [Displaying and Understanding the Questionnaire Editor](#)
- Policy Editor to view a selected, associated Audit Policy in detail; for more information, see [Policies](#).

For more information, see [Creating a Work Plan](#).

DISPLAYING THE WORK PLAN MANAGER

To display the [Work Plan Manager](#):

Step	Action
1	Do one of the following: <ul style="list-style-type: none">• Choose Edit > Work Plan from the menu bar.• Click the Work Plan button on the toolbar.

USING THE WORK PLAN MANAGER

The following table describes how to use the components of the [Work Plan Manager](#):

Component	Work Plan Manager Location	Description
Action buttons	Top left	<p>This portion of the Work Plan Manager consists of the following action buttons:</p> <ul style="list-style-type: none"> • New. This action button allows you to create a Work Plan. (You can perform the same action by choosing Work Plan > New from the Work Plan Manager menu.) For more information, see Creating a Work Plan. • Save. This action button allows you to save a Work Plan that you have created. (You can perform the same action by choosing Work Plan > Save from the Work Plan Manager menu.) For more information, see Creating a Work Plan. • Save As. This action button allows you to save an edited version of a Work Plan as a new Work Plan. (You can perform the same action by choosing Work Plan > Save As from the Work Plan Manager menu.) For more information, see Editing a Work Plan. • Edit. This action button allows you to edit a Work Plan that you created. (You can perform the same action by choosing Work Plan > Edit from the Work Plan Manager menu.) For more information, see Editing a Work Plan. You cannot edit a built-in Work Plan. • Activate/Inactivate. These action buttons allow you to activate and inactivate a Work Plan, respectively. (You can perform the same action by choosing Work Plan > Activate or Work Plan > Inactivate from the Work Plan Manager menu, respectively.) For more information, see Activating/Inactivating a Work Plan. • Cancel. This action button displays whenever you are creating a new Work Plan, or editing a Work Plan. You can click this button to cancel any Work Plan creation or editing actions. (You can perform the same action by choosing Work Plan > Cancel from the Work Plan Manager menu.) • Close. This action button closes the Work Plan Manager.

Component	Work Plan Manager Location	Description
Work Plan list	Top left	<p>This portion of the Work Plan Manager lists all Work Plans, either imported (built-in) or created.</p> <p>Optionally, you can click the Show inactive work plan checkbox to display inactive Work Plans; for more information on activating/inactivating Work Plans, see Activating/Inactivating a Work Plan. By default, the Work Plan Manager only displays active Work Plans.</p> <p>You can click a Work Plan in the tree view to display the details of the Work Plan (as explained in the following Work Plan, Questionnaire and Audit Policy rows of this table).</p>
Work Plan	Top right	<p>This portion of the Work Plan Manager displays the details of a Work Plan. Specifically, it consists of the following fields:</p> <ul style="list-style-type: none"> • Name, i.e., the name of the Work Plan. • Description, i.e., the description of the Work Plan. When you import a built-in Questionnaire, AppDetectivePro imports a built-in Work Plan (defined in the XML import file) as well. You cannot edit any of the fields in a built-in Work Plan. However, if you create your own Work Plan (as explained in Creating a Work Plan), you can modify the values in the Name and Description fields. • Date modified, i.e., the last date the Questionnaire was imported, created, or modified.
Show inactive work plan checkbox	Bottom left	<p>Unchecked by default, this checkbox allows you to display (or hide) inactive Work Plans in the Work Plan list portion of the Work Plan Manager; for more information, see Activating/Inactivating a Work Plan.</p>

Component	Work Plan Manager Location	Description
Questionnaire	Middle right	<p>This portion of the Work Plan Manager displays a summary of the Questionnaire that is part of your Work Plan. Specifically, it consists of the following fields:</p> <ul style="list-style-type: none">• Name, i.e., the name of the Questionnaire.• Description, i.e., the description of the Questionnaire.• Application Type, i.e., the database type the Questionnaire applies to (for example, SQL Server).• Questionnaire type, i.e., the type of Questionnaire. (Click the blue right-arrow icon to open the Questionnaire Editor and view the associated Questionnaire in detail.) <p>If you create (or are editing) your own Work Plan, this portion of the Work Plan Manager also displays two additional buttons:</p> <ul style="list-style-type: none">• Add, which allows you to select a questionnaire to the Work plan.• Remove, which allows you to remove a Questionnaire from the Work Plan. <p>For more information on:</p> <ul style="list-style-type: none">• creating a Work Plan, see Creating a Work Plan• editing a Work Plan (that you have created), see Editing a Work Plan.

Component	Work Plan Manager Location	Description
Audit Policy	Bottom right	<p>This portion of the Work Plan Manager displays a list of Audit Policies associated with the Questionnaire in the Work Plan. Specifically, it consists of the following fields and icons:</p> <ul style="list-style-type: none"> • Name, i.e., the name of the Audit Policy. • Description, i.e., the description of the Audit Policy. (Click the blue right arrow icon to open the Policy Editor and view the associated, highlighted Audit Policy in detail.) <p>If you create (or are editing) your own Work Plan, this portion of the Work Plan Manager also displays two buttons:</p> <ul style="list-style-type: none"> • Add, which allows you to add an Audit Policy to a Work Plan • remove, which allows you to remove an Audit Policy from a Work Plan. <p>For more information on:</p> <ul style="list-style-type: none"> • creating a Work Plan, see Creating a Work Plan • editing a Work Plan (that you have created), see Editing a Work Plan.

Displaying and Understanding the Interview Tool

When you conduct an Interview, you are responding to questions from a Questionnaire in the Work Plan you selected during the Interview, using check result data from the Audit associated with the Interview. AppDetectivePro maps the Audit result data to checks in check-associated questions from the Questionnaire (which display as part of the information during the Interview). The Audit check result data provides support data for your response to these questions.

The [Interview](#) tool allows you to conduct the actual Interview. Before you begin the Interview, there are some steps you must complete. These are explained in [Interview](#)

Work Flow. Basically, once you have Discovered and Audited a database, and imported a built-in Questionnaire, you are ready to conduct an Interview.

To display the **Interview** tool, do one of the following:

- Right-click a completed Audit in the network tree view and choose **Interview**.
- Click **Interview** on the toolbar.
- Choose **Run > Interview** from the main AppDetectivePro menu bar.

The following table describes the components of the [Interview](#) tool.

Component	Interview Tool Location	Description
Interview summary fields	Top	<p>This portion of the Interview tool displays the following Interview information:</p> <ul style="list-style-type: none"> • Interview status, i.e., the current status of the Interview. The Interview status can be one of the following: Not Started, In Progress, or Closed. • Application, i.e., the database application on which the Interview is conducted. • IP address, i.e., the IP address where the database application for the Interview (and the Audit for the Interview) resides. • Port, i.e., the port where database application for the Interview (and Audit for the Interview) resides. • Start date, i.e., the date you started the Interview. • Last update date, i.e., the date you last updated the Interview. • Work Plan, i.e., the Work Plan that contains the Questionnaire used by the Interview, for example, SRR DB Checklist for Oracle 10g. For more information, see Displaying and Understanding the Work Plan Manager. • Audit Policy, i.e., name of the Audit Policy used during the Audit of the target database to obtain all check result data (which is used to support the responses for the Interview). For more information, see Interview Work Flow Step 3: Running an Audit. • Questionnaire, i.e., the name of the Questionnaire that contains the questions that you will have to answer for this particular Interview (for example, Oracle 10g DB Checklist). For more information, see Questionnaires and Built-In Questionnaires and Built-In Work Plans. • Questionnaire type, i.e., the type of Questionnaire (for example, DISA-STIG).

Component	Interview Tool Location	Description
Questions panel	Left	<p>The left panel of the Interview tool lists each question from the Questionnaire. As you go through the list of questions, the current question is highlighted in this panel. The corresponding question details display in the Question detail portion (in the upper right portion of the Interview tool).</p> <p>The bottom of the panel displays the following information:</p> <ul style="list-style-type: none"> • Questions, i.e., the total number of questions in the Questionnaire • Answered, i.e., the number of questions you have answered. For questions that have a default response, the question is considered “answered” only if you change the default response. When you answer a question, the color of the question icon changes from red to green. • Unanswered, i.e., the number of questions you have not yet answered. For questions that have a default response, the question is considered “unanswered” if the default response is unchanged. <p>Reminder: You do not have to answer every question in one sitting. In other words, you can always edit an in-progress Interview (as explained in Editing the Interview).</p>

Component	Interview Tool Location	Description
Question detail portion	Upper right	<p>This portion of the Interview tool displays the following information about each question:</p> <ul style="list-style-type: none">• Name, i.e., the name of the question (for example, Application owner object accounts are not disabled).• Description, i.e., a detailed description of the question.• References, i.e., applicable Type/Value references to the question (for example, STIG ID/D00236).

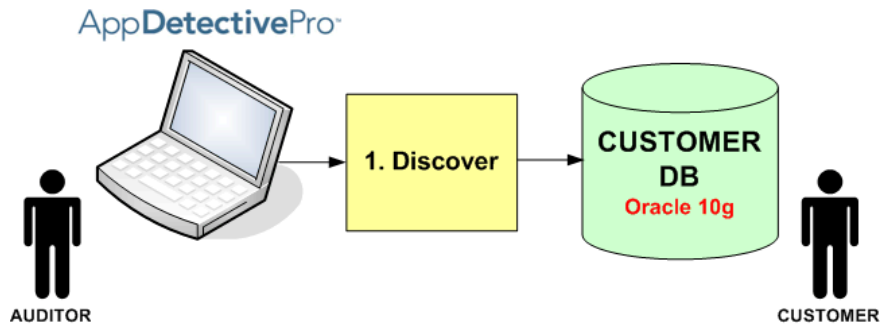
Component	Interview Tool Location	Description
<p>Response detail portion</p>	<p>Middle right</p>	<p>This portion of the Interview tool allows you to respond to each question from a Questionnaire. There are two types of responses, i.e., choice (single or multiple choice) and text responses. Specifically, this portion of the Interview tool consists of:</p> <ul style="list-style-type: none"> • Choice response buttons (where applicable), i.e., Open Finding, Not Reviewed, Not a Finding, and Not Applicable. You can choose your response to a question by clicking the corresponding option button. • Text response, i.e., a free-form Remarks field that allows you to enter comments related to a given question. <p>In addition, this portion of the Interview tool includes Checks Results, i.e., applicable Check Name, Status, and Vulnerability Detail information derived from your completed Audit, which can serve as proof when responding to a question. The Audit name (identified as data and the time when the Audit was run) displays at the top of the check result table.</p> <p>The arrow button at top right of the check result table allows you to view the full contents of all check results. When you click the arrow button, a check results window displays all check results, allowing you to easily view the full contents.</p>

Component	Interview Tool Location	Description
Action buttons	Bottom right	<p>This portion of the Interview tool consists of the following action buttons:</p> <ul style="list-style-type: none"> • Start Interview and Finish Interview. These action buttons allow you to start and finish the Interview, respectively. <p>You must click the Start Interview button when you start an Interview in order to activate the Interview tool. This enables you to enter responses to questions from the Questionnaire used in the Interview; for more information, see Taking the Interview.</p> <p>Similarly, you can click the Finish Interview button when you finish responding to the Questionnaire.</p> <p>You can finish an Interview regardless of whether you have answered all questions in the Questionnaire. If you do not answer any questions, AppDetectivePro uses the default responses (as defined for the question). For more information, see Finishing the Interview.</p> <ul style="list-style-type: none"> • Clear Response. Allows you to clear a response in the Response detail portion of the Interview tool (for a selected question). • Continue Later. Allows you to save an in-progress Interview and continue/complete it later (for more information, see • <Previous and Next >. Allow you to return to the previous question or advance to the next question, respectively.

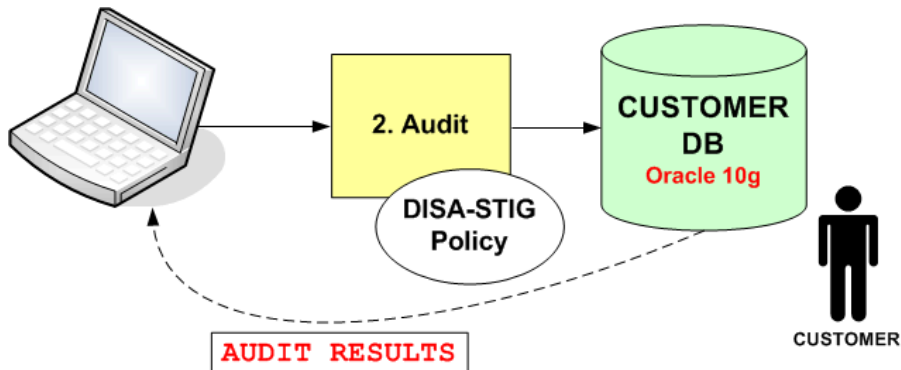
Interview Work Flow

The Interview work flow consists of the following steps:

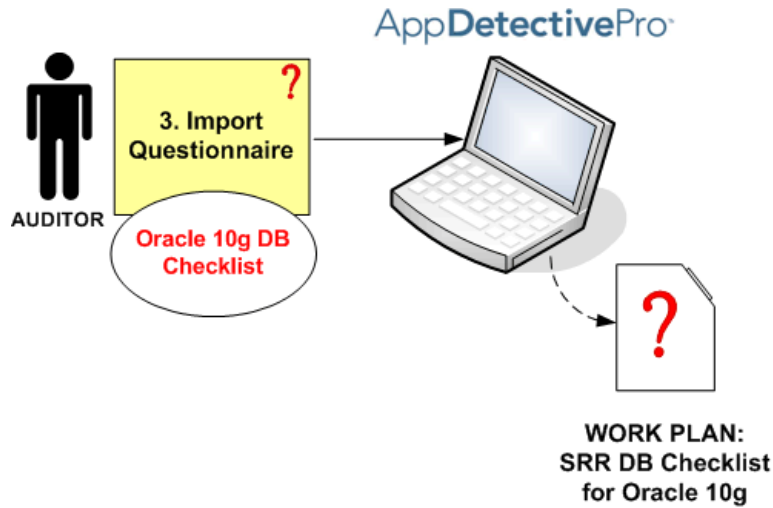
Step 1. Run a Discovery; for more information, see Interview Work Flow Step 1: Running a Discovery.



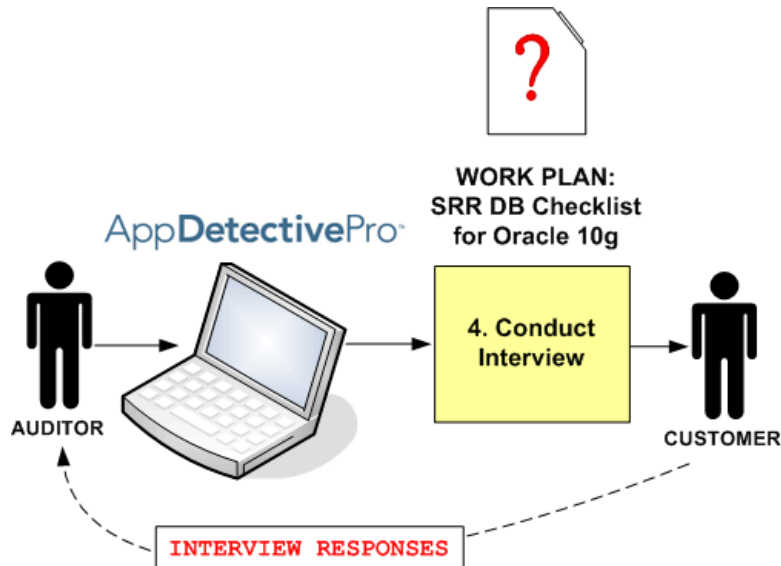
Step 2. Create a Custom Work Plan or Import a built-in DISA-STIG Questionnaire (which creates a Work Plan). For more information, see [Interview Work Flow](#).



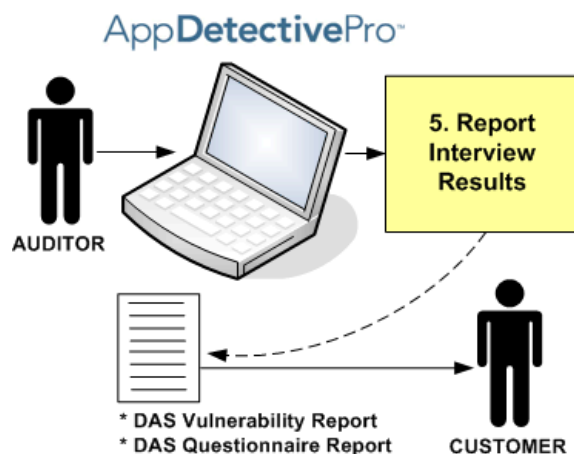
Step 3. Run an Audit (using the policy associated to the Work Plan); for more information, see Interview Work Flow Step 3: Running an Audit.



Step 4. Conduct the Interview; for more information, see Interview Work Flow Step 4: Conducting the Interview.



Step 5. Report on Interview results; for more information, see Interview Work Flow Step 5: Generating an Interview Questionnaire Report.



Interview Work Flow Step 1: Running a Discovery

Step 1 of the Interview Work Flow requires you to run a Discovery.

Interviews are conducted with a Questionnaire/Work Plan against a database. Therefore, you must run a Discovery to find the target database (against which the Interview will be conducted) before you can conduct the Interview.

For more information, on:

- built-in Questionnaires and their compatible Audit Policies, as well as Questionnaire-supported target databases; for more information, see Built-In Questionnaires and Built-In Work Plans
- running a Discovery, see Running a Discovery.

Interview Work Flow Step 2: Importing a Built-In Questionnaire/Creating a Custom Questionnaire

Step 2 of the Interview Work Flow requires you to create a custom work plan or import a built-in DISA-STIG Questionnaire.

This topic consists of the following subtopics:

- About Built-In and Custom Questionnaires
- Interview Work Flow
- Creating a Custom Questionnaire.

ABOUT BUILT-IN AND CUSTOM QUESTIONNAIRES

You cannot conduct an Interview without having Audit check result data that is obtained by running an Audit (using a Compatible Audit Policy). Compatible Audit Policies for a Questionnaire are defined in Work Plan; for more information, see Built-In Questionnaires and Built-In Work Plans.

AppDetectivePro installs Questionnaire XML files that contain built-in Questionnaires and built-in Work Plans associated with these Questionnaires for import. Currently, the only Questionnaire XML files available for import are DISA-STIG built-in Questionnaires for Microsoft SQL Server and Oracle; for more information, see Built-In Questionnaires and Built-In Work Plans. Built-in Questionnaires are located, by default, in the following location: `<installation folder>\AppSecInc\AppDetective\Questionnaire\Import`.

Alternately, you can create a custom Questionnaire within a Work Plan, which allows you to add your own questions, edit existing Questionnaire questions from a built-in Questionnaire (then save the built-in Questionnaire under a different name), and associate the custom Questionnaire with a Questionnaire type (allowing you to provide custom question and response fields within a Questionnaire).

When you import a built-in DISA-STIG Questionnaire, AppDetectivePro also imports a built-in Work Plan for the built-in Questionnaire (defined in the Questionnaire import XML file).

After you import a Questionnaire (and the associated built-in Work Plan), you can view the Questionnaire details in [Questionnaire Editor](#), and the Work Plan details in the [Work Plan Manager](#). You can also create a new Work Plan for the imported Questionnaire (using compatible Audit Policies).

IMPORTING A BUILT-IN QUESTIONNAIRE

To import a built-in Questionnaire:

Step	Action
1	Choose Tools > Import/Export Questionnaire from the menu bar. The Import/Export Questionnaire dialog box displays open to the Import Questionnaire tab.

Step	Action
2	<p>You can manually enter the Questionnaire XML file path (including file name) in the File Path: field. Or, complete the following steps to locate the Questionnaire XML file on your computer or network:</p> <ul style="list-style-type: none">• Click the Browse button to display the Open Questionnaire File dialog box.• Navigate to the <installation folder>\AppSecInc\AppDetective\Questionnaire\Import folder.• Select a built-in Questionnaire XML file; for more information, see Built-In Questionnaires and Built-In Work Plans.• Double click the Questionnaire XML file, or highlight the Questionnaire XML file and click the Open button. <p>The Open Questionnaire File dialog box automatically closes, and the File Path: field in the Import Questionnaire dialog box is populated with your selected Questionnaire XML file.</p> <p>Hint: You can click the Clear button to clear the selected Questionnaire XML file from the File Path: field.</p>
3	<p>Click the Import button to import the selected Questionnaire XML file. A progress status bar displays on the Import Questionnaire dialog box. A success message displays when the Questionnaire XML file is successfully imported.</p>
4	<p>Click the Close button to close the Import/Export Questionnaire dialog box.</p> <p>The imported built-in Work Plan (for the associated built-in Questionnaire) is now available to use in an Interview; for more information, see Interview Work Flow.</p>

CREATING A CUSTOM QUESTIONNAIRE

To create a custom Questionnaire:

Step	Action
1	Choose Edit > Questionnaire from the menu bar. The Questionnaire Editor dialog box appears.
2	Click the New from the menu bar.
3	Under the Questionnaire heading input details for the following: <ul style="list-style-type: none">• Name• Description• Application type; select an application type using the drop-down menu. If you are creating a general questionnaire not tied to a specific application, choose "N/A".• Questionnaire type; Click the Select button. The Select Questionnaire Type for Questionnaire dialog box will display. Choose a Questionnaire Type by marking the check box on the left side. Click the Ok button. If you want to create a new Questionnaire Type, click the Create button (See Working with Questionnaire Types for details).

Step	Action
4	<p>Click the Add button next to the Questions heading. The Question Editor dialog box will display. Input details for the following:</p> <ul style="list-style-type: none">• Name• Description• Response Type (Options available are associated with the Questionnaire Type)• Response Options; Mark a checkbox of all the possible options you want available in the Interview. Right-click on open of the Response Options to create it as a default response when starting the Interview.• References; Click the Add button. This will display the Question Reference dialog box. Select a type for the drop-down menu and input a value. Click Ok.• Associated checks; Click the Add button if you want to map a check to the question. This will display the Select Associated Check for Question dialog box. This will list all the available checks available for the Application type chosen in the Questionnaire. Mark the checkbox to the left of one or more checks you want to associate with this question. Hint: Click on the blue right blue if you want to see the details of the check in the Policy Editor. Note: Adding an associated check is optional.
5	Click the Save button to save the question.
6	Click the New button to add more questions. When you're complete adding Questions to the Questionnaire, click the Close button to close the Question Editor dialog box.
7	Click the Save button on the Questionnaire Editor dialog box to save the Questionnaire. Click the Close button to close out.

EDITING A CUSTOM QUESTIONNAIRE

Note :	Built-in DISA Questionnaires cannot be modified.
------------------	--

To edit a custom Questionnaire:

Step	Action
1	Choose Edit > Questionnaire from the menu bar. The Questionnaire Editor dialog box appears.
2	Click the Edit from the menu bar.
3	You can Edit the following fields under the Questionnaire heading input details for the following: <ul style="list-style-type: none"> • Name • Description • Application type; select an application type using the drop-down menu. If you are creating a general questionnaire not tied to a specific application, choose "N/A". • Questionnaire type; Click the Select button. The Select Questionnaire Type for Questionnaire dialog box will display. Choose a Questionnaire Type by marking the check box on the left side. Click the Ok button. If you want to create a new Questionnaire Type, click the Create button (See Working with Questionnaire Types for details).

Step	Action
4	<p>Working with Questions:</p> <p>You can choose to Add, Delete or Edit Questions from a custom Questionnaire.</p> <ul style="list-style-type: none"> • If you choose to Add a Question, follow Step 4 in Creating a Custom Questionnaire. • If you choose to Delete a Question, highlight the Question by selecting it with your cursor and click the Delete button. • If you choose to Edit a Question, highlight the Question by selecting it with your cursor and click the Edit button. This will open the question in Edit mode in the Question Editor dialog box. Make any necessary changes and click Save. (See Step 4 in Creating Custom Questionnaire for details) Click Close to exit out.
5	Click the Save button on the Questionnaire Editor dialog box to save the Questionnaire. Click the Close button to close out.

EXPORTING A QUESTIONNAIRE

To export a Questionnaire:

Step	Action
1	Choose Tools > Import/Export Questionnaire from the menu bar. The Import/Export dialog box appears. Click on the Export Questionnaire tab.
2	Using the drop-down selection, choose a Questionnaire Type. Select the Questionnaire Type to display the associated Questionnaires.
3	<p>Mark the check box to the left of the Questionnaire file you wish to export.</p> <p>Click the Browse button to select the file location you wish the file to be exported to.</p> <p>Click the Export button. Upon completion of the export, a confirmation dialog box will display. Click OK.</p>

Step	Action
4	Click the Close button to close the Import/Export Questionnaire dialog box.

Interview Work Flow Step 3: Running an Audit

Step 3 of the Interview Work Flow requires you to run an Audit.

Before you can conduct an Interview, you must generate Audit result data for all checks associated with the Questionnaire. AppDetectivePro uses this Audit result data to support your responses. In order to generate Audit result data, you must run an Audit (against a Discovered database) using a compatible Audit Policy; for more information, see Interviews, Questionnaires, and Work Plans.

First, you need find out which compatible Audit Policy to use. You can find a compatible Audit Policy by opening the [Work Plan Manager](#), selecting the Work Plan that you will use for the Interview, and find the Audit Policies in the [Audit Policy](#) section; for more information, see Displaying and Understanding the Work Plan Manager.

Make sure you have imported a built-in DISA-STIG Questionnaire (which, in turn, automatically imports a built-in Work Plan). Or, make sure you have already created a Work Plan.

Important!

Certain **Microsoft SQL Server** DISA-STIG Database Security Configuration checks require you to be a member of the `sysadmin` fixed server role or the `db_owner` fixed database role on the publication database. For more information, see [Microsoft SQL Server Audit Privileges and User Creation Scripts in Appendix G: Audit and User Rights Review Privileges](#).

In addition, the Oracle Audit check `_TRACE_FILES_PUBLIC` undocumented configuration parameter is NOT set to FALSE (which is part of the built-in DISA-STIG Database Security - Audit Policy) must have sysdba privileges. For more information, see [Oracle Audit Privileges in Appendix G: Audit and User Rights Review Privileges](#).

Next, run an Audit against the target database using the compatible Audit Policy. After the Audit is completed, AppDetectivePro maps the Audit result data to checks which are associated with questions from the Questionnaire. These Audit check results will display as part of question information during Interview.

For more information, on:

- built-in Questionnaires and their compatible Audit Policies, as well as Questionnaire-supported target databases; for more information, see Built-In Questionnaires and Built-In Work Plans
- running an Audit, see Running an Audit.

Interview Work Flow Step 4: Conducting the Interview

Step 4 of the Interview Work Flow requires you to conduct the Interview. Interviews can be based on Audit results, but could also be for pure information gathering. You cannot conduct an Interview against a target database without having first run an Audit using a compatible Audit Policy (defined in the Work Plan). The Work Plan must also contain a compatible Questionnaire (used for the Interview). The presence of the compatible Audit Policy and Questionnaire ensure that all Audit check result data (used to support Interview responses) are ready before you conduct the Interview.

Conducting the Interview consists of the following sub-tasks:

- Starting the Interview
- Taking the Interview
- Editing the Interview (if you don't finish the Interview in one sitting)
- Finishing the Interview.

You can only use the results from an Audit for one Interview at a time, using the Work Plan that contains the Questionnaire used for the Interview. If you want to conduct another Interview for the same Work Plan, using the same Audit results, you must purge the existing Interview first; for more information, see Purging an Interview.

When you finish an Interview, its status (in the Interview summary fields of the [Interview](#) tool) changes to [Closed](#). You cannot make any changes to a closed Interview. You can only view the Interview; for more information, see Viewing the Results of a Completed Interview.

Let's assume you have already done the following:

- Discovered an Oracle 10g database (as described in Interview Work Flow Step 1: Running a Discovery).
- Imported the built-in Questionnaire **Oracle 10g DB Checklist** as described in Interview Work Flow Step 2: Importing a Built-In Questionnaire/Creating a Custom Questionnaire.
- We can further assume this action also imported the built-in Work Plan **SRR DB Checklist for Oracle 10g**, which contains the built-in Questionnaire **Oracle 10g DB Checklist**, as well as the Audit Policy **DISA-STIG Database Security - Audit (Built-in)** (which is compatible with the Questionnaire).

This Work Plan will allow you to conduct your Interview using the Questionnaire in the Work Plan. This Interview will also use check result data obtained after running an Audit (using the Audit Policy from the Work Plan).

- Audited the database with the Audit Policy **DISA-STIG Database Security - Audit (Built-in)**, i.e., a compatible Audit Policy for Questionnaire **Oracle 10g DB Checklist** in the Work Plan (Work Flow Step 3) (as described in Interview Work Flow Step 3: Running an Audit).

STARTING THE INTERVIEW

Once you have completed the prerequisite steps for the Interview, you can start the Interview by displaying the **Interview** tool; for more information, see *Displaying and Understanding the Interview Tool*. During the Interview, you can enter responses for each question derived from the Questionnaire included in the selected Work Plan.

To start the Interview:

Step	Action
1	<p>In order to start the Interview, you must display the Interview tool by doing any of the following:</p> <ul style="list-style-type: none"> • Right click a completed Audit in the network tree view; then see Step 2. • Click the Interview button on the toolbar or choose Run > Interview from the menu bar.; then see Step 3.

Step	Action
2	<p>The first way to start the Interview is to do the following:</p> <ul style="list-style-type: none">• Right-click a completed Audit in the network tree view.• Select Interview > <Work Plan Name>, for example, Interview > SRR DB Checklist for Oracle 10g. If no Work Plan displays when you select an Audit, this probably means you did not import a Questionnaire that matches your database type. A second possibility is you ran an Audit with an incompatible Policy. A third possibility is you already conducted an Interview for this Work Plan (which already exists in association with the same Audit). For more information, see Interview Troubleshooting. <p>Once you select a Work Plan, the Interview dialog box appears.</p> <p>Note that a preliminary Missing Audit Check Information dialog box may appear, informing you certain checks (which are associated with Interview questions) did not run during the Audit. You can click the Continue anyway button and still take the Interview. However, certain answers for check-associated questions will not have check result support. The Missing Audit Check Information dialog box will list the specific checks that did not run during the Audit.</p>

Step	Action
3	<p>The second way to start the Interview is to do the following:</p> <ul style="list-style-type: none"> • Click the Interview button on the toolbar, or choose Run > Interview from the menu bar, to display the AppDetectivePro - Choose an Audit dialog box. • Highlight a completed Audit in the left portion of the AppDetectivePro - Choose an Audit dialog box. • Use the Work Plan: drop down to select a Work Plan. You will use this Work Plan's associated Questionnaire for the Interview. If no Work Plan displays when you select an Audit, this probably means you did not import a Questionnaire that matches your database type. A second possibility is you ran an Audit with an incompatible Policy. A third possibility is you already conducted an Interview for this Work Plan (which already exists in association with the same Audit). For more information, see Interview Troubleshooting. <p>Once you select a Work Plan, the Interview dialog box appears.</p> <p>Note that a preliminary Missing Audit Check Information dialog box may appear, informing you certain checks (which are associated with Interview questions) did not run during the Audit. You can click the Continue anyway button and still take the Interview. However, certain answers for check-associated questions will not have check result support. The Missing Audit Check Information dialog box will list the specific checks that did not run during the Audit.</p> <ul style="list-style-type: none"> • Click the Run Interview button to display Interview tool. • Go to Taking the Interview.

TAKING THE INTERVIEW

After you successfully start the Interview, you can take the interview, using the **Interview** tool. You can take the Interview in one sitting, or over the course of several

sittings. You should first read [Displaying and Understanding the Interview Tool](#) to familiarize yourself with the features and functionality of the [Interview](#) tool.

Caution!

As noted in [Taking the Interview](#), a preliminary **Missing Audit Check Information** dialog box may inform you that certain Audit checks (which are associated with Interview questions) did **not** run during the Audit. You can click the **Continue anyway** button and still take the Interview. However, certain answers will **not** include check support. The **Missing Audit Check Information** dialog box will list the specific checks that did not run during the Audit.

To take the Interview:

Step	Action
1	Click the Start Interview button in the lower right-hand portion of the Interview tool.

Step	Action
2	<p>Respond to the first question from the Questionnaire. The details of each question display in the Question detail portion of the Interview tool. For more information on the components of the Interview tool, see <i>Displaying and Understanding the Interview Tool</i>.</p> <p>AppDetectivePro automatically saves your response whenever you:</p> <ul style="list-style-type: none"> • click the < Previous or Next > button to respond to the previous or next question, respectively • click on a question node (in the left question list panel) to respond to a different question • click the Continue Later button • click the Finish Interview button. <p>After you save a response, the bottom of the Questions panel in the Interview tool displays the following information:</p> <ul style="list-style-type: none"> • Questions, i.e., the total number of questions in the Questionnaire. • Answered, i.e., the number of questions you have answered. A question is considered “answered” when the default response has been modified. When you answer a question, the color of the question icon changes from red to green. • Unanswered, i.e., the number of Questions you have not yet answered. A question is considered “unanswered” if it has default response, and has not been modified.
3	<p>Go to the next question by or Next > button (at the bottom of the Interview tool), or any other question (by clicking a question node (in the question list in the left panel of the Interview tool).</p> <p>Alternately, you can go back to any previous question by clicking the < Previous button (at the bottom of the Interview tool).</p> <p>Repeat Step 2.</p>

Step	Action
4	<p>Respond to as many questions as you want.</p> <p>If you respond to all the questions, you are ready to finish the Interview; for more information, see <i>Finishing the Interview</i>.</p> <p>Or, if you want, you can finish the Interview even if you have not responded to all the questions; for more information, see <i>Finishing the Interview</i>.</p> <p>Or, if you have not responded to all questions, and you want to continue the Interview later, you can click the Continue Later button to save an in-progress Interview and edit it later; for more information, see <i>Editing the Interview</i>.</p>
5	<p>View Interview summary information.</p> <p>When you click the Finish Interview or Continue Later on the Interview tool, or close the Interview tool, an Interview node will display under the Audit node (where the Interview was conducted) in the application tree. This Interview node is located in the top left of the AppDetectivePro main page.</p> <p>Select the Interview node, click the Details tab (located in the top right portion of AppDetectivePro main page). AppDetectivePro displays summary information about the Interview. Information about what questions have (or have not) been answered displays in the Details tab.</p>

EDITING THE INTERVIEW

You can take the Interview in one sitting, or over the course of several sittings. Let's assume you successfully started the Interview (as explained in *Starting the Interview*). Let's assume, too, that you started taking the Interview (as explained in *Taking the Interview*), but did not finish the Interview. In such a case, the **Interview** tool lets you edit an in-progress Interview.

To edit the Interview:

Step	Action
1	Right-click an Interview in the network tree view; for more information, see Network Tree View .
2	Select Edit Interview to display your in-progress Interview in the Interview tool.
3	Respond to the Interview questions, as explained in Steps 2-3 of Taking the Interview.
4	Respond to as many questions as you want. If you respond to all the questions, you are ready to finish the Interview; for more information, see Finishing the Interview . Or, if you want, you can finish the Interview even if you have not responded to all the questions; for more information, see Finishing the Interview .
5	You can view Interview summary information, as explained in Step 5 of Taking the Interview .

FINISHING THE INTERVIEW

To finish the Interview:

Step	Action
1	<p>You can finish the Interview at any time by clicking the Finish Interview button.</p> <p>Regardless of whether you answer every question, a pop up informs you that once you finish the Interview, AppDetectivePro will close the Interview and not allow any changes in your responses. You can click the:</p> <ul style="list-style-type: none">• Yes button to finish the Interview• No button to go back and respond to unanswered questions and/or modify your responses. <p>Additionally, if you do not respond to every question in the Questionnaire, AppDetectivePro displays a second pop-up message to inform you that not all questions have been answered, and that AppDetectivePro will use default response (if one exists) as the answer for these questions.</p> <p>You can click the:</p> <ul style="list-style-type: none">• Yes button to finish the Interview (with default responses for unanswered questions)• No button to go back and respond to the unanswered questions.
2	<p>Click the Close button to close the Interview tool.</p> <p>Now you can:</p> <ul style="list-style-type: none">• report on the results of a completed Interview; for more information, see Interview Work Flow Step 5: Generating an Interview Questionnaire Report• view the results of a completed Interview; for more information, see Viewing the Results of a Completed Interview.

Interview Work Flow Step 5: Generating an Interview Questionnaire Report

After you finish an Interview, you can optionally report on the Interview Questionnaire results by running an [Audit Findings Report \(Detailed or Summary\)](#) or a [DAS Questionnaire](#) report. For more information, see Reports.

Viewing the Results of a Completed Interview

Once you finish an Interview, AppDetectivePro closes the Interview and does not allow you to make any changes to your responses. However, AppDetectivePro does allow you to display the [Interview](#) tool and view the read-only results of a completed Interview.

To view the results of a completed Interview:

Step	Action
1	Right click an Interview in the network tree view; for more information, see Network Tree View .
2	Select View Interview to display the Interview tool and view the results of the completed Interview.

Copying a Completed Interview

AppDetectivePro allows you to copy a completed Interview to use in other Audits. This convenient, time-saving function allows you to:

- correct any errors in a completed Interview
- answer questions that apply to multiple databases in one Interview, then copy the answers to an open Interview for a different database
- conduct follow-up Audits, i.e., copy the results from a previous Audit and modify, as necessary.

After you copy a completed Interview, the Interview status (in the [Interview](#) tool) changes to [In Progress](#); for more information, see [Displaying and Understanding the Interview Tool](#).

There are two ways to copy an Interview. Specifically, you can copy an Interview from the:

- network tree view
- AppDetectivePro menu bar.

To copy a completed Interview from the network tree view:

Step	Action
1	Right click a completed Interview in the network tree view; for more information, see Network Tree View .
2	Select Copy to display the Copy Interview dialog box.
3	An Interview is already selected (and hence grayed out) in the Select an Interview: portion of the Copy Interview dialog box.
4	Select one or more available target Audits in the Select an Audit(s): portion of the Copy Interview dialog box. The Select an Audit(s): portion of the Copy Interview dialog box only displays Audits that are compatible with the database version and Work Plan of the source Interview.
5	Click the Copy Interview button.
6	AppDetectivePro copies the Interview and automatically refreshes the network tree. The Interview status (in the Interview tool) of the copied Interview is In Progress . You can now edit the copied Interview; for more information, see Editing the Interview .

To copy a completed Interview from the AppDetectivePro menu bar:

Step	Action
1	Choose Edit > Interview > Copy from the main AppDetectivePro menu bar to display the Copy Interview dialog box.
2	Select a completed Interview in the Select an Interview: portion of the Copy Interview dialog box.

Step	Action
3	Select one or more available target Audits in the Select an Audit(s): portion of the Copy Interview dialog box. The Select an Audit(s): portion of the Copy Interview dialog box only displays Audits that are compatible with the database version and Work Plan of the source Interview.
4	Click the Copy Interview button.
5	AppDetectivePro copies the Interview and automatically refreshes the network tree. The Interview status (in the Interview tool) of the copied Interview is In Progress . You can now edit the copied Interview; for more information, see Editing the Interview .

Purging an Interview

AppDetectivePro allows you to purge an Interview (completed or in-progress).

Caution!	When you purge an Interview, you permanently delete it from the system.
-----------------	---

To purge an Interview:

Step	Action
1	Right click an Interview in the network tree view; for more information, see Network Tree View .
2	Select Purge Interview .
3	A pop-up prompts you to confirm the purge. If you're sure you want to purge the Interview, click the Yes button. The Interview is permanently purged from AppDetectivePro.

Working with Questionnaire Types

The [Questionnaire Type Settings](#) dialog box allows you to create a Questionnaire type, which you can associate with a custom Questionnaire. You can also revise certain parameters of a built-in Questionnaire (i.e., [DISA-STIG](#) or [General](#)). A

Questionnaire type consists of question fields and response fields. For more information, see *Working with Questionnaire Types*.

This topic consists of the following subtopics:

- Understanding the Questionnaire Type Settings Dialog Box
- CREATING a NEW Questionnaire Type
- EDITING aN EXISTING Questionnaire Type
- DELETING AN EXISTING Questionnaire Type

UNDERSTANDING THE QUESTIONNAIRE TYPE SETTINGS DIALOG BOX

The following table describes the components of the [Questionnaire Type Settings](#) dialog box:

Component	Questionnaire Editor Location	Description
Action buttons	Top left	<p>This portion of the Questionnaire Type Settings consists of the following action buttons:</p> <ul style="list-style-type: none"> • New. This action button allows you to create a Questionnaire Type. • Save. This action button allows you to save a Questionnaire Type that you have created. • Save As. This action button allows you to save an edited version of a Questionnaire Type as a new Questionnaire Type. • Edit. This action button allows you to edit a Questionnaire Type that you created. <p>Note: You cannot edit the built-in Questionnaire types (DISA-STIG and General)</p> <ul style="list-style-type: none"> • Cancel. This action button displays whenever you are creating a new Questionnaire Type, or editing a Questionnaire Type. • Close. This action button closes the Work Plan Manager. <p>Close. This action button closes the Work Plan Manager.</p>
Questionnaire Types	Left	<p>This portion of the Questionnaire Type Settings dialog box displays the available Questionnaire Types. Click on one to see the details.</p>
Name and Description	Top Right	<p>This portion of the Questionnaire Type Settings dialog box displays the name and description of the Questionnaire Type selected.</p>

Component	Questionnaire Editor Location	Description
Question Fields	Middle Right	<p>This portion of the Questionnaire Type Settings dialog box displays detailed information about the Question fields that are allowed. Specifically, it consists of the following fields:</p> <ul style="list-style-type: none"> • Name. This is a non-modifiable field. Enter in text for your question or control objective name. • Description. This is a non-modifiable field. Enter in details about the question name • References. Use the Add button to add in custom reference fields; for example PCI DSS sub-requirement number.
Response Fields	Bottom Right	<p>This portion of the Questionnaire Type Settings dialog box displays detailed information about the Question responses that are allowed. Specifically, it consists of the following fields:</p> <ul style="list-style-type: none"> • Remarks. This is a non-modifiable field. This allows for free text to me added when taking the Interview. • Response Options. Use the Add button to add in custom response types; for example Not a Finding, Open Finding, etc.

CREATING A NEW QUESTIONNAIRE TYPE

To create a new Questionnaire type:

Step	Action
1	Choose Edit > Questionnaire Type Settings from the main AppDetectivePro menu bar to display the Questionnaire Type Settings dialog box.
2	Click on the New button.

Step	Action
3	Input a Name and Description for the Questionnaire Type.
4	Click the Add button next to References. This will display a New Reference Type dialog box. Enter in a value, for example PCI DSS sub-requirement number. Click the Ok button.
5	<p>Click the Add button next to Response Options. This will display a New Response Option dialog box. Enter in the following:</p> <ul style="list-style-type: none"> • Name. This will display as an option to choose for your response when taking the Interview, for example Not a Finding, Open Finding, Not Reviewed, etc. • Code. This is used as a reference for the Response Option name in reports, for example NR for “Not Reviewed” • Finding Level. Use the drop-down and select a Finding Level. This is used to help summarize Interview results in reports. • Optionally set one of the New Response Options as the default, for example Not Reviewed. <p>Repeat this step for as many Response Options you want to be made available in the Questionnaire Type.</p>
6	Click the Save button when you are finished. Click the Close button to exit out.

EDITING AN EXISTING QUESTIONNAIRE TYPE

To edit an existing Questionnaire type:

Step	Action
1	Choose Edit > Questionnaire Type Settings from the main AppDetectivePro menu bar to display the Questionnaire Type Settings dialog box.
2	Select a Questionnaire Type from the left column. Click the Edit button.

Step	Action
3	You are now able to edit any of the following fields: <ul style="list-style-type: none"> • Name • Description • References • Response Options
4	Click the Save button when you are done editing.

DELETING AN EXISTING QUESTIONNAIRE TYPE

To delete an existing Questionnaire type:

Step	Action
1	Choose Edit > Questionnaire Type Settings from the main AppDetectivePro menu bar to display the Questionnaire Type Settings dialog box.
2	Select a Questionnaire Type from the left column.
3	Click the Delete button. You will be asked to confirm the action. Click Yes to proceed.
4	Click the Close button to exit out.

Deleting a Questionnaire

AppDetectivePro allows you to delete a Questionnaire (including an imported built-in Questionnaire).

Caution!

When you delete a Questionnaire, you will permanently delete not only the Questionnaire itself, but also all related Work Plans and Interviews that use the Questionnaire. Once you delete a Questionnaire, you **cannot** use it in association with a Work Plan (unless you re-import the Questionnaire XML file; for more information, see Interview Work Flow Step 2: Importing a Built-In Questionnaire/Creating a Custom Questionnaire).

Questionnaire names must be unique. Duplicate Questionnaires are not allowed. If you want to import the same Questionnaire again, you **must** delete the Questionnaire that was imported before.

To delete a Questionnaire:

Step	Action
1	Display the Questionnaire Editor ; for more information, see Displaying and Understanding the Questionnaire Editor .
2	Right click a Questionnaire in the Questionnaire list in the left column of the Questionnaire Editor .
3	Select Delete .
4	A pop-up prompts you to confirm the delete. If you're sure you want to delete the Questionnaire, click the Yes button. The Questionnaire is deleted. You cannot use it in association with a Work Plan (unless you re-import the Questionnaire XML file; for more information, see Interview Work Flow Step 2: Importing a Built-In Questionnaire/Creating a Custom Questionnaire).

Creating a Work Plan

When you import a built-in Questionnaire (as explained in Interview Work Flow Step 2: Importing a Built-In Questionnaire/Creating a Custom Questionnaire), AppDetectivePro also imports a built-in Work Plan for the associated built-in Questionnaire (defined in the same Questionnaire import XML file). You cannot modify any portion of the built-in Work Plan.

You can, however, use the [Work Plan Manager](#) to create a new Work Plan. As explained below, when you create a Work Plan, you must:

- give the Work Plan a unique **name** and **description**
- select an **application type** and a **Questionnaire** for the Interview
- add one or more **Audit Policies**, which, when used to run an Audit, generate check result data for the Interview.

Note:	When you save a Work Plan, AppDetectivePro validates whether the associated Audit Policies are compatible with the Questionnaire in the Work Plan. A compatible Audit Policy for a Questionnaire must contain all checks associated with the Questionnaire; for more information, Understanding Interviews, Questionnaires, and Work Plans.
--------------	--

You cannot create a new Work Plan for the same Questionnaire and same Audit Policy that already exist in another Work Plan. Instead, you should use the existing Work Plan when you conduct an Interview.

To create a Work Plan:

Step	Action
1	Display the Work Plan Manager ; for more information, see Displaying and Understanding the Work Plan Manager .
2	Click the New button on the Work Plan Manager toolbar. The Work Plan Manager displays new Work Plan fields.

Step	Action
3	<p>When you create a Work Plan, the Work Plan Manager allows you to populate the Work Plan with information. Specifically, you can do the following:</p> <ul style="list-style-type: none">• Enter a Work Plan Name in the Work Plan portion of the Work Plan Manager.• Enter a Work Plan Description in the Work Plan portion of the Work Plan Manager.• Add a Questionnaire to the Work Plan in the Questionnaire portion of the Work Plan Manager.• Add Audit Policies to the Work Plan in the Audit Policy portion of the Work Plan Manager. <p>For more information, on using the Work Plan Manager, see Displaying and Understanding the Work Plan Manager.</p>
4	<p>When you're done, you can click the Save button to save your Work Plan. AppDetectivePro checks if each Audit Policy added is compatible with the Questionnaire in the Work Plan. AppDetectivePro only allows you to save compatible Audit Policies in your Work Plan.</p> <p>Once you successfully save your Work Plan, you can conduct an Interview using the Questionnaire associated with the Work Plan; for more information, see Interview Work Flow Step 4: Conducting the Interview.</p> <p>You can always go back and edit any Work Plan that you have created, and even save an edited version under a different name; for more information, see Editing a Work Plan.</p> <p>Click Cancel (on the Work Plan Manager menu) or choose Work Plan > Cancel (on the Work Plan Manager toolbar) to cancel your new Work Plan.</p>

Editing a Work Plan

When you import a built-in Questionnaire (as explained in Interview Work Flow Step 2: Importing a Built-In Questionnaire/Creating a Custom Questionnaire), AppDetectivePro also imports a built-in Work Plan for the built-in Questionnaire (defined in the Questionnaire import XML file). You cannot modify any portion of the built-in Work Plan.

However, you can use the [Work Plan Manager](#) to edit a custom, user-created Work Plan (as explained in Creating a Work Plan). When you create a Work Plan, you can:

- edit its **name** and **description**
- add and remove a **Questionnaire**
- add and remove compatible **Audit Polices**.

You can go back and edit any modifiable portion of any Work Plan that you have created, and even save an edited version under a different name. This topic explains how.

Note:	If you edit a Work Plan that was previously used in an Interview, AppDetectivePro automatically creates a new Work Plan with the same name in order to maintain the integrity between Work Plan and Interview. Subsequently, a previously-run Interview can still retain old Work Plan information (for viewing only).
--------------	--

To edit a Work Plan that you have created:

Step	Action
1	Display the Work Plan Manager ; for more information, see Displaying and Understanding the Work Plan Manager .
2	Click the Edit button on the Work Plan Manager toolbar.

Step	Action
3	<p>When you edit a Work Plan, the Work Plan Manager allows you to do the following:</p> <ul style="list-style-type: none"> • Edit the Work Plan Name in the Work Plan portion of the Work Plan Manager. The Work Plan name is unique. • Edit a Work Plan Description in the Work Plan portion of the Work Plan Manager. • Use the Add and Remove buttons in the Questionnaire portion of the Work Plan Manager. • Use the Add and Remove buttons in the Audit Policy portion of the Work Plan Manager. <p>For more information, on using the Work Plan Manager, see Displaying and Understanding the Work Plan Manager.</p>
4	<p>When you're done, you can click the:</p> <ul style="list-style-type: none"> • Save button to save your edited Work Plan • Save As button to save the edited version of your Work Plan as a new Work Plan (but with a different associated Audit Policy). <p>Hint: You can always click the Cancel button (on the Work Plan Manager menu) or choose Work Plan > Cancel (on the Work Plan Manager toolbar) to cancel the editing of your Work Plan before you save it.</p> <p>You can now conduct an Interview using the Questionnaire associated with the Work Plan; for more information, see Interview Work Flow Step 4: Conducting the Interview.</p>

Activating/Inactivating a Work Plan

As explained in Interview Work Flow Step 2: Importing a Built-In Questionnaire/Creating a Custom Questionnaire, when you create a Work Plan, AppDetectivePro automatically imports a built-in Work Plan (which you can view in the read-only Work Plan Manager; for more information, see Displaying and Understanding the Work Plan Manager).

AppDetectivePro allows you to activate and inactivate Work Plans. As explained in Understanding Interviews, Questionnaires, and Work Plans, a Work Plan stores a

Questionnaire and one or more compatible Audit Policies in a convenient way, allowing you to conduct an Interview.

Logically, then, when a Work Plan is active, you can use it to conduct an Interview. When you activate a Work Plan, you are setting an inactivated Work Plan back to active status so it can be used for an Interview. This is useful when you want to use an inactivated Work Plan to conduct a new Interview.

When a Work Plan is inactive, you cannot use it to conduct an Interview. Inactivating a Work Plan sets its status to inactive. Although an inactivated Work Plan cannot be used for new Interviews, previously-run Interviews that used the Work Plan will display the Work Plan information. Inactivating a Work Plan is useful when you don't want to use the Work Plan for new Interviews (at least for the time being), but you want to be able to view the Work Plan in previously-run Interviews that used the Work Plan (before it is inactivated). If you don't have any Interviews that use a particular Work Plan, you may consider deleting the Work Plan, instead of inactivating it; for more information, see [Deleting a Work Plan](#).

Hint: The **Work Plan Manager** contains a **Show inactive work plan** checkbox. Unchecked by default, this checkbox allows you to display (or hide) inactive Work Plans in the Work Plan Manager; for more information, see [Displaying and Understanding the Work Plan Manager](#).

To activate a Work Plan:

Step	Action
1	Display the Work Plan Manager ; for more information, see Displaying and Understanding the Work Plan Manager .
2	<ul style="list-style-type: none"> • Select the desired work plan in the Work Plan list in the left column. Click the Activate button on the Work Plan Manager toolbar. • Select the desired work plan in the Work Plan list in the left column. Right-click on it and select Activate.

To inactivate a Work Plan:

Step	Action
1	Display the Work Plan Manager ; for more information, see Displaying and Understanding the Work Plan Manager .
2	<ul style="list-style-type: none"> • Select the desired work plan in the Work Plan list in the left column. Click the Inactivate button on the Work Plan Manager toolbar. • Select the desired work plan in the Work Plan list in the left column. Right-click on it and select Inactivate.

Deleting a Work Plan

AppDetectivePro allows you to delete a Work Plan, regardless if it is active or inactive. Deleting a Work Plan permanently deletes the Work Plan from your system. Once you delete a Work Plan, it's gone forever. You will not be able to view the Work Plan information in any Interview that uses the Work Plan. Make sure that no Interview uses the Work Plan before you delete it.

To delete a Work Plan:

Step	Action
1	Display the Work Plan Manager ; for more information, see Displaying and Understanding the Work Plan Manager .
2	Select the desired work plan in the Work Plan list in the left column. Right-click on it and select Delete.
3	A pop-up prompts you to confirm the delete. If you're sure you want to delete the Work Plan, click the Yes button. The Work Plan is permanently deleted from AppDetectivePro.

Interview Troubleshooting

If no Work Plan displays when you select an Audit (as explained in Starting the Interview), this probably means you did not do at least one of the following:

- You did **not** Import a Questionnaire for a matching database type.
- You did **not** run an Audit with an Audit Policy that exists in a Work Plan associated with a Questionnaire. (Meaning, you **must** verify that your Audit Policy and Questionnaire are compatible.)
- You did **not** conduct an Interview using the same Work Plan as you used previously.

In a successful Interview scenario, it can be assumed that you:

- Discovered a supported database, for example, Oracle 10g
- Imported a built-in Questionnaire, for example, [Oracle 10g DB Checklist](#)
- Audited the database with a compatible Audit Policy (defined in a matching Work Plan) to associate with a Questionnaire, for example, [DISA-STIG Database Security - Audit \(Built-in\)](#) Policy defined in the Work Plan [SRR DB Checklist for Oracle 10g](#).

When you import the Questionnaire, AppDetectivePro also imports a built-in Work Plan associated with the Questionnaire [SRR DB Checklist for Oracle 10g](#). When you select the Audited Oracle 10g database, you can use the [SRR DB Checklist for Oracle 10g](#) (and its associated Questionnaire) to conduct an Interview.

Let's look at two unsuccessful Interview scenarios.

TROUBLESHOOTING SCENARIO #1:

Imagine that you did the following:

- Discovered an Oracle 10g database
- Audited the database with the [HIPAA - Audit](#) Policy
- Imported the [Oracle 10g DB Checklist](#) built-in Questionnaire.

Upon Taking the Interview, you do not see any Work Plans associated with your Audited Oracle 10g database.

Question: What happened?

Answer: You Audited your database with a Policy (i.e., an [HIPAA - Audit Policy](#)) that does not exist in a Work Plan containing the Questionnaire [Oracle 10g DB Checklist](#). The Audit Policy may be incompatible with the Questionnaire.

In order to use the Interview feature in AppDetectivePro, your Audit Policy and Questionnaire must be compatible. You need add the Audit Policy to an Work Plan to verify if it is compatible with the Questionnaire in the Work Plan.

As explained in this example Work Plan that contains a [HIPAA - Audit Policy](#) and a built-in Questionnaire [Oracle 10g DB Checklist](#) does not exist. Furthermore, it has not been verified that the Audit Policy is compatible with the Questionnaire. The table in Built-In Questionnaires and Built-In Work Plans lists each built-in Questionnaire, and its compatible Audit Policy and database type/version.

TROUBLESHOOTING SCENARIO #2:

Let's say you did the following:

- Discovered an Microsoft SQL Server 2005 database.
- Imported the [Oracle 10g DB Checklist](#) built-in Questionnaire.
- Audited the database with the [DISA-STIG Database Security - Audit Policy](#)

Upon Taking the Interview, you do not see any Work Plans associated with your Audited Oracle 11g database.

Question: What happened?

Answer: In this case, the Questionnaire you imported ([Oracle 10g DB Checklist](#)) does not match the database type that you Audited (i.e., Microsoft SQL Server 2005). That's your problem.

In order to use the Interview feature in AppDetectivePro, there must be a logical match between the Audited database type and the database version of the associated Questionnaire. The table in Built-In Questionnaires and Built-In Work Plans lists each built-in Questionnaire, and its compatible Audit Policy and database type/version.

Reports

This section consists of the following topics:

- [What are AppDetectivePro Reports?](#)
- [Pen Test and Audit Reports](#)

- [User Rights Review Reports](#)
- [Questionnaire Reports](#)
- [Report Formats](#)
- [Running Reports](#)
- [Printing and Exporting Reports](#)
- [Suppressing Vulnerabilities](#)

What are AppDetectivePro Reports?

AppDetectivePro allows you to generate Reports designed to communicate vulnerabilities Discovered by AppDetectivePro (and actions taken) to all levels of your organization. AppDetectivePro also allows you to report on User Rights Review scan data.

AppDetectivePro supports the following Report types:

- [Pen Test and Audit Reports](#)
- [User Rights Review Reports](#)

Pen Test and Audit Reports

AppDetectivePro includes the following standard Pen Test and Audit Reports:

- [Application Banners](#)
- [Application Inventory](#)
- [Check Status](#)
- [Policy](#)
- [Summary Report](#)
- [User Information](#)
- [Vulnerability Differences for Application](#)
- [Vulnerability Details](#)
- [Vulnerability Summary](#)
- [DAS Vulnerability](#).

Details on each standard Pen Test and Audit Report follow:

- [Application Banners](#). This type of report displays information found within the Details tab of the main window for the currently loaded Session.

- **Application Inventory.** Use this report to generate a snapshot of your applications. This report is useful in summarizing the state of your network applications according to the currently loaded Session.
- **Check Status.** Creates a report of all security checks run on an application and their results. The following table explains possible **Status** field messages.

If the Status field reads:	It means a check:
Violation Found	Found at least one vulnerability.
No Violation Found	Found no vulnerabilities.
Failed	Failed for some reason (an explanation message appears).
Working	Is currently running.
Skipped	Could not be executed for some reason and was skipped (an explanation message appears).

- **Policy.** Generates a report based on the Policy you choose. You can generate a Policy Report on inactive Policies. For more information, see *Activating/Deactivating a Policy*. You can include exception and risk acceptance information by marking the checkbox 'Include exception and risk acceptance information in this report' prior to hitting the Next button in the Report Wizard.
- **Summary Report.** Displays a high-level summary of all the applications and vulnerabilities Discovered on the network or in a particular folder.
- **User Information.** Creates a report containing a list of user logins and related information.
- **Vulnerability Differences for Application.** Generates a report showing the differences in vulnerabilities between two Pen Tests or Audits of a specific application.

- **Vulnerability Details.** Creates a report containing all the Vulnerability details found for each Audit and Pen Test performed for the current Session. This report can potentially contain a large number of records, which may span multiple pages if you generate an HTML report. You can configure the maximum number of records to display per page. For more information on the HTML report format, see Report Formats. You can include exception and risk acceptance information by marking the checkbox 'Include exception and risk acceptance information in this report' prior to hitting the Next button in the Report Wizard.
- **Vulnerability Summary.** Creates a report which contains all the vulnerabilities found for each Audit and Pen Test performed for the current Session.
- **DAS Vulnerability.** Generates an XML report of vulnerability and configuration issues mapped to elements of the DISA STIG, which includes IA control, STIG ID, Key, and more.

Note:	AppDetectivePro does not automatically display the DAS Vulnerability report will not be displayed automatically when the report generation finishes. A message box indicating the location where the report has been saved will be showed instead.
--------------	--

User Rights Review Reports

This section consists of the following topics:

- [Understanding the Relationship Between a Microsoft SQL Server Login and Database User in User Rights Review Reporting](#)
- [Grant Paths in User Rights Review Reports](#)
- [Understanding Implicit Privileges](#)
- [Standard User Rights Review Reports](#)
- [Difference Reports](#)

UNDERSTANDING THE RELATIONSHIP BETWEEN A MICROSOFT SQL SERVER LOGIN AND DATABASE USER IN USER RIGHTS REVIEW REPORTING

For the purpose of User Rights Review reporting, AppDetectivePro treats the relationship between a Microsoft SQL Server login and a Microsoft SQL Server database user as a role relationship, with each database user mapped as a role to its corresponding login when possible. Microsoft SQL Server differentiates between the login used to connect to the database instance and the privileges acquired while

using a particular database within the instance. The inheritance of privileges between a login and all of the database users it may become works like a role relationship, since the full list of privileges for a login includes all privileges that are attached to database users that login may become.

For example, a user may use the login `sa` to connect to a Microsoft SQL Server instance, but this login may become `master.dbo` when using the master database or `tempdb.dbo` when using the `tempdb` database. Consequently, when you select a Microsoft SQL Server login as the target for the [All Roles for a User Report](#), AppDetectivePro displays all database users this login may become when using various databases listed in the report. In addition, when selecting a Microsoft SQL Server login for the [All Effective Privileges for a User Report](#), AppDetectivePro displays all privileges the login takes on when using various databases, because of the database users that login is mapped to.

Application Security, Inc. recommends you run the [All Effective Privileges for a User Report](#) on a login rather than a database user for Microsoft SQL Server instances, since logins may be assigned to server roles that affect their privileges as database users. AppDetectivePro does not display the privileges granted to a login through server logins when you run an [All Effective Privileges for a User Report](#) only on a database user.

GRANT PATHS IN USER RIGHTS REVIEW REPORTS

Roles are sets of privileges that can be assigned to either a user or another role in a database. When a user or role obtains a privilege in a database, that privilege may be either directly granted to the user or role, or it may be inherited from another role assignment.

For example, if the user `SYS` is granted the role `DBA`, and `DBA` is granted the role `EXP_FULL_DATABASE`, then `SYS` inherits permissions from both `DBA` and `EXP_FULL_DATABASE`. Subsequently, AppDetectivePro User Rights Review Reports show this inheritance relationship using a list of users and roles called a grant path.

So, continuing the above example, if `EXP_FULL_DATABASE` is granted the privilege `SELECT ON SYS.AUD$`, both the `DBA` role and the `SYS` user would obtain this privilege as well, and the [All Effective Privileges for a User Report](#) for `SYS` would contain this privilege with the grant path `SYS -> DBA -> EXP_FULL_DATABASE`. This means the privilege was granted to `EXP_FULL_DATABASE`, but `SYS` obtained the privilege because `SYS` was granted `DBA`, and `DBA` was, in turn, granted `EXP_FULL_DATABASE`.

Grant paths appear in the following User Rights Review Reports:

- Standard User Rights Review Reports ([All Effective Privileges for a User](#) and [All Effective Privileges for a Role](#))
- Difference Reports ([Differences Report For All Effective Privileges for a Role](#) and [Differences Report For All Effective Privileges for a User](#)).

Note:	Starting with AppDetectivePro 6.3, you can optionally check the Exclude Grant Path from this Report checkbox (in the AppDetectivePro - Report Wizard) to exclude grant path information from all applicable User Rights Review Reports.
--------------	--

UNDERSTANDING IMPLICIT PRIVILEGES

Some system privileges that apply to multiple objects are presented in User Rights Review reports as roles. For example, a system privilege of the form [SELECT ANY TABLE](#) applies to multiple tables in the database, and for the purpose of reporting is expanded into the specific object privileges it implies.

A specific object privilege like [SELECT ON SCOTT.EMP](#) that is generated from a system privilege such as [SELECT ANY TABLE](#) is called an implicit privilege in User Rights Review reports. Implicit privileges display in certain User Rights Review reports and the system privileges that generate them display in grant paths as special roles surrounded by braces; for example, [[SELECT ANY TABLE Privilege](#)]. The roles that generate Implicit privileges do not exist as actual roles in your database, they are only presented that way in reports so that specific object privileges can be associated with the privilege or role that they were granted from.

The screen shot below shows implicit privileges generated from a `DELETE ANY TABLE` system privilege in an All Effective Privileges For a User report. The system privilege appears as a role in the grant path `SYS -> [DELETE ANY TABLE Privilege]` to clarify the source of the implicit privilege. Each individual implicit privilege is listed on a row by itself. All of the object privileges listed below are implicitly granted to `SYS` because the system privilege `DELETE ANY TABLE` is granted to `SYS`.

Privilege	Type	Grant Path	Grantee Type
DELETE ON CTXSYS.CTX_SERVERS	Object Privilege	SYS -> [DELETE ANY TABLE Privilege]	Implicit Privilege
DELETE ON CTXSYS.CTX_SQES	Object Privilege	SYS -> [DELETE ANY TABLE Privilege]	Implicit Privilege
DELETE ON CTXSYS.CTX_STOPLISTS	Object Privilege	SYS -> [DELETE ANY TABLE Privilege]	Implicit Privilege
DELETE ON CTXSYS.CTX_STOPWORDS	Object Privilege	SYS -> [DELETE ANY TABLE Privilege]	Implicit Privilege
DELETE ON CTXSYS.CTX_SUB_LEXERS	Object Privilege	SYS -> [DELETE ANY TABLE Privilege]	Implicit Privilege

Standard User Rights Review Reports

AppDetectivePro includes the following standard User Rights Review reports:

- [All Users in a Database Instance Report](#)
- [All Roles in a Database Instance Report](#)
- [All Effective Privileges for a User Report](#)
- [All Effective Privileges for a Role Report](#)
- [All Roles for a User](#)
- [All Roles for a Role](#)
- [Object Access](#)
- [All Effective Members of a Role Report](#)

Note:

With the exceptions of the All Roles for a User and the All Roles for a Role User reports, each standard User Rights Review report allows you to use the Properties branch and configure the maximum amount of records that display per page (for HTML and MHT formats only). For more information on using the Properties branch, see Properties. For more information on report formats, see Report Formats.

ALL USERS IN A DATABASE INSTANCE REPORT

This User Rights Review report lists all database users who have access to the instance. Users in the report are identified by both a name and a type. If a user rights review has been run against a Microsoft SQL Server database, many types of users may appear in this report. When a user connects to a Microsoft SQL Server instance, they must authenticate with the server through a login. Once authenticated and using a particular database, the user is associated with a database user in that particular database. A full list of Microsoft SQL Server user types follows:

- **Microsoft SQL Server SQL Login.** A login authenticated with a username and password
- **Microsoft SQL Server Windows Login.** A login associated with a Windows user.
- **Microsoft SQL Server Implicit Windows Group.** A Windows group that can log in to the instance because it is contained in another Windows group associated with a login.
- **Microsoft SQL Server Implicit Windows User.** A Windows user that can log in to the instance because it is contained in another Windows group associated with a login.
- **Microsoft SQL Server Windows Group Login.** A login associated with a Windows group.
- **Microsoft SQL Server Certificate Mapped Login.** A login associated with a certificate.
- **Microsoft SQL Server Asymmetric Key Mapped Login.** A login associated with an asymmetric key.
- **Microsoft SQL Server SQL User.** A database user associated with a SQL Login.
- **Microsoft SQL Server Windows User.** A database user authenticated through Windows authentication.
- **Microsoft SQL Server Windows Group User.** A database user authenticated through Windows authentication, based on the users' membership in a Windows group.
- **Microsoft SQL Server Certificate Mapped User.** A database user associated with a Certificate Mapped Login.
- **Microsoft SQL Server Asymmetric Key Mapped User.** A database user associated with an Assymmetric Key Mapped Login.

- **Microsoft SQL Server Unmapped SQL User.** A SQL User that is not known to be associated with any login. These orphaned users can occur, for example, when a database is backed up and restored on another server.
- **Microsoft SQL Server Unmapped Windows User.** A Windows User that is not known to be associated with any login.
- **Microsoft SQL Server Unmapped Windows Group User.** A Windows Group User that is not known to be associated with any login.

This User Rights Review Report consists of the following columns:

- **User Type.** The type of user.
- **User.** The name of the user.
- If you run this Report at the Session level, the following two columns also display:
 - **IP/Port.** The IP and port of the database the user belongs to.
 - **Database Type.** A short description of the type of database

Note:	This report can potentially contain a large number of records, which may span multiple pages if you generate an HTML or MHT report. However, you can use the Properties branch and configure the maximum amount of records that display per page (for HTML and MHT formats only). For more information on using the Properties branch, see Properties. For more information on report formats, see Report Formats.
--------------	--

ALL ROLES IN A DATABASE INSTANCE REPORT

This User Rights Review report lists all roles that *can be* granted to users or roles in the database instance. Roles are collections of privileges that can be applied to multiple users, roles, or applications using a database instance. Roles in this report are identified by both a name and a type. If you run a User Rights Review against a Microsoft SQL Server instance, this report displays up to three different types of roles:

- **Microsoft SQL Server Role.** A role that applies to a login and any database users associated with that login (Example: `sysadmin`)
- **Microsoft SQL Server Database Role.** A role that can apply to users and roles at the database level only (Example: `master.public`)

- **Microsoft SQL Server Application Role.** A role that can only be associated with an application.

This User Rights Review Report consists of the following **columns**:

- **Role Type.** The type of role
- **Role.** The name of the role

If you run this Report at the Session level, the following two columns also appear:

- **IP/Port.** The IP and port of the database the user belongs to
- **Database Type.** A short description of the type of database

Note:

This report can potentially contain a large number of records, which may span multiple pages if you generate an HTML or MHT report. However, you can use the **Properties** branch and configure the maximum amount of records that display per page (for HTML and MHT formats only). For more information on using the **Properties** branch, see Properties. For more information on report formats, see Report Formats.

ALL EFFECTIVE PRIVILEGES FOR A USER REPORT

Given a user, this User Rights Review report provides an exhaustive list of **everything** a user can do in a database, i.e., privileges on tables, stored procedures, functions, and views, as well as system privileges such as the ability to connect to a database or create a table. This report breaks down any umbrella system privileges such as "select from any table" into individual object privileges, as well as taking into account the effect of any **REVOKEs** or **DENYS** of privileges.

This User Rights Review Report consists of the following columns:

- **Privilege.** A description of the privilege granted; for example, **CREATE TABLE**.
- **Type.** Either **System Privilege** or **Object Privilege**. **System privileges** are server-level privileges such as **CREATE TABLE** or **CONNECT TO DATABASE**. **Object privileges** are privileges associated with a particular table, view, stored procedure or any other kind of database object; for example, **SELECT ON SCOTT.BONUS**.

- **Grant Path.** The path, through roles, **from** the user/role selected for this Report **to** the user/role assigned the privilege; for more information on grant paths, see Grant Paths in User Rights Review Reports.

Note:	Starting with AppDetectivePro 6.3, you can optionally check the Exclude Grant Path from this Report checkbox (in the AppDetectivePro - Report Wizard) to exclude grant path information from the All Effective Privileges for a User Report . For more information on grant paths, see Grant Paths in User Rights Review Reports.
--------------	---

- **Grantee Type.** The type of the user or role assigned the privilege.

Note the following:

- You can run an **All Effective Privileges for a User Report** for multiple users.
- When you run an **All Effective Privileges for a User Report** against a Microsoft SQL Server database, AppDetectivePro may translate both **SELECT** and **UPDATE** table privileges in the database into their respective column privileges. For example, AppDetectivePro may present the **SELECT** privilege on a **USERS** table -- with columns **ID** and **NAME** -- as two **SELECT** privileges: one on the **ID** column of **USERS** and one on the **NAME** column of **USERS**. AppDetectivePro can correctly determine the effect of column-level **DENY** privileges in the case of Microsoft SQL Server 2000, Microsoft SQL Server 2005, and Microsoft SQL Server 2008 instances when the "common criteria compliance enabled" option is turned on. Without the "common criteria compliance enabled" option turned on in Microsoft SQL Server 2005 and Microsoft SQL Server 2008, the interaction between column and table-level **GRANT** and **DENY** privileges is inconsistent with the way **DENY** behaves in other versions of Microsoft SQL Server; for more information, see <http://msdn.microsoft.com/en-us/library/bb326650.aspx>.
- This report can potentially contain a large number of records, which may span multiple pages if you generate an HTML report. You can configure the maximum number of records to display per page. For more information on the HTML report format, see Report Formats.

- Roles are sets of privileges that can be assigned to either a user or another role in a database. When a user or role obtains a privilege in a database, that privilege may be either directly granted to the user or role, or it may be inherited from another role assignment. Subsequently, some AppDetectivePro User Rights Review Reports -- including the **All Effective Privileges for a User Report** -- show this inheritance relationship using a list of users and roles called a grant path. For more information, see Grant Paths in User Rights Review Reports. This report excludes privileges inherited from any public role. Public roles include `PUBLIC` in Oracle, as well as the server-level and database-level public roles in Microsoft SQL Server. This report does **not** display any privileges inherited from any of these roles.

Important!

Application Security, Inc. recommends you run the **All Effective Privileges for a Role Report** on a login rather than a database user for Microsoft SQL Server instances, since logins may be assigned to server roles that affect their privileges as database users. AppDetectivePro does **not** display the privileges granted to a login through server logins when you run an **All Effective Privileges for a Role Report** only on a database user.

Note:

This report can potentially contain a large number of records, which may span multiple pages if you generate an HTML or MHT report. However, you can use the **Properties** branch and configure the maximum amount of records that display per page (for HTML and MHT formats only). For more information on using the **Properties** branch, see Properties. For more information on report formats, see Report Formats.

ALL EFFECTIVE PRIVILEGES FOR A ROLE REPORT

Given a role, the User Rights Review report lists **everything** pertaining to a role in a database, including privileges on tables, stored procedures, functions, views, and system privileges such as the ability to connect to a database or create a table. This report breaks down any umbrella system privileges such as "select from any table" into individual object privileges, and accounts for the effect of any `REVOKEs` or `DENYs` of privileges. You can generate this report for multiple users.

This User Rights Review Report consists of the following **columns**:

- **Privilege.** A description of the privilege granted; for example, `CREATE TABLE`.
- **Type.** Either `System Privilege` or `Object Privilege`. **System privileges** are server-level privileges such as `CREATE TABLE` or `CONNECT TO DATABASE`. **Object privileges** are privileges associated with a particular table, view, stored procedure or any other kind of database object; for example, `SELECT ON SCOTT.BONUS`.
- **Grant Path.** The path, through roles, **from** the user/role selected for this Report **to** the user/role assigned the privilege; for more information on grant paths, see Grant Paths in User Rights Review Reports. Starting with AppDetectivePro 6.3, you can optionally check the **Exclude Grant Path from this Report** checkbox (in the **AppDetectivePro - Report Wizard**) to exclude grant path information from the **All Effective Privileges for a Role Report**. For more information on grant paths, see Grant Paths in User Rights Review Reports.
- **Grantee Type.** The type of the user or role assigned the privilege.

Note the following:

- You can run an **All Effective Privileges for a Role Report** for multiple users.
- When you run an **All Effective Privileges for a Role Report** against a Microsoft SQL Server database, AppDetectivePro may translate both `SELECT` and `UPDATE` table privileges in the database into their respective column privileges. For example, AppDetectivePro may present the `SELECT` privilege on a `USERS` table -- with columns `ID` and `NAME` -- as two `SELECT` privileges: one on the `ID` column of `USERS` and one on the `NAME` column of `USERS`. AppDetectivePro can correctly determine the effect of column-level `DENY` privileges in the case of Microsoft SQL Server 2000, Microsoft SQL Server 2005, and Microsoft SQL Server 2008 instances when the "common criteria compliance enabled" option is turned on. Without the "common criteria compliance enabled" option turned on in Microsoft SQL Server 2005 and Microsoft SQL Server 2008, the interaction between column and table-level `GRANT` and `DENY` privileges is inconsistent with the way `DENY` behaves in other versions of Microsoft SQL Server; for more information, see <http://msdn.microsoft.com/en-us/library/bb326650.aspx>.
- This report can potentially contain a large number of records, which may span multiple pages if you generate an HTML report. You can configure the maximum number of records to display per page. For more information on the HTML report format, see Report Formats.

- Roles are sets of privileges that can be assigned to either a user or another role in a database. When a user or role obtains a privilege in a database, that privilege may be either directly granted to the user or role, or it may be inherited from another role assignment. Subsequently, some AppDetectivePro User Rights Review Reports -- including the [All Effective Privileges for a Role Report](#) -- show this inheritance relationship using a list of users and roles called a grant path. For more information, see Grant Paths in User Rights Review Reports.

This report excludes privileges inherited from any public role. Public roles include `PUBLIC` in Oracle, as well as the server-level and database-level public roles in Microsoft SQL Server. This report does **not** display any privileges inherited from any of these roles. Furthermore, you **cannot** select public roles as targets in this report.

Important!	Application Security, Inc. recommends you run the All Effective Privileges for a Role Report on a login rather than a database user for Microsoft SQL Server instances, since logins may be assigned to server roles that affect their privileges as database users. AppDetectivePro does not display the privileges granted to a login through server logins when you run an All Effective Privileges for a Role Report only on a database user.
-------------------	--

Note:	This report can potentially contain a large number of records, which may span multiple pages if you generate an HTML or MHT report. However, you can use the Properties branch and configure the maximum amount of records that display per page (for HTML and MHT formats only). For more information on using the Properties branch, see Properties. For more information on report formats, see Report Formats.
--------------	--

ALL ROLES FOR A USER

This User Rights Review report lists all roles and system privileges that generate implicit privileges assigned to a particular user. The set of all roles assigned to a user consists of all roles assigned directly to a given user and all roles inherited as a result of direct assignments. For example, if the role `CONNECT` is assigned to the role

OEM_MONITOR -- and the role **OEM_MONITOR** is assigned to the user **SYS** -- then **SYS** is effectively granted all privileges from both **OEM_MONITOR** and **CONNECT**.

Each row of this report lists a single role granted to the user (**Role Granted**), the type of that role (**Role Type**), and the user or role directly responsible for the role grant (**Granted From**). Roles may appear multiple times in the **Role Granted** column if they have been granted both directly and indirectly or if they have been granted indirectly from multiple roles.

This User Rights Review Report consists of the following **columns**:

- **Role Granted.** A role that has been assigned to the chosen user/role.
- **Role Type.** The type of role in the **Role Granted** column.
- **Granted From.** The user/role that was granted the role in the **Role Granted** column. This column explains why the chosen user/role has the role in the **Role Granted** column. For example, if the user **SYS** is granted the **DBA** role, and the **DBA** role is granted the **EXECUTE_CATALOG_ROLE** role, this report run with **SYS** as the chosen user would show **EXECUTE_CATALOG_ROLE** as **Role Granted** and **DBA** as **Granted From**.

ALL ROLES FOR A ROLE

This User Rights Review report lists all roles and system privileges that generate implicit privileges assigned to a given role. The set of all roles assigned to a role consists of all roles and implicit privileges assigned directly to a given role and all roles inherited as a result of direct assignments.

For example, if the role **CONNECT** is assigned to the role **OEM_MONITOR**, and the role **OEM_MONITOR** is assigned to the role **DBA**, then **DBA** is effectively granted all privileges from both **OEM_MONITOR** and **CONNECT**. Each row of this report lists a single role granted to the role (**Role Granted**), the type of that role (**Role Type**), and the role directly responsible for the role grant (**Granted From**). Roles may appear multiple times in the **Role Granted** column if they have been granted both directly and indirectly or if they have been granted indirectly from multiple roles.

This User Rights Review Report consists of the following **columns**:

- **Role Granted.** A role that has been assigned to the chosen user/role.
- **Role Type.** The type of role in the **Role Granted** column.

- **Granted From.** The user/role that was granted the role in the **Role Granted** column. This column explains why the chosen user/role has the role in the **Role Granted** column. For example, if the user `SYS` is granted the `DBA` role, and the `DBA` role is granted the `EXECUTE_CATALOG_ROLE` role, this report run with `SYS` as the chosen user would show `EXECUTE_CATALOG_ROLE` as **Role Granted** and `DBA` as **Granted From**.

OBJECT ACCESS

Given a database object (a table, view, stored procedure, function, etc.), this User Rights Review Report lists all privileges associated with the object. You can generate this report for multiple users.

This User Rights Review Report consists of the following **columns**:

- **Granted To.** The path, through roles, from the user/role who inherits this privilege to the user/role assigned this privilege.
- **Grantee Type.** The type of the user/role who inherits this privilege
- **State.** The privilege state, for example, `GRANT` or `DENY`.
- **Privilege.** The type of privilege; for example, `SELECT`, `UPDATE`, or `EXECUTE`.
- **Object.** The object associated with the privilege. This column may contain sub-objects of the object selected for the report, for example, columns of a table selected or parameters of a function selected.

Note the following:

- You can run an **Object Access** Report for multiple users.
- The **Object Access** Report consists of checkboxes which allow you to filter objects in the following categories: **Table**, **Procedure**, **Function**, **View**, and **Other**. You can filter the object list by selecting one or more object types. By default, all objects are selected (meaning, no filtering is applied).
- This report can potentially contain a large number of records, which may span multiple pages if you generate an HTML report. You can configure the maximum number of records to display per page. For more information on the HTML report format, see Report Formats.

- Roles are sets of privileges that can be assigned to either a user or another role in a database. When a user or role obtains a privilege in a database, that privilege may be either directly granted to the user or role, or it may be inherited from another role assignment. Subsequently, some AppDetectivePro User Rights Review Reports -- including the **Object Access Report** -- show this inheritance relationship using a list of users and roles called a grant path. For more information, see Grant Paths in User Rights Review Reports.

Note:	This report can potentially contain a large number of records, which may span multiple pages if you generate an HTML or MHT report. However, you can use the Properties branch and configure the maximum amount of records that display per page (for HTML and MHT formats only). For more information on using the Properties branch, see Properties. For more information on report formats, see Report Formats.
--------------	--

ALL EFFECTIVE MEMBERS OF A ROLE.

This User Rights Review report allows a you to select a role (or multiple roles) and report on every effective user assigned to that role. The first page of the report displays the selected roles, as well as a graphical, proportional breakdown of how many effective users belong to each role. Subsequent report pages list each individual effective user that belongs to one more of the selected roles, and whether a given effective user was granted the role directly.

This User Rights Review Report consists of the following **columns**:

- **User.** The individual effective user assigned to a selected role.
- **Granted Directly.** Indicates whether the user/role that was granted the role directly (**Yes**) or indirectly (**No**), i.e., via grant paths.

DIFFERENCE REPORTS

Starting with AppDetectivePro 6.2, you can generate User Rights Review Difference Reports. For the purposes of a Differences Report, you should note the following:

- One privilege -- in either the **Differences Report for All Effective Privileges for a User Report** or the **Differences Report for Object Access** -- is equivalent to another if the privilege (for example, `SELECT`, `INSERT`, etc.) and the full object

name (if one exists, for example, `SCOTT.EMP`) match. System privileges, which have no associated object, are compared to each other based solely on the privilege (for example, `CREATE TABLE`).

- One object privilege in the **Differences Report for Object Access** is equivalent to another if the database object, privilege grantee, and principal assigned the privilege are all equivalent. The privilege grantee and the principal assigned the privilege are the two ends of the grant path; for more information on grant paths, see Grant Paths in User Rights Review Reports.

- Privileges may be inherited from multiple sources, so an individual user or role may inherit a particular privilege (for example, `CREATE TABLE`) from multiple sources, but the effect of a privilege is always binary: a user or role either has it or they do not. The **Differences Report for All Effective Privileges for a User** and **Differences Report for All Effective Privileges for a Role** contain the effective differences in privileges, which means they will only report when a privilege has been effectively added or removed.

- For example, if a particular user inherits `CREATE TABLE` from five different sources, then inherits it from three more sources, the `CREATE TABLE` privilege will not show up in the corresponding Differences Report, since there is no change in the user's effective privileges with regard to that privilege (the user had `CREATE TABLE` before, and still has it). On the other hand, if the `CREATE TABLE` privilege is removed from all five sources the user inherits it from, it will show up as a privilege removed in the difference report, since the user has now effectively lost the privilege of `CREATE TABLE`.
- Differences Reports can potentially contain a large number of records, which may span multiple pages if you generate an HTML or MHT report. However, you can use the **Properties** branch and configure the maximum amount of records that display per page (for HTML and MHT formats only). For more information on using the **Properties** branch, see Properties. For more information on report formats, see Report Formats.

Caution!

You should **not** run Difference Reports (i.e., a **Differences Report for All Effective Privileges for a Role** report, a **Differences Report for All Effective Privileges for a User** report, or a **Differences Report for Object Access** report) on snapshots taken with versions of AppDetectivePro earlier than 7.0 because of incompatibilities in the way snapshots are stored. For this reason, **you should only run Differences Reports on User Rights Review scans created with AppDetective Pro 7.0 or later.**

AppDetectivePro includes the following standard Difference Reports:

- **Differences Report for All Effective Privileges for a Role**
- **Differences Report for All Effective Privileges for a User**
- **Differences Report for Object Access.**

Details on each standard Difference Report follow:

- **Differences Report for All Effective Privileges for a Role.** This report allows you to select an application and display all completed User Rights Review scans on the application. Subsequently, you can select two completed and report on the differences between all effective privileges for a selected **role**.

- **Differences Report for All Effective Privileges for a User.** This report allows you to select an application and display all completed User Rights Review scans on the application. Subsequently, you can select two completed scans and report on the differences between all effective privileges for a selected **user**.
- **Differences Report for Object Access.** This report allows you to select an application and display all completed User Rights Review scans on the application. Subsequently, you can select two completed scans and report on the differences between a specific Object, User, or Role.

The **Differences Report for Object Access** Report consists of checkboxes which allow you to filter objects in the following categories: **Table**, **Procedure**, **Function**, **View**, and **Other**. You can filter the object list by selecting one or more object types. By default, all objects are selected (meaning, no filtering is applied).

Note:	Starting with AppDetectivePro 6.3, you can optionally check the Exclude Grant Path from this Report checkbox (in the AppDetectivePro - Report Wizard) to exclude grant path information from any of the Differences Reports (i.e., Differences Report for All Effective Privileges for a Role , Differences Report for All Effective Privileges for a User , and Differences Report for Object Access). For more information on grant paths, see Grant Paths in User Rights Review Reports.
--------------	--

Questionnaire Reports

AppDetectivePro includes the following standard Questionnaire Reports:

- **Audit Findings Detailed**
- **Audit Findings Summary**
- **DAS Questionnaire.**

Details on each standard Questionnaire Report follow:

- **Audit Findings Detailed.** This report displays a detailed view of findings found in an Audit based on the Work Plan(s) ran against it. For more information, see [Interviews, Questionnaires, and Work Plans](#).

- **Audit Findings Summary.** This report displays a summary view of findings found in the audit based on the Work Plan(s) ran against it. For more information, see [Interviews, Questionnaires, and Work Plans](#).
- **DAS Questionnaire.** Generates an XML report of Interview answers and associated data, including check results mapped to the elements of the DISA STIG, including, STIG ID, VKey, and more. For more information, see [Interviews, Questionnaires, and Work Plans](#).

Report Formats

AppDetectivePro generates reports in the following report formats:

- **Crystal Reports.** Generated using Crystal Reports 9.0 and are easily printable. These are also exportable to other formats from within the Crystal Reports viewer.
- **HTML** (i.e., a report that can be viewed in a web browser and is stored in a directory) or **HTML (Single File)** (i.e., the same report generated by the HTML report, but in MHT web archive format so everything is stored in one file).

Certain AppDetectivePro reports can potentially contain a large number of records, which may span multiple pages if you generate an HTML or MHT report.

Specifically, this issue can apply to:

- the **Vulnerability Details** report; for more information, see [Pen Test and Audit Reports](#)
- certain standard User Rights Review reports (i.e., the **All Users in a Database Instance Report**, the **All Roles in a Database Instance Report**, the **All Effective Privileges for a User Report**, the **All Effective Privileges for a Role Report**, and the **Object Access** report); for more information, see [Standard User Rights Review Reports](#)
- all Differences Reports (i.e., the **Differences Report for Object Access** report, the **Differences Report for All Effective Privileges for a User** report, and the **Differences Report for All Effective Privileges for a Role** report); for more information, see [Difference Reports](#).

You can use the **Properties** branch to configure the maximum amount of records that display per page (for HTML and MHT formats only). For more information on using the Properties branch, see [Properties](#). For more information on report formats, see [Report Formats](#).

When an HTML report is paginated, AppDetectivePro creates a folder to store all the files. This folder is the same place where AppDetectivePro stores your reports. The folder name follows the same format as the report names. For example, when AppDetectivePro creates an **All Effective Privileges for a User Report**, and the HTML version of the report is paginated, the folder will have a name like: `All_Effective_Privileges_for_a_User_Report_2009-06-04_12_57_22`. Subsequently, the paginated files in the folder will have names like:

`All_Effective_Privileges_for_a_User_Report_page_1.mht`,
`All_Effective_Privileges_for_a_User_Report_page_2.mht`,
`All_Effective_Privileges_for_a_User_Report_page_3.mht`, and so on.

- **Text.** Report that can be viewed in any text or word processing program.
- **XML.** This is the data source that is used by both HTML reports. It is the bare XML skeleton that can be used to generate custom reports.
- **TMA XML.** Generates XML output intended for use by the TMA and TMA contractors for importing to the TAD system. This option is available for the **Vulnerability Details Report** only.

Running Reports

AppDetectivePro allows you to run reports via the **Report Wizard**, or run a report “on the fly” -- against a single application -- from the network view. This section consists of the following topics:

- Running a Pen Test, Audit, User Rights Review, or Questionnaire Report Using the Report Wizard
- Running an “On the Fly” Report from the Network View.

RUNNING A PEN TEST, AUDIT, USER RIGHTS REVIEW, OR QUESTIONNAIRE REPORT USING THE REPORT WIZARD

The **Report Wizard** allows you to run Reports on your completed Pen Test, Audit, User Rights Review, and Questionnaire data. For a more information on supported:

- Pen Test and Audit Reports, see Pen Test and Audit Reports
- User Rights Review Reports, see User Rights Review Reports
- Questionnaire Reports, see Questionnaire Reports.

To run a Pen Test, Audit, User Rights Review, or Questionnaire Report using the **Report Wizard**:

Step	Action
1	<p>Do one of the following to display the Report Wizard:</p> <ul style="list-style-type: none"> • Choose View > Reports from the menu bar. • Click the Reports button on the toolbar. <p>The Report Wizard dialog box appears.</p>
2	<p>The Report Wizard dialog box allows you to select whether you want to run a Pen Test/Audit Report, a User Rights Review Report, or a Questionnaire Report.</p> <p>If you want to run a:</p> <ul style="list-style-type: none"> • Pen Test or Audit Report, click the Audit and Pen Tests Report tab; for information on available Pen Test and Audit Reports, see Pen Test and Audit Reports • User Rights Review Report, click the User Rights Review Reports tab; for information on available User Rights Review Reports, see User Rights Review Reports • Questionnaire Report, click the Questionnaire Reports tab; for information on available Questionnaire Reports, see Questionnaire Reports.
3	Click a Report type.
4	<p>Click the Next button.</p> <p>AppDetectivePro may prompt you to specify the data sets for Report. For instance, you can run Reports on an entire Session, folder, or a single application. Select the data set you want to use.</p>
5	Click the Next button.

Step	Action
6	<p>AppDetectivePro prompts you to specify a report format, i.e., Crystal Reports, HTML, HTML (Single File), Text, and XML; for more information, see Report Formats.</p> <p>When selecting HTML, HTML (Single File), Text, and XML, you can optionally specify a creation location. By default this location is: <code>%UserProfile%\<LocalAppData>\AppSecInc\AppDetective\Reports</code>. For example:</p> <ul style="list-style-type: none"> • On Windows XP/2003: <code>C:\Documents and Settings\<UserName>\Local Settings\Application Data\AppSecInc\AppDetective\Reports</code> • On Windows Vista/2008: <code>C:\Users\<UserName>\AppData\Local\AppSecInc\AppDetective\Repts</code>
7	<p>Click the Next button.</p> <p>A verification page appears.</p>
8	<p>Confirm the correct report will be generated.</p>
9	<p>Click the Next button.</p> <p>AppDetectivePro generates your report. Crystal reports display in the Crystal Reports viewer. Text reports display in Notepad. HTML and XML reports display in a web browser.</p> <p>AppDetectivePro does not automatically display the DAS Vulnerability report will not be displayed automatically when the report generation finishes. A message box indicating the location where the report has been saved will be showed instead. For more information on the DAS Vulnerability report, see Pen Test and Audit Reports.</p>
10	<p>After you generate your report, the Report Wizard remains open. If you want to:</p> <ul style="list-style-type: none"> • create another report, click the Generate Another Report button to start again from the beginning of the Report Wizard • close the Report Wizard, click the Finish button.

RUNNING AN “ON THE FLY” REPORT FROM THE NETWORK VIEW

AppDetectivePro allows you to run an “on the fly” Report from the network view for a single completed Pen Test, Audit, User Rights Review, or Questionnaire:

Step	Action
1	In the network tree view, locate a completed Pen Test, Audit, User Rights Review, or Questionnaire (you can click the + icons in the tree to expand the nodes).
2	Right click the completed Pen Test, Audit, User Rights Review, or Questionnaire yellow magnifying glass icon. A list of available Reports appears. For more information on available: <ul style="list-style-type: none"> • Pen Test and Audit Reports, see Pen Test and Audit Reports • User Rights Review Reports, see User Rights Review Reports • Questionnaire Reports, see Questionnaire Reports.
3	Choose the available Report that you want to run “on the fly”. AppDetectivePro creates your Report in Crystal Reports format.

Printing and Exporting Reports

Note: This topic applies **only** to Crystal Reports.

AppDetectivePro allows you to print and export Crystal Reports. This section consists of the following topics:

- Printing a Crystal Report
- Exporting a Crystal Report.

PRINTING A CRYSTAL REPORT

To print a Crystal Report:

Step	Action
1	Click the print icon in the toolbar. The Print pop-up appears.
2	Select All or Pages . (If you select Pages , enter the page range you want to print.)
3	Click the OK button.

EXPORTING A CRYSTAL REPORT

AppDetectivePro allows you to export Crystal Reports to different file formats, such as Adobe PDF format.

To export a Crystal Report:

Step	Action
1	Click the export report icon in the toolbar. The Export pop-up appears.
2	Use the Export pop-up to select a report format. AppDetectivePro will export the report data <i>from</i> the Crystal Report format <i>to</i> the selected report format (for example, Adobe Acrobat PDF).
3	Use the Disk File drop-down to save the exported Crystal Report to your hard drive.
4	Click the OK button. The Export Options pop-up appears.
5	Select All or Pages . (If you select Pages , enter the page range you want to export.)
6	Click the OK button. The Choose export file pop-up appears.

Step	Action
7	Specify where on your computer or network you want to export the report, and enter a file name.
8	Click the Save button.

Suppressing Vulnerabilities

AppDetectivePro allows you to suppress vulnerabilities in reports.

To suppress a vulnerability:

Step	Action
1	In the vulnerability view, double click the vulnerability you want to suppress (for more information on the vulnerability view, see Navigating Page Views).
2	Check Suppress this vulnerability .
3	Run the report. The suppressed vulnerability is excluded from the report.

Edit and Tools Menu Tasks

This section consists of the following topics:

- [What are the Edit Menu Tasks?](#)
- [What are the Tools Menu Tasks?](#)
- [Adding an Application to a Session](#)
- [Working with Folders](#)
- [Properties](#)
- [Exporting/Purging Data](#)
- [Importing Data](#)

What are the Edit Menu Tasks?

The AppDetectivePro **Edit** menu allows you to:

- add an application; for more information, see [Adding an Application to a Session](#)
- manage security vulnerabilities found in a Session with the Vulnerability Manager; for more information, see [What is the Vulnerability Manager?](#)
- rename Policies, create a new Policy, edit a selected Policy and set a selected Policy as current (default); for more information, see [What are Policies?](#)
- create your own MS-SQL and Oracle checks in order to add depth to your existing corporate information security policies; for more information, see [What are User-Defined Checks?](#)
- create, move, delete, and rename folders, which you can use to group IP address by business unit or other logical groups; for more information, see [Working with Folders](#)
- view and modify AppDetectivePro properties; for more information, see [Properties](#).

What are the Tools Menu Tasks?

The AppDetectivePro **Tools** menu allows you to:

- export/purge data; for more information, see Exporting/Purging Data
- import data; for more information, see Importing Data
- import a Questionnaire; for more information, see Interview Work Flow Step 2: Importing a Built-In Questionnaire/Creating a Custom Questionnaire (which is part of the Interview Work Flow)

Adding an Application to a Session

AppDetectivePro allows you to add an application to a Session manually. For example, you can add an application that AppDetectivePro did not Discover. You must have an open Session to add an application. If you do not have an open Session, AppDetectivePro prompts you to open a blank Session.

To add an application:

Step	Action
1	Choose Edit > Add Application from the menu bar. The Add Application dialog box appears.
2	Click the IP Address tab. You can: <ul style="list-style-type: none"> • use the DNS Name: drop-down to choose a hostname of the application server and click the Resolve button to populate the IP Address: field, or • enter the IP address of the application server in the IP Address: field.
3	Click the Port tab. You can: <ul style="list-style-type: none"> • use the Default Port drop-down to select a default port, or • enter a single application port in the Single Port field.
4	Click the Platform tab.
5	Use the Application Platform drop-down to select the application platform type.

Step	Action
6	<p>Click the Miscellaneous tab.</p> <p>You can:</p> <ul style="list-style-type: none"> • use the Application Type drop-down to choose the application type, or • enter an application in the Application Name field.
7	<p>Click the Add button.</p> <p>Your new application displays in the Discovery Results window. For more information, see Post-Discovery.</p>

Working with Folders

Folders allow you to group IP address by business unit or other logical groups. This section consists of the following topics:

- Creating a Folder
- Moving an IP Address to a Folder
- Deleting a Folder
- Renaming a Folder.

CREATING A FOLDER

To create a folder:

Step	Action
1	<p>Choose Edit > Folder > from the menu bar.</p> <p>The New folder dialog box appears.</p>
2	<p>Enter the name of the folder.</p>
3	<p>Click the OK button.</p> <p>Your folder displays in the network tree view; for more information, see Navigating Page Views.</p>

MOVING AN IP ADDRESS TO A FOLDER

To move an IP address to a folder:

Step	Action
1	In the network tree view, highlight the IP address you want to move to a folder; for more information, see Navigating Page Views .
2	Choose Edit > Folder > Move to from the menu bar. The Move Folder dialog box appears.
3	Use the Move folder to: drop-down to choose the folder where you want to move the IP address highlighted in the network tree view.
4	Click the OK button. The selected folder contains the IP address.

DELETING A FOLDER

To delete a folder:

Step	Action
1	In the network tree view, highlight the folder you want to delete; for more information, see Navigating Page Views .
2	Choose Edit > Folder > Delete from the menu bar. A pop-up prompts you to confirm the delete.
3	Click the Yes button. The selected folder is deleted.

RENAMING A FOLDER

To rename a folder:

Step	Action
1	In the network tree view, highlight the folder you want to rename; for more information, see Navigating Page Views .
2	Do one of the following: <ul style="list-style-type: none"> • Choose Edit > Folder > Rename from the menu bar • Click the highlighted folder in the network tree view.
3	Rename the folder.

Properties

AppDetectivePro allows you to view and modify application properties, for example, page refresh time, report logos, password parameters, and more. This section consists of the following topics:

- Displaying the Properties Branches
- Understanding the Properties Branches.

DISPLAYING THE PROPERTIES BRANCHES

To display the **Properties** branches, choose **Edit > Properties** from the menu bar. The **Properties** dialog box appears.

UNDERSTANDING THE PROPERTIES BRANCHES

Branch	Description
Screen Refresh	This branch allows you to set the refresh interval of AppDetectivePro during a Session to an arbitrary number of seconds. Also, checking Always run silently places AppDetectivePro into "Silent Mode", which can increase performance at the cost of limited feedback during Discovery and testing phases.

Branch	Description
<p>Reports</p>	<p>This branch allows you to:</p> <ul style="list-style-type: none"> display your company name on AppDetectivePro reports display your company logo on AppDetectivePro reports by checking Select a logo for use on the reports and browsing for graphic files. <p>Some Audits and Pen Tests crack passwords. To:</p> <ul style="list-style-type: none"> hide cracked user passwords in AppDetectivePro reports using *****, check Hide Cracked Passwords. If Hide Cracked Passwords is checked, then when a listener password <i>is</i> provided, AppDetectivePro sends it encrypted over the network. display cracked passwords in reports, uncheck Hide Cracked Passwords. <p>Certain AppDetectivePro reports can potentially contain a large number of records, which may span multiple pages if you generate an HTML or MHT report. Specifically, this issue can apply to:</p> <ul style="list-style-type: none"> the Vulnerability Details report; for details, see Pen Test and Audit Reports. certain standard User Rights Review reports (i.e., the All Users in a Database Instance Report, the All Roles in a Database Instance Report, the All Effective Privileges for a User Report, the All Effective Privileges for a Role Report, and the Object Access report); for details, see Standard User Rights Review Reports all Differences Reports (i.e., the Differences Report for Object Access report, the Differences Report for All Effective Privileges for a User report, and the Differences Report for All Effective Privileges for a Role report); for details, see Difference Reports. the Audit Finding Details report; for details, see Questionnaire Reports. <p>Use this branch to configure the maximum amount of records that display per page (for the HTML and HTML (Single File) formats only). Specifically, you can configure the maximum number of records that display per page in:</p> <ul style="list-style-type: none"> Vulnerability Details reports, by entering a maximum amount of records to display per page in the Vulnerability Assessment reports: field (default value = 10000 records) applicable User Rights Review reports—and all Differences Report pages—by entering a maximum amount of records to display per page in the User Rights Review reports: field (default value = 10000 records). You can enter a value of 0 records per page to disable report pagination. Audit Finding Details reports, by entering a maximum number of records to display per page in the Interview Questionnaire reports: field.

Branch	Description
Backend Timeout	<p>This branch allows you to enter a command timeout, which specifies the maximum number of seconds AppDetectivePro will wait for a SQL command to complete. This is only for SQL commands that have been executed against its backend database. In order for this value to take effect, restart AppDetectivePro. Changing this value may result in unpredictable AppDetectivePro behavior. Specify zero seconds for infinite timeout.</p>
<p>Database (for Access) or Backend Database Info (for Microsoft SQL Server)</p>	<ul style="list-style-type: none"> • Database. This branch allows you to provide a facility for compacting the AppDetectivePro back-end database. This can result in significant space saving. (This branch is available only with Microsoft Access.) • Backend Database Info. This branch allows you to change the Microsoft SQL Server authentication user name and password that you created during the database installation. Available only for Microsoft SQL Server back-end. This option only displays if you choose Microsoft SQL Server authentication when you install a Microsoft SQL Server back-end database. <p>This option is not available if you select Windows Authentication when you install a Microsoft SQL Server back-end database. Nor is this option available if you switch to Microsoft SQL Server authentication after initially selecting Windows Authentication.</p>

Branch	Description
Tracing	<p>This branch allows you to set tracing, i.e., the amount of detail AppDetectivePro collects in log files for the purposes of troubleshooting AppDetectivePro problems with Application Security, Inc. Support. The default tracing level is Normal. If you modify the tracing level, and perform an ASAP Update, the tracing level automatically returns to Normal. For more information on ASAP Updates, see Performing an ASAP Update.</p> <p>The most verbose level of tracing (Debug) provides the most detail to Application Security, Inc. Support and can expedite troubleshooting. However, a verbose level of tracing can also slow AppDetectivePro performance. In contrast, the least verbose level of tracing (Critical) will not slow down AppDetectivePro performance as much as a more verbose level, but the tracing log files will not be as detailed and may hinder Application Security, Inc. Support's abilities to troubleshoot your AppDetectivePro problems.</p> <p>The Tracing Level: lever allows you to select the AppDetectivePro tracing level, which controls the volume of log information AppDetectivePro outputs to its log file. You can select:</p> <ul style="list-style-type: none"> • Debug (the most verbose level) • Normal (default value) • Warning • Error • Critical (the least verbose level) • Off (to de-activate tracing). <p>AppDetectivePro also includes System Auditing, an audit tracing component that tracks user actions (events). These events are logged to a log file and in the Windows Event Log. You can modify the System Auditing settings under the Tracing branch. Specifically, if you want to:</p> <ul style="list-style-type: none"> • log events into a log file, check Log events into a log file • log events into the Windows Event Log, check Log events into Windows Event Log • turn off System Auditing, uncheck Enable System Auditing. <p>For more information on System Auditing, see Appendix O: Oracle Critical Patch Update Detection.</p> <p>Collected tracing logs are located by default in the following location: <code>c:\Program Files\AppSecInc\ AppDetective\logs\</code>. When troubleshooting an AppDetectivePro problem, Application Security, Inc. Support may ask you to send the tracing log file(s).</p>

Branch	Description
Discovery	<p>This branch allows you to change the AppDetectivePro's Discovery parameters. This tab consists of these sub-branches:</p> <ul style="list-style-type: none"> Network Adapter. Use the drop-down to specify which adapter to use for port scanning. When you select a network adapter, the Properties dialog box displays the following adapter parameters: IP Address, Netmask, and Gateway. <p>Before you can run a Discovery, you must select the network adapter. If you do not, AppDetectivePro will not let you run a Discovery.</p> <ul style="list-style-type: none"> Port Scanning. This sub-branch allows you to specify the rate at which AppDetectivePro scans ports during a Discovery. You can modify the number of packets in a single burst (default = 100), milliseconds between bursts (default = 10), or milliseconds for final delay (default = 10000). <p>This sub-branch also contains a Scan ports even if IP is not responding checkbox. If unchecked (default), AppDetectivePro probes one port (for each IP address) to determine if the machine is responsive. If the machine is <i>responsive</i>, Discovery probes <i>all</i> ports for the IP address to scan applications. If the machine is <i>unresponsive</i>, Discovery ends for this IP address. AppDetectivePro does not probe the rest of the ports for this IP address. If checked, AppDetectivePro probes all ports of each IP address to scan applications.</p> <ul style="list-style-type: none"> App Detection. This sub-branch allows you to specify Discovery options related to application detection. There is a slight delay between each connection attempt when AppDetectivePro detects applications. This delay prevents the Discovery from creating a “bottleneck” on your network. This sub-branch allows you to modify the number milliseconds between connections (default = 10). <p>AppDetectivePro also allows you to detect multiple applications simultaneously. This sub-branch allows you to modify the applications at once number, i.e., the maximum number of applications AppDetectivePro detects simultaneously (default = 256). An appropriate timeout is required when AppDetectivePro detects applications. If you increase the timeout interval (in the Wait for a response up to field), the overall Discovery time increases. If the timeout value is too low, AppDetectivePro may not Discover all applications. The default value (10 seconds) is recommended.</p> <ul style="list-style-type: none"> Discover HTTP web servers. This sub-branch allows you to specify whether you want to Discover HTTP web servers (unchecked by default).

Branch	Description
Pen Testing/ Auditing	<p>This branch allows you to set the parameters for use during a Pen Test or Audit. This branch consists of six sub-branches.</p> <ul style="list-style-type: none"> • Timeout. This sub-branch allows you to enter a value (in seconds) in the following fields: <ul style="list-style-type: none"> - Wait for a response up to __ second(s). AppDetectivePro requires a timeout when it Audits an application. If the application being Audited is slow to respond, you may need to increase the value. The default value is 30 seconds. - Default SSH/Telnet connection timeout: __ second(s). AppDetectivePro requires a timeout it when connecting to the host machine's operating system during an Audit. If the machine being Audited is slow to respond, you may need to increase the value. The default value is 180 seconds. <p>AppDetectivePro uses the SSH/Telnet connection timeout value specified above as the default timeout value for all Audits. You can modify the timeout for an individual Audit in the Connections Details dialog box when you schedule an Audit; for more information, see <i>Scheduling an Audit Job</i>.</p> • Concurrency. When you run a Pen Test or Audit, you can run multiple tests simultaneously. By setting the value, you can configure how many tests to run simultaneously. • Oracle. Allows you to select whether to use the Java Method or the OS Method to check whether an Oracle CPU has been applied to the target database. By default, AppDetectivePro uses the OS Method. For more information, see Appendix O: Oracle Critical Patch Update Detection. • Lotus Domino. Resets the Lotus Groupware Session after a specified number of connections has been made. This will free up cached memory used by the Lotus APIs.

Branch	Description
<p>Pen Testing/ Auditing (cont'd)</p>	<ul style="list-style-type: none"> • Microsoft SQL Server. <ul style="list-style-type: none"> - Attempt to use Windows Authentication when performing a Pen Test on Microsoft SQL Server. Uncheck this option to force AppDetectivePro to skip this step, which enhances information gathering. - Connect to Microsoft SQL Servers via Named Pipes. Check this option to force AppDetectivePro to use named pipes. You must check this option if you want to Audit a Microsoft SQL Server database (using Windows Authentication) against a machine on a different or untrusted domain. Additional steps are required. For more information, see Auditing Microsoft SQL Server (Using Windows Authentication) Against a Machine on a Different or Untrusted Domain. <p>AppDetectivePro does not support Pen Testing any Microsoft SQL Server instances which use named pipes for connection.</p> • DB2 Mainframe. Allows you to select which security option AppDetectivePro should use to authenticate a DB2 mainframe application. You can select: <ul style="list-style-type: none"> - Use authentication value in server's DBM configuration - Client authentication - Server authentication - Server authentication with encryption - DDCS authentication - DDCS authentication with encryption. • Operating System Checks. When attempting to connect to an operating system via Telnet or SSH, the success or failure of the connection attempt is determined by the response of the remote machine to the login/password combination that is sent. Some default patterns have already been entered for searching for a successful connection. If the current strings do not allow you to perform OS level checks on UNIX machines, you will have to provide a pattern that is present in the login page for your system. <p>Enter a definitive response string indicating a success or failure in the text field, and add it by clicking the Add button. Uncheck the Denotes Success checkbox if this string displays when the user/password pair has been rejected. To remove a response string, select the row and click the Remove button.</p>

Branch	Description
Passwords	<p>This branch allows you to set AppDetectivePro password parameters.</p> <ul style="list-style-type: none">• Oracle Listener. This tab allows you to enter a default value to try as the Oracle Listener password.

Branch	Description
Check Point Info	<p>AppDetectivePro allows you to forward Pen Test and Audit results to a Check Point Event Logging Server (Check Point SmartView Tracker). This branch allows you to send a log entry for every vulnerability a Check Point Event Logging Server. For more information, see Appendix L: Check Point Logging Properties Installation.</p> <p>This branch consists of the following fields:</p> <ul style="list-style-type: none"> • Enable Check Point SmartCenter Server logging. Check to enable logging capability. • Authentication Type. Allows you to specify an authentication method. Check Point provides several methods. Application Security, Inc. recommends SSLCA for log sending. • Target Server IP Address. Allows you to specify the server machine where Check Point SmartCenter Server is installed. • Target Server Port. Allows you to specify the port on the server machine where the Check Point ELA Server is enabled. • Target SIC Name. This field allows you enter the Secure Internal Communication (SIC) name of your Check Point SmartCenter Server. SIC is Check Point’s proprietary internal communication method for the components within a Next Generation (NG) Check Point System. In order for AppDetectivePro to communicate with a Check Point SmartCenter server in SSLCA mode, the SIC name of the Check Point SmartCenter Server is required. • Client SIC Name. For SSLCA authentication, Check Point requires each client to be registered on Check Point SmartCenter Console. This field allows you to add the computer where AppDetectivePro is installed. • P12 Key File. Allows you to enter the location of the .p12 file generated after you execute the <code>opsec_pull_certificate.exe</code> command. You can click the Browse button to search for the .p12 file on your computer.

Exporting/Purging Data

AppDetectivePro allows you to:

- **export Session data** to a Microsoft Access database file other than the one used by AppDetectivePro (i.e., [AppDetective.mdb](#)) and **Policies** (including any user-defined checks in the Policy)
- **purge default database data** (the [AppDetective.mdb](#) file is located in: [C:\Program Files\AppSecInc\AppDetective](#)) and **Policies** (including any user-defined checks in the Policy).

Note: Purged and exported data includes all Session data (including Pen Test, Audit, or User Rights Review data) contained in a given Session.

This section consists of the following topics:

- Exporting Data
- Purging Data.

EXPORTING DATA

To export data:

Step	Action
1	Choose Tools > Export/Purge Data from the menu bar. The Import/Export/Purge Data dialog box appears.
2	Click one of the following tabs: <ul style="list-style-type: none"> • Export/Purge Session • Export/Purge Policy.
3	Highlight the Session or Policy you want to export. You can preview the Session by checking Preview session selected above.
4	Click the Export button. The Export dialog box appears.
5	Specify the path and file name of the new database or Policy file.

Step	Action
6	Click the Save button. A pop-up appears, notifying you AppDetectivePro has exported your Session data or Policy as an AppDetectivePro database file (.adb).
7	Click the OK button.

PURGING DATA

To purge data:

Step	Action
1	Choose Tools > Export/Purge Data from the menu bar. The Import/Export/Purge Data dialog box appears.
2	Click the Export/Purge session tab (default).
3	Highlight the Session you want to purge.
4	Click the Purge button. A pop-up prompts you to confirm the purge. Check Do not ask me this again to prevent AppDetectivePro from displaying the confirmation pop-up. If your AppDetectivePro back-end database is Microsoft Access, you may receive the following error while purging a User Rights Review: File sharing lock count exceeded. Increase MaxLocksPerFile registry entry. For information on troubleshooting this error, see Running User Rights Review With an Access Back-End.
5	Click Yes . AppDetectivePro purges your Session data.

Importing Data

AppDetectivePro allows you to import Session or Policy data from a database. This is useful if you want to transfer Sessions or Policies between machines, or use Sessions from a prior installation.

Note:	Imported Policies include any user-defined checks that are part of the Policy.
--------------	--

To import data:

Step	Action
1	Choose Tools > Import Data from the menu bar. The Import/Export/Purge Data dialog box appears.
2	Click one of the following tabs: <ul style="list-style-type: none"> • Import Session • Import Policy.
3	Click the Set Import File button. The Set Import File dialog box appears.
4	Specify the path and file name of the AppDetectivePro database file (.adb). You can preview the Session by checking Preview session selected above.
5	Click the Import button. A pop-up appears, notifying you AppDetectivePro has exported your Session or Policy data as an AppDetectivePro database file (.adb). The imported Session or Policy is now available.

Job Scheduler

This section consists of the following topics:

- [What is the Job Scheduler?](#)
- [Scheduling a Job](#)
- [Generating a Job Report](#)

What is the Job Scheduler?

The [Job Scheduler](#) allows you to specify the date and time when you want to run a task, such as a Pen Test or Audit.

Caution!	You cannot use the Job Scheduler for User Rights Reviews. For more information, see Pen Tests, Audits, and User Rights Reviews.
-----------------	--

For example, you can use the [Job Scheduler](#) to perform a weekly Pen Test of your Oracle servers starting at 2:30 A.M every Saturday, then have AppDetectivePro email you the results in a Report.

The [Job Scheduler](#) consists of the following tabs:

- **Job Queue.** Allows you to view all AppDetectivePro jobs currently scheduled; for more information, see Job Queue Tab and Viewing/Deleting Scheduled Jobs in the Job Queue
- **Search for Applications.** Allows you to schedule a Discovery; for more information, see Search for Applications Tab and Scheduling a Discovery Test Job
- **Run Pen Test.** Allows you to schedule a Pen Test; for more information, see Run Pen Test Tab and Scheduling a Pen Test Job
- **Run Audit.** Allows you to schedule an Audit; for more information, see Run Audit Tab and Scheduling an Audit Job
- **ASAP Update.** Allows you to schedule an AppDetectivePro upgrade to the latest version; for more information, see ASAP Update Tab and Scheduling an ASAP Update Job
- **Logging.** Allows you to view logged job data; for more information, see Logging Tab and Refreshing and Pruning the AppDetectivePro Log File.

JOB QUEUE TAB

This tab allows you to view and/or delete jobs currently scheduled. It consists of the following buttons:

- **Close.** Click to close the **Job Scheduler**.
- **Delete Job.** Click to delete a highlighted job from the queue.
- **Refresh List.** Click to refresh the displayed list of jobs.

SEARCH FOR APPLICATIONS TAB

This tab allows you to schedule a Discovery. It consists of the following parts:

- **Single Host tab.** Allows you to enter the IP address or hostname for a single host. You can click the **Resolve** button to obtain the machine name if available.
- **Range tab.** Allows you to enter the IP address range to use when Discovering a range of IPs. You can also enter the starting and ending IP addresses.
- **Discover Default Ports tab.** Allows you to select well-known application ports that you want to Discover.
- **Discover Range of Ports tab.** Allows you to perform a Discovery against a range of ports. Enter the starting and ending port range to Discover.
- **Create Job button.** Click to set up the time to run the job as well as what reports to generate.

RUN PEN TEST TAB

This tab lets you schedule a Pen Test. The following options are available:

- **Application checkboxes.** Check the applications you want to Pen Test.
- **Policy to Use drop-down.** Choose the Policy to use for the scheduled Pen Test.
- **Create Job button.** Opens the next window which will set up the time to run the job as well as what reports to generate.

RUN AUDIT TAB

This tab lets you schedule a Security Audit. The following options are available:

- **Checkboxes.** Check the applications you want to Audit.
- **Policy to Use drop-down.** Choose the Policy to use for the scheduled Audit.

- **Change Info button.** Click this button to change the login information for the selected application to be Audited.

Note: AppDetectivePro encrypts your password in its back-end database.

- **Create Job button.** Opens the next window which will set up the time to run the job as well as what reports to generate.

ASAP UPDATE TAB

This tab allows you to schedule downloads of the latest AppDetectivePro update. The following options are available:

- **Create Job button.** Opens the next window which will set up the time to run the job as well as what reports to generate.

LOGGING TAB

This tab allows you to view and manage the contents of the job log. The following options are available:

- **Refresh.** Updates the log on the page.
- **Prune Log.** Clears the log.

Scheduling a Job

The [Job Scheduler](#) allows you to schedule a job (for example, a Pen Test, an Audit, a Discovery, or an ASAP Update).

Caution! You **cannot** use the [Job Scheduler](#) for User Rights Reviews. For more information, see Pen Tests, Audits, and User Rights Reviews.

For each scheduled job, you can, among other details, specify its:

- **Frequency**, i.e., the interval for which you want to run the job (for example, daily)
- **Time**, i.e., the time when you want to run the job (for example, 12:00 PM).

Note: To schedule a Pen Test or Audit job, you **must** open a Session with Discovered applications.

The [Job Scheduler](#) also allows you to:

- view and/or delete scheduled jobs in the job queue
- refresh and prune the AppDetectivePro log file.

For more information on:

- scheduling an Audit job, see [Scheduling an Audit Job](#)
- scheduling a Pen Test job, see [Scheduling a Pen Test Job](#)
- scheduling a Discovery job, see [Scheduling a Discovery Test Job](#)
- scheduling an ASAP Update job, see [Scheduling an ASAP Update Job](#)
- viewing and/or deleting scheduled jobs in the job queue, see [Viewing/Deleting Scheduled Jobs in the Job Queue](#)
- refresh and prune the AppDetectivePro log file, see [Refreshing and Pruning the AppDetectivePro Log File](#).

SCHEDULING AN AUDIT JOB

The [Job Scheduler](#) allows you to schedule an Audit job. An Audit tests the security of your application using an “inside out” approach. Audits require that you already have access to a system, such as Oracle. The Audit checks your Discovered applications for password configurations, table access, user roles, and other vulnerabilities. For more information on Audits, see [What are Pen Tests, Audits, and User Rights Reviews?](#)

To schedule an Audit job:

Step	Action
1	Do one of the following: <ul style="list-style-type: none">• Choose Run > Job Scheduler from the menu bar.• Click the Schedule button. The Job Scheduler dialog box appears.
2	Click the Run Audit tab. The Audit job scheduling portion of the Job Scheduler dialog box appears.

Step	Action
3	<p>The following options are available:</p> <ul style="list-style-type: none"> • Checkboxes. Check the applications you want to Audit. • Policy to Use drop-down. Choose the Policy to use for the scheduled Audit. • Change Info button. Click this button to display the Connection Details dialog box and change the current login information for the selected application to be Audited; for more information, see Understanding the Connection Details Dialog Box. <p>AppDetectivePro encrypts your password in its back-end database.</p>
4	<p>Click the Create Job button.</p> <p>The Date/Time To Run: portion of the Job Scheduler dialog box appears.</p>
5	<p>The Date/Time To Run: portion of the Job Scheduler dialog box allows you to:</p> <ul style="list-style-type: none"> • specify the date/time when you want to run your Audit job, as well as the frequency (i.e., Daily, Monthly, etc.) • generate an Application Inventory or Application Banners Job Report; for more information see Generating a Job Report.

SCHEDULING A PEN TEST JOB

The [Job Scheduler](#) allows you to schedule a Pen Test job. A Pen Test assesses the security of your applications by running security checks (based on a Policy you choose). Pen Tests:

- are run from an “outside-in” perspective
- give a good simulation of what a hacker or intruder might try in order to get past your application defenses
- commonly uncover mis-configuration errors in addition to well-known application vulnerabilities.

For more information on Pen Tests, see [What are Pen Tests, Audits, and User Rights Reviews?](#)

To schedule a Pen Test job:

Step	Action
1	<p>Do one of the following:</p> <ul style="list-style-type: none"> • Choose Run > Job Scheduler from the menu bar. • Click the Schedule button. <p>The Job Scheduler dialog box appears.</p>
2	<p>Click the Run Pen Test tab.</p> <p>The Pen Test job scheduling portion of the Job Scheduler dialog box appears.</p>
3	<p>The following options are available:</p> <ul style="list-style-type: none"> • Application checkboxes. Check the applications you want to Pen Test. • Policy to Use drop-down. Choose the Policy to use for the scheduled Pen Test.
4	<p>Click the Create Job button.</p> <p>The Date/Time To Run: portion of the Job Scheduler dialog box appears.</p>
5	<p>The Date/Time To Run: portion of the Job Scheduler dialog box allows you to:</p> <ul style="list-style-type: none"> • specify the date/time when you want to run your Pen Test job, as well as the frequency (i.e., Daily, Monthly, etc.) • generate a: <ul style="list-style-type: none"> -User Information Report -Check Status for all apps Job Report -Check Status for each app Job Report -Vulnerability Details for all apps Job Report -Vulnerability Details for each app Job Report -Vulnerability Summary for all apps Job Report -Vulnerability Summary for each app Job Report. <p>For more information, see Generating a Job Report.</p>

SCHEDULING A DISCOVERY TEST JOB

The [Job Scheduler](#) allows you to schedule a Discovery job. When AppDetectivePro performs a Discovery, it:

- locates applications on your network
- identifies the applications' IP addresses (as well as ports used to provide network services)
- automatically creates a Session (a prerequisite to the Pen Test or Audit).

For more information, see [What is Discovery?](#)

To schedule a Discovery job:

Step	Action
1	Do one of the following: <ul style="list-style-type: none"> • Choose Run > Job Scheduler from the menu bar. • Click the Schedule button. The Job Scheduler dialog box appears.
2	Click the Search for Applications tab. The Discovery job scheduling portion of the Job Scheduler dialog box appears.
3	The following sub-tabs are available: <ul style="list-style-type: none"> • Single Host tab. Allows you to enter the IP address or hostname for a single host. You can click the Resolve button to obtain the machine name if available. • Range tab. Allows you to enter the IP address range to use when Discovering a range of IPs. You can also enter the starting and ending IP addresses. • Discover Default Ports tab. Allows you to select well-known application ports that you want to Discover. • Discover Range of Ports tab. Allows you to perform a Discovery against a range of ports. Enter the starting and ending port range to Discover.

Step	Action
4	Click the Create Job button. The Date/Time To Run: portion of the Job Scheduler dialog box appears.
5	The Date/Time To Run: portion of the Job Scheduler dialog box allows you to: <ul style="list-style-type: none"> • specify the date/time when you want to run your Discovery job, as well as the frequency (i.e., Daily, Monthly, etc.) • generate an Application Inventory or Application Banners Job Report; for more information see Generating a Job Report.

SCHEDULING AN ASAP UPDATE JOB

The **Job Scheduler** allows you to schedule an ASAP Update job. The ASAP Update feature allows you to update AppDetectivePro to the latest version. Updates generally contain new security checks for Pen Tests and Audits, as well as performance enhancements and new features. For more information, see [Performing an ASAP Update](#).

To schedule an ASAP Update job:

Step	Action
1	Do one of the following: <ul style="list-style-type: none"> • Choose Run > Job Scheduler from the menu bar. • Click the Schedule button. The Job Scheduler dialog box appears.
2	Click the ASAP Update tab. The ASAP Update job scheduling portion of the Job Scheduler dialog box appears.
3	Click the Create Job button. The Date/Time To Run: portion of the Job Scheduler dialog box appears.

Step	Action
4	The Date/Time To Run: portion of the Job Scheduler dialog box allows you to specify the date/time when you want to run your ASAP Update job, as well as the frequency (i.e., Daily, Monthly , etc.).

VIEWING/DELETING SCHEDULED JOBS IN THE JOB QUEUE

The **Job Scheduler** allows you to view and/or delete jobs currently scheduled.

To view/delete a scheduled job in the job queue:

Step	Action
1	Do one of the following: <ul style="list-style-type: none"> • Choose Run > Job Scheduler from the menu bar. • Click the Schedule button. The Job Scheduler dialog box appears.
2	Click the Job Queue tab. The job queue portion of the Job Scheduler dialog box appears.
3	You can: <ul style="list-style-type: none"> • view the Date, Time, and Command to Run for all scheduled jobs • click the Close button to close the Job Scheduler. • highlight a scheduled jobs and click the Delete Job button to delete it from the queue. • click the Refresh List to refresh the displayed list of jobs.

REFRESHING AND PRUNING THE APPDETECTIVEPRO LOG FILE

The **Job Scheduler** allows you to view and manage the contents of the job log.

To refresh and prune the AppDetectivePro log file:

Step	Action
1	<p>Do one of the following:</p> <ul style="list-style-type: none"> • Choose Run > Job Scheduler from the menu bar. • Click the Schedule button. <p>The Job Scheduler dialog box appears.</p>
2	<p>Click the Logging tab.</p> <p>The job log portion of the Job Scheduler dialog box appears.</p>
3	<p>You can:</p> <ul style="list-style-type: none"> • view the contents of the job log; for example: <pre>[2007-06-07 16:58:46] Added a job for [6/21/2007@5:03 P.M.]: Scheduled Penetration Test with SessionID 1 using the Evaluation (Built-in) policy, send reports to 'schnore@gmail.com', SMTP ip address , SMTP port 25, reports to generate: User Information</pre> <ul style="list-style-type: none"> • click the Refresh button to update the log on the page • highlight a log and click the Prune log button to clear the log.

Generating a Job Report

If you are scheduling a Discovery, Audit, or a Pen Test job, you can generate a Job Report in the **Date/Time To Run:** portion of the **Job Scheduler** dialog box. Different report types exist for Discoveries, Pen Tests, and Audits. For more information, see [Scheduling an Audit Job](#), [Scheduling a Pen Test Job](#), and [Scheduling a Discovery Test Job](#), respectively.

To generate a [Job Report](#):

Step	Action
1	<p>Schedule your Audit, Pen Test, or Discovery job. For more information, see Scheduling an Audit Job, Scheduling a Pen Test Job, and Scheduling a Discovery Test Job, respectively.</p>

Step	Action
2	Display the Date/Time To Run: portion of the Job Scheduler dialog box.
3	Check which report(s) you want to generate. Different report types exist for Discoveries, Pen Tests, and Audits.
4	<p>Choose where to send the reports.</p> <ul style="list-style-type: none">• Email Reports. Choose this option if you would like the report sent to you via email. <p>AppDetectivePro will prompt you for your account and password.</p> <ul style="list-style-type: none">• Email Address. Enter your email address.• Email Settings. Set up your email settings by clicking the Change Info button.<ul style="list-style-type: none">-Server. Enter the IP address of your SMTP server.-Port. Enter the port of your SMTP Server.-Use Authentication. Enables authentication.-User. Enter the user name.-Password. Enter the password.• Save Reports to a Directory. Choose this option if you would like the report to be saved as a file.
5	Click the Browse button to select a destination location for the report.

Vulnerability Manager

This section consists of the following topics:

- [What is the Vulnerability Manager?](#)
- [Working With Filters](#)
- [Checking For Vulnerabilities](#)
- [Exporting Vulnerabilities](#)
- [Deleting Vulnerabilities](#)

What is the Vulnerability Manager?

The [Vulnerability Manager](#) allows you to manage security vulnerabilities found in a Session. You can apply filters to help you assess the status of various application vulnerabilities.

Working With Filters

This section consists of the following topics:

- [Adding a Filter](#)
- [Modifying a Filter](#)
- [Deleting a Filter](#)

ADDING A FILTER

To add a filter:

Step	Action
1	Click the Add Filter button on the Vulnerability Manager . A numbered filtered tab is added to the Vulnerability Manager .
2	Choose Risk Level from the filter drop-down to filter all vulnerabilities by risk level. You can check one to four of the risk level checkboxes (High , Medium , Low , and Informational).

Step	Action
3	<p>Choose Vulnerability from the filter drop-down to filter vulnerabilities that contain specific words. In the Search Patterns portion of the dialog box you can select:</p> <ul style="list-style-type: none">• Contains and enter specific, comma-separated search values in the field• Equals and choose a pre-set value from the drop-down (for example, 404 Redirection).
4	<p>Choose IP Address from the filter drop-down to filter vulnerabilities based on a single IP address, or a range of IP addresses. In the Search Patterns portion of the dialog box you can select:</p> <ul style="list-style-type: none">• Range and enter a range of comma-separated IP address in the field. <p>Note: To enter a range of IP addresses, use a dash to separate your beginning and ending values.</p> <ul style="list-style-type: none">• Equals and choose a pre-set IP address from the drop-down.
5	<p>Choose Port from the filter drop-down to filter vulnerabilities based on a single port or a range of ports. In the Search Patterns portion of the dialog box you can select:</p> <ul style="list-style-type: none">• Range and enter a range of comma-separated ports in the field. To enter a range of ports, use a dash to separate your beginning and ending values.• Equals and choose a pre-set port from the drop-down.
6	<p>Choose Application Type from the filter drop-down to filter vulnerabilities based on a single application or a range of applications. In the Search Patterns portion of the dialog box you can select:</p> <ul style="list-style-type: none">• Contains and enter specific, comma-separated applications in the field. To enter a range of applications, use a dash to separate your beginning and ending values.• Equals and choose a pre-set application from the drop-down.

Step	Action
7	<p>Do the following:</p> <ul style="list-style-type: none"> • Choose Test Time from the filter drop-down to filter vulnerabilities based on the date and time when a test was performed. • In the From: and To: date portions of the dialog box, you can click the Change Date button to display the Date pop up, which allows you to use the time and calendar drop-downs and specify the From: and To: times and dates for your filter. • When you're done, click the Set Date button.
8	<p>Check for application vulnerabilities; for more information, see Checking For Vulnerabilities.</p>

MODIFYING A FILTER

To modify a filter:

Step	Action
1	<p>Click a numbered filter tab in the Vulnerability Manager dialog box.</p>
2	<p>Use the filter drop-down to modify any of the following filter items:</p> <ul style="list-style-type: none"> • Risk Level • Vulnerability • IP Address • Port • Application Type • Test Time
3	<p>Check for application vulnerabilities; for more information, see Checking For Vulnerabilities.</p>

DELETING A FILTER

To delete a filter:

Step	Action
1	Click a numbered filter tab in the Vulnerability Manager dialog box.
2	Click the Delete Filter button. Your filter is deleted from the Vulnerability Manager .

Checking For Vulnerabilities

After you create or modify filters in the **Vulnerability Manager**, you can check for vulnerabilities.

To check for vulnerabilities:

Step	Action
1	Click a numbered filter tab in the Vulnerability Manager dialog box.
2	Check Show only latest tests to show only the latest tests performed on an application.
3	Click the Show Results button. Your filtered vulnerability results display in the results pane of the Vulnerability Manager , sorted by: Test Time , Risk Level , Vulnerability , IP Address , Port , Application Type , Suppress (Yes/No) , and Details .

Exporting Vulnerabilities

After you check for vulnerabilities, you can export results as an Excel `.csv` or text (`.TXT`) file.

To export vulnerabilities:

Step	Action
1	<p>Highlight one or more vulnerabilities in the results pane of the Vulnerability Manager.</p> <p>You can select multiple, consecutive vulnerabilities by highlighting the vulnerability names and pressing <code><SHIFT></code>. You can select multiple, non-consecutive vulnerabilities by highlighting the check names and pressing <code><CTRL></code>.</p>
2	<p>Click the Export button.</p> <p>The Export... pop-up appears.</p>
3	<p>You can select:</p> <ul style="list-style-type: none"> • Export all records displayed in the Vulnerability Manager to export all vulnerabilities, or the • Export only the selected records to export the vulnerabilities selected in Step 1.
4	<p>In the Select the fields to export portion of the Export... pop-up, check (or uncheck) the following checkboxes to include (or remove) the respective vulnerability data in your Excel <code>.csv</code> or text (<code>.TXT</code>) file:</p> <ul style="list-style-type: none"> • Test Time • Risk Level • Vulnerability • IP Address • Port • Application • Details.

Step	Action
5	Click the Export button. The Save As dialog box appears.
6	Do one of the following: <ul style="list-style-type: none"> • use the Save in drop-down to choose where you want to save the exported vulnerability file • enter the vulnerability file name in the File name field • use the Save as type drop down to choose the file format, i.e., Excel (.csv) or text (.txt) file • click the Save button to export the vulnerability file. Your vulnerability file is exported to the chosen location.

Deleting Vulnerabilities

You can delete vulnerabilities from the **Vulnerability Manager**.

Caution!	This process is irreversible.
-----------------	-------------------------------

To delete a vulnerability:

Step	Action
1	Highlight one or more vulnerabilities in the results pane of the Vulnerability Manager . You can select multiple, consecutive vulnerabilities by highlighting the vulnerability names and pressing <SHIFT>. You can select multiple, non-consecutive vulnerabilities by highlighting the check names and pressing <CTRL>.
2	Click the Delete button. AppDetectivePro prompts you to confirm the delete.
3	Click the Yes button to delete the highlighted vulnerabilities. The vulnerabilities are deleted from the results pane of the Vulnerability Manager .

User-Defined Checks

This section consists of the following topics:

- [What are User-Defined Checks?](#)
- [User-Defined Check Workflow](#)
- [Two Examples of User-Defined Checks](#)
- [Creating a User-Defined Check](#)
- [Adding a User-Defined Check to a Non-Built-In Policy](#)
- [Editing a User-Defined Check](#)
- [Deleting a User-Defined Check](#)

What are User-Defined Checks?

AppDetectivePro allows you to create user-defined checks, i.e., customized SQL code written to enhance your existing Policies. When your user-defined SQL statement returns a result set, AppDetectivePro applies the criteria specified in your user-defined check and identifies vulnerable values.

For example, if your user-defined SQL statement is `SELECT * FROM USERS`, and the criteria specified in your user-defined check is where `username in (bob, jim)`, AppDetectivePro identifies `jim` and `bob` as vulnerable values, not all values returned.

AppDetectivePro only supports user-defined checks for Oracle 8.1.7.4 and greater.

User-Defined Check Workflow

The user-defined checks wizard allows you to create user-defined checks. The user-defined workflow checklist follows:

User-defined checks wizard page

Allows you to:

Example:

1

Enter the SQL statement that comprises your user-defined check.

Do not include a semicolon (;) at the end of a `SELECT` statement (for example, `SELECT * FROM DBA_USERS;`). The semicolon causes the user-defined check to fail.

AppDetectivePro audits your database for vulnerable values according to the criteria that you specify. If you don't specify **any** criteria, then **all** matching values are vulnerable (i.e., instances where all passwords are the same as the user name).

```
SELECT NAME, PASSWORD FROM
MASTER.DBO.SYSLOGINS WHERE
NAME = PASSWORD
```

User-defined checks wizard page

2

Allows you to:

Click the **Add** button to display the **Check Criteria** dialog box, and specify the following criteria for your user-defined check:

- **Column.** This drop-down allows you to choose the column 's index within the result set obtained from the SQL statement provided. The index starts at 1.
- **Operator.** This drop-down allows you to choose one of the following operators for your criteria:
`=, <, >, <>, IN, NOT IN`
- **Value.** This field allows you to enter the specific criteria for your user-defined check.

Alternately, you can click the:

- **Edit** button to edit an existing set of criteria
- **Delete** button to delete an existing set of criteria.

Example:

Assume for the SQL statement (`SELECT NAME, PASSWORD FROM MASTER.DBO. SYSLOGINS WHERE NAME = PASSWORD`) you want to specify a check criteria "password **not** equal to JOE". In this case, specify the following check criteria:

- **Column** = 2
- **Operator** = <>
- **Value** = joe

When you run the user-defined check with this criteria, AppDetectivePro flags all passwords that are the same as the user name (with the **exception** of the user name and password `joe`) as vulnerabilities.

User-defined checks wizard page

Allows you to:

Example:

- 3 Enter a check name and a check summary in the **Check Name** and a **Check Summary** fields, respectively (both required).
- 4 Enter overview and fix information for the check in the **Overview** and **Fix Information** fields, respectively (optional). **Fix Information** typically details what patches, fix packs, patch sets, etc., should be applied. You can also specify any workarounds available if AppDetectivePro detects vulnerabilities.
- **Check Name:** User Name is Password Check (exception “Joe”).
 - **Check Summary:** This check flags all passwords that are the same as the user name (with the exception of the user name and password JOE) as vulnerabilities.
 - **Overview:** Strong passwords should be used for all Oracle users. If you allow accounts to have passwords that are the same as the username, an attacker can easily guess the password and break into a database.
 - **Fix Information:** Change the passwords for the users in questions and enable strong password validation.

User-defined checks wizard page

Allows you to:

Example:

- | | | |
|---|--|---|
| 5 | <p>Enter versions affected and reference information in the Version(s) affected and Reference(s) fields, respectively (optional).</p> <p>Version(s) affected typically specifies the vulnerable version(s) of a particular database, for example, "All versions of Oracle", "Oracle8 and later", etc.</p> <p>Reference(s) typically lists links that contain information about the vulnerability, for example, <i>For more information, see http://www.oracle.com/bad-vulnerability</i></p> | <ul style="list-style-type: none"> • Version(s) affected: All versions of Oracle. • Reference(s): For more information, see http://www.oracle.com/bad-vulnerability |
| 6 | <p>Specify the following for your user-defined check:</p> <ul style="list-style-type: none"> • Corresponding Application (i.e., Microsoft SQL Server, Oracle, Sybase, IBM DB2, or IBM DB2 z/OS) • Risk Level, i.e., 1 = High, 2 = Medium, 3 = Low, or 4 = Informational. | <ul style="list-style-type: none"> • Corresponding Application: Oracle • Risk Level: High. |
| 7 | <p>Review the summary of your user-defined check.</p> | <p>N/A</p> |
| 8 | <p>Finish creating your user-defined check</p> | |

Two Examples of User-Defined Checks

This topic consists of two user-defined check examples.

SIMPLE USER-DEFINED CHECK EXAMPLE

This is a simple user-defined check for Oracle. It queries the list of tables and their owners from `dba_tables` that include the string `TEST` in the table name. It is not using any criteria beyond the ones in the `WHERE` clause of the PL/SQL statement.

Below is the PL/SQL statement for a simple user-defined check:

```
select owner, table_name, tablespace_name from dba_tables where
table_name like '%TEST%'
```

Below are the result details for this check:

```
(col1=ODM_MTR) (col2=MAGAZINE_2D_TEST_BINNED) (col3=ODM)
(col1=ODM_MTR) (col2=CENSUS_2D_TEST_BINNED) (col3=ODM)
(col1=ODM_MTR) (col2=CENSUS_2D_TEST_UNBINNED) (col3=ODM)
(col1=ODM) (col2=ODM_TEST_RESULT) (col3=ODM)
(col1=ODM) (col2=ODM_CLASSIFICATION_TEST_RESULT) (col3=ODM)
```

The table below contains additional information about the check.

Criteria	None
Check Name	Find <code>TEST</code> tables
Summary	Find tables with <code>TEST</code> in the table name.
Overview	Database developers and DBAs sometimes create temporary tables for testing purposes. Often these tables include the string <code>TEST</code> in the name. This user-defined check flags all tables that match this criteria.
Fix Information	Remove the found tables by calling <code>DELETE TABLE TableName</code> .
Version(s) Affected	All versions of Oracle.
Reference(s)	None

Criteria	None
Application	Oracle
Risk Level	Low

ADVANCED USER-DEFINED CHECK EXAMPLE

This is an advanced user-defined check. Its purpose is to find all databases that have not been backed-up for more than 48 hours. Such checks demonstrate the full power of advanced query support inherent to AppDetectivePro user-defined checks.

Below is the T-SQL statement for an advanced user-defined check:

```
set noCount on
-- Creating a temporary table for
-- the list of all last backed up databases names and
-- backup dates
Create Table #Last_Databases_backup
    (Database_name sysname,
     Last_Backup_date datetime)
-- populate table by querying the msdb.dbo.backupset
-- system table
Insert #Last_Databases_backup
    (Database_name , Last_Backup_date)
select database_name, max(backup_finish_date)
    from msdb.dbo.backupset
    group by database_name
-- report the last backup date and the hours since then
-- or NULL if the database has never been backed up
-- The left outer join will list also databases that
-- have never been backed up
-- datediff will take care of the hours range condition
Select x.database_name , x.BackupDate, Hours
from
    (Select a.name as database_name ,
```

```
datediff (Hour,b.Last_Backup_date ,getDate()) as Hours ,
        b.Last_Backup_date as BackupDate
        from master.dbo.sysdatabases a
                Left Outer Join #Last_Databases_backup b
                on a.name = b.Database_name) x
WHERE x.BackupDate is NULL
OR Hours > 48
    Drop table #Last_Databases_backup
set noCount off
```

Below are the result details of this advanced user-defined check:

```
(coll=tempdb) (col2=) (col3=)
(coll=model) (col2=) (col3=)
(coll=msdb) (col2=) (col3=)
(coll=ReportServer) (col2=) (col3=)
(coll=ReportServerTempDB) (col2=) (col3=)
(coll=StoreFront) (col2=2007-03-19 11:44:23.000) (col3=1729)
(coll=master) (col2=) (col3=)
(coll=Northwind) (col2=) (col3=)
```

The table below contains additional information about the advanced user-defined check.

Criteria	None
Check Name	Databases not backed up in the last 48 hours.
Summary	Databases should be backed up in regular intervals in order to minimize data loss.
Overview	This check finds all databases that have not been backed-up for more then 48 hours.
Fix Information	Set an automatic backup schedule for the reported databases.
Version(s) Affected	All versions of Microsoft SQL Server.
Reference(s)	None

Criteria	None
Application	Microsoft SQL Server
Risk Level	Low

Creating a User-Defined Check

The **user-defined checks wizard** allows you to create a user-defined check in AppDetectivePro for Microsoft SQL Server, Oracle, Sybase, IBM DB2, or IBM DB2 z/OS, then add the check to a non-built-in Policy.

To create a user-defined check:

Step	Action
1	<p>Do one of the following:</p> <ul style="list-style-type: none"> Choose Edit > User-Defined Checks from the menu bar. Click the User-Defined button from the Policy Editor. <p>The user-defined checks wizard appears.</p>
2	Select Create a New Check .
3	Click the Next button.
4	<p>Enter the SQL statement that comprises your user-defined check. For example, enter the following SQL statement:</p> <pre>SELECT NAME, PASSWORD FROM MASTER.DBO.SYSLOGINS WHERE NAME = PASSWORD</pre> <p>Do not include a semicolon (;) at the end of a <code>SELECT</code> statement, for example, <code>SELECT * FROM DBA_USERS;</code>. The semicolon causes the user-defined check to fail.</p> <p>AppDetectivePro audits your database for vulnerable values according to the criteria that you specify. If you don't specify any criteria, then all matching values are vulnerable (i.e., instances where all passwords are the same as the user name).</p>
5	Click Next .

Step	Action
6	<p>Click the Add button to display the Check Criteria dialog box, and specify the following criteria for your user-defined check:</p> <ul style="list-style-type: none"> • Column. This drop-down allows you to choose the column 's index within the result set obtained from the SQL statement provided. The index starts at 1. • Operator. This drop-down allows you to choose one of the following operators for your criteria: =,<,>,<>,IN, NOT IN • Value. This field allows you to enter the specific criteria for your user-defined check. <p>For example, assume for the SQL statement (<code>SELECT NAME, PASSWORD FROM MASTER.DBO.SYSLOGINS WHERE NAME = PASSWORD</code>) you want to specify a check criteria "password not equal to JOE". In this case, specify the following check criteria:</p> <ul style="list-style-type: none"> • Column = 2 • Operator = <> • Value = joe <p>When you run the user-defined check with this criteria, AppDetectivePro flags all passwords that are the same as the user name (with the exception of the user name and password JOE) as vulnerabilities.</p> <p>Alternately, click:</p> <ul style="list-style-type: none"> • Edit to edit an existing set of criteria • Delete to delete an existing set of criteria.
7	<p>Click Next and enter a check name and a check summary in the Check Name and a Check Summary fields, respectively (both required).</p>
8	<p>Click Next and enter overview and fix information in the Overview and Fix Information fields, respectively (optional).</p> <p>Fix Information typically details what patches, fix packs, patch sets, etc., should be applied. You can also specify any workarounds available if AppDetectivePro detects vulnerabilities.</p>

Step	Action
9	<p>Click the Next button and enter versions affected and reference information in the Version(s) affected and Reference(s) fields, respectively (optional).</p> <p>Version(s) affected typically specifies the vulnerable version(s) of a particular database, for example, "All versions of Oracle", "Oracle8 and later", etc.</p> <p>Reference(s) typically lists links that contain information about the vulnerability, for example, For more information, see http://www.oracle.com/bad-vulnerability.</p>
10	<p>Click Next and use the drop-downs to specify the:</p> <ul style="list-style-type: none"> • Corresponding Application (i.e., Microsoft SQL Server, Oracle, Sybase, IBM DB2, or IBM DB2 z/OS) • Risk Level for the check, i.e., 1 = High, 2 = Medium, 3 = Low, or 4 = Informational. <p>You can use the Policy Editor to modify the risk level of user-defined check (as well as built-in checks) in association with a custom Policy. For more information, see Modifying the Risk Level of Checks Associated With Custom Policies.</p>
11	Click Next and review the summary of your user-defined check.
12	Click Next to finish creating your user-defined check.
13	Add the user-defined check to an existing non-built-in Audit Policy or Pen Test Policy; for more information, see Adding a User-Defined Check to a Non-Built-In Policy .

Adding a User-Defined Check to a Non-Built-In Policy

To add a user-defined check to an existing non-built-in Audit Policy:

Step	Action
1	<p>Do one of the following:</p> <ul style="list-style-type: none"> • Choose Edit > Policies from the menu bar. • Click the Policy button on the toolbar. • Press <CTRL>+L. <p>The Policies dialog box appears.</p>
2	Select a Policy.
3	<p>Click the View Selected button.</p> <p>The Policy Editor appears.</p>
4	<p>Add your user-defined check to an existing non-built-in Audit Policy.</p> <p>If you export your Policy, AppDetectivePro also exports any user-defined checks that are part of the Policy. For more information, see Exporting/Purging Data.</p>
5	Click Save As to save the Policy.
6	<p>Re-open the Policy to confirm the addition of your user-defined check. (Alternately, click the Continue Editing Rules button to create a new user-defined check; for more information, see Creating a User-Defined Check).</p>

Editing a User-Defined Check

The **user-defined checks wizard** allows you to edit a user-defined check in AppDetectivePro.

Important!

If you export your Policy, AppDetectivePro also exports any user-defined checks that are part of the Policy. For more information, see Exporting/Purging Data.

To edit a user-defined check:

Step	Action
1	Choose Edit > User-Defined Checks from the menu bar. The user-defined checks wizard appears.
2	Select Edit an Existing Check .
3	Click the Next button.
4	Edit the SQL statement that comprises your user-defined check; for more information, Creating a User-Defined Check .
5	Click the Next button.
6	Click the Add button to display the Check Criteria dialog box, and edit the criteria for your user-defined check; for more information, Creating a User-Defined Check . Alternately, click the: <ul style="list-style-type: none"> • Edit button to edit an existing set of criteria • Delete button to delete an existing set of criteria.
7	Click the Next button and edit the check name and check summary in the Check Name and Check Summary fields, (both required).
8	Click the Next button and edit the overview and fix information in the Overview and Fix Information fields (optional).
9	Click the Next button and edit the versions affected and reference information in the Version(s) Affected and Reference information field.
10	Click the Next button and use the drop-downs to edit the: <ul style="list-style-type: none"> • Corresponding Application (MS-SQL or Oracle) • Risk Level for the check (High, Medium, Low, or Informational). You can use the Policy Editor to modify the risk level of user-defined check (as well as built-in checks) in association with a custom Policy. For more information, see Modifying the Risk Level of Checks Associated With Custom Policies.

Step	Action
11	Click the Next button and review the summary of your edited user-defined check.
12	Click the Next button to finish editing your user-defined check.
13	Add the edited user-defined check to an existing non-built-in Audit Policy or Pen Test Policy; for more information, see Adding a User-Defined Check to a Non-Built-In Policy.

Deleting a User-Defined Check

The **user-defined checks wizard** allows you to delete a user-defined check in AppDetectivePro.

To delete a user-defined check:

Step	Action
1	Do one of the following: <ul style="list-style-type: none"> Choose Edit > User-Defined Checks from the menu bar. Click the User-Defined button from the Policy Editor. The user-defined checks wizard appears.
2	Select Delete a Check .
3	Click the Next button.
4	Choose a user-defined check to delete. You can select multiple, consecutive checks by highlighting the check names and pressing <SHIFT>. You can select multiple, non-consecutive checks by highlighting the check names and pressing <CTRL>.
5	Click the Next button.
6	AppDetectivePro prompts you to confirm the delete. Click the Yes button to confirm.

Fix Scripts

This section consists of the following topics:

- [What are Fix Scripts?](#)
- [Generating a Fix Script](#)

What are Fix Scripts?

The Fix Scripts utility generates SQL scripts designed to correct mis-configurations and address vulnerabilities identified by AppDetectivePro during an Audit. The Fix Scripts utility allows you to:

- review a Fix Script
- customize the Fix Script
- voluntarily (not automatically) deploy the Fix Script on to your database.

For more information on:

- generating a Fix Script, see [Generating a Fix Script](#)
- the details of the AppDetectivePro Fix Scripts for all supported operating applications, see [Appendix K: Fix Scripts \(Detail\)](#).

Generating a Fix Script

To generate a Fix Script:

Step	Action
1	Audit your applications; for more information, see Running an Audit .
2	Select a vulnerability in the vulnerability view, or an Audit in the network tree view; for more information, see Navigating Page Views .

Step	Action
3	<p>Click Fix on the toolbar. If you chose:</p> <ul style="list-style-type: none">• both a vulnerability and an Audit in Step 2, then AppDetectivePro prompts you to choose whether you want to choose a specific vulnerability, or the entire Audit selected• an Audit in Step 2, AppDetectivePro prompts you to choose which vulnerabilities to include in the Fix Script. AppDetectivePro generates and displays the Fix Script SQL to execute.
4	<p>You can edit the Fix Script. (If AppDetectivePro creates parameters in the SQL, you are prompted for corresponding values.)</p>
5	<p>Optionally, you can:</p> <ul style="list-style-type: none">• click the Copy to Clipboard button to copy the Fix Script SQL code into your clipboard• paste the Fix Script SQL into your SQL editor• deploy the Fix Script to your database.

Viewing SCAP Information

AppDetectivePro implements the Security Content Automation Protocol (SCAP) standard in several ways. Specifically, for:

- **Common Platform Enumeration (CPE)**, AppDetectivePro imports the CPE Dictionary provided by NIST. CPE tags are available in all XML reports. For more information, see [Understanding CPE](#).
- **Common Configuration Enumeration (CCE)**, AppDetectivePro contains a mapping of all configuration checks to CCE references. If no CCE reference is available, AppDetectivePro maps the check to a **CCE-NO-MATCH** reference. For more information, see [Understanding CCE](#).
- **Common Vulnerabilities and Exposure (CVE)**, AppDetectivePro contains a mapping of all vulnerability checks to CVE references. If no CVE reference is available, AppDetectivePro maps the check to a **CVE-NO-MATCH** reference. CVE references are available in all product output, including the AppDetectivePro UI, reporting, and within the vulnerability knowledgebase. For more information, see [Understanding CVE](#).

This section consists of the following topics:

- [Viewing SCAP Information in AppDetectivePro](#)
- [Understanding CPE, CCE, and CVE](#)

Viewing SCAP Information in AppDetectivePro

To view SCAP information in AppDetectivePro:

Step	Action
1	Choose View > SCAP Info in the menu. A dialog box displays the most current information about CPE, CCE, and CVE, including when each component was updated in the product and when last updated by the National Institute of Standards and Technology (NIST). AppDetectivePro updates this information with each release.

Understanding CPE, CCE, and CVE

This section consists of the following topics:

- [Understanding CPE](#)
- [Understanding CCE](#)
- [Understanding CVE](#)

UNDERSTANDING CPE

AppDetectivePro imports the CPE Dictionary from the NIST feed. AppDetectivePro stores the CPE Dictionary in its backend repository. The use of the CPE standard is tied to applications Discovered by AppDetectivePro. CPE tags are included in all XML reports.

UNDERSTANDING CCE

AppDetectivePro contains a mapping of all configuration checks to CCE references. When available, AppDetectivePro uses the CCE vulnerability feed provided from NIST.

Note:	All configuration checks currently are mapped to a CCE-NO-MATCH reference.
--------------	---

UNDERSTANDING CVE

AppDetectivePro is a declared CVE-compatible product. All vulnerability checks, when available, contain CVE identifiers. For all vulnerability checks that do not have a CVE identifier, AppDetectivePro maps the check to a CVE-NO-MATCH identifier. CVE identifiers are searchable in the product using the Policy Editor.

This section consists of the following appendices:

- [Appendix A: Command Line Reference](#)
 - [Appendix B: Viewing Check Descriptions](#)
 - [Appendix C: Troubleshooting](#)
 - [Appendix D: Using Default and Custom Dictionaries](#)
 - [Appendix E: Using NMAP](#)
 - [Appendix F: Clearing Sybase Application Logs](#)
 - [Appendix G: Audit and User Rights Review Privileges](#)
 - [Appendix H: Using Microsoft SQL Server with AppDetectivePro](#)
 - [Appendix I: Enabling SSL Encryption on AppDetectivePro](#)
 - [Appendix J: Default Ports](#)
 - [Appendix K: Fix Scripts \(Detail\)](#)
 - [Appendix L: Check Point Logging Properties Installation](#)
 - [Appendix M: Customizing Reports with Your Company Logo](#)
 - [Appendix N: Integrating a Custom Dictionary to Uncover Easily-Guessed Passwords](#)
 - [Appendix O: Oracle Critical Patch Update Detection](#)
 - [Appendix P: Migrating Your Back-End Database](#)
 - [Appendix Q: Understanding System Auditing](#)
 - [Appendix R: Updating Your Back-End Database from Microsoft SQL Server 2000 to Microsoft SQL Server 2005 or Microsoft SQL Server 2008](#)
 - [Appendix S: Dynamic Shell Prompt Handling](#)
 - [Appendix T: AppDetectivePro Application Log Files and Installation/Upgrade Log Files](#)
 - [Appendix U: Open Ports \(on Computers Running Microsoft SQL Server\) Required to Run Discoveries, Pen Tests, and Audits](#)
 - [Appendix V: Uploading Comma-Delimited Text Files, CSV Files, or NMAP Files Containing IP Addresses \(or IP Addresses and Ports\) to Discover](#)
-

Appendix A: Command Line Reference

Command line reference functionality allows you to run a Discovery, Pen Test, Audit, or a Report using the command line. You can also use the command line to purge tests and Sessions. Command line functionality is not currently supported for User Rights Reviews.

This appendix consists of the following topics:

- Command Line Overview
- Command Line Usage
- Scheduling AppDetectivePro Tasks
- Command Line Test Configuration.

Command Line Overview

You can use AppDetectivePro in conjunction with scheduler programs that run applications at specific times during the day.

In order to run AppDetectivePro with a scheduler, AppDetectivePro is packaged with the file `asiengine.exe` which you can run at the command line.

This program is available at the following location, by default: `<installation directory>\Program Files\AppSecInc\AppDetective\asiengine.exe`. For more information, see Command Line Usage.

Command Line Usage

This topic explains how to perform AppDetectivePro tasks from the command line. This is useful for performing AppDetectivePro tasks within scripts or from a task scheduler.

Caution! Command line functionality is **not** currently supported for User Rights Reviews.

This topic consists of the following sub-topics:

- .The ASIEngine.exe Executable File
- Command Line Hints
- Key to Symbols Used
- General Parameters
- Running a Discovery from the Command Line

- Running a Pen Test from the Command Line
- Running an Audit from the Command Line
- Creating Reports from the Command Line
- Purging Tests and Sessions from the Command Line.

THE ASIENGINE.EXE EXECUTABLE FILE

The `ASIEngine.exe` executable file is located, by default, in the following location:

```
"<installation directory>\Program Files\AppSecInc\AppDetective\ASIEngine.exe"
```

In order to use `AppDetectivePro` at the command line, enter the `ASIEngine.exe` command followed by the appropriate options. You should change directories to the installation directory before doing so, for example, `cd C:\Program Files\AppSecInc\AppDetective\`. Otherwise, enclose the `ASIEngine.exe` path in double quotes if there is space in the path, for example, `"C:\Program Files\AppSecInc\AppDetective\ASIEngine.exe"`.

COMMAND LINE HINTS

- Enclose in double quotes `ASIEngine.exe` path if there is space in the path.
- Enclose in single quotes any parameters that contain more than one word.
- Parameters are required unless specified as optional.
- You must use the `^` and `&` with escape characters, or the Windows command line will misread them. The escape character is `^`. For example, to enter `^x&y` on the command line, enter the command: `^^x^&y`

KEY TO SYMBOLS USED

Symbol	Definition
()	Description of flag.
< >	Fill in the value for your purposes.
[]	Optional flags.
	"OR".

GENERAL PARAMETERS

The following table defines general parameters.

Option	Definition
-L -1	The latest Session ID.
-T	Test ID.
-F	File name to be used as input to <code>ASIShield.exe</code> . Contains parameters and arguments. Usage: <code>ASIShield.exe -F 'full path to file'</code>

RUNNING A DISCOVERY FROM THE COMMAND LINE**Syntax:**

```
ASIShield.exe -PS (-R <RANGE_TO_SCAN> | <SCAN_FILE_INFO>) [-B (for silent mode)] [<REPORTS_TO_CREATE>]
```

Where	=
-PS	Discovery.
-R	A range of ports to Discover.
-N	Indicates an NMAP file to use (only used for NMAP normal output files as input). Enter the full path information if the file is not in the current directory.
-B	Run in silent mode (optional).

Where	=
<pre>-SC <search criteria></pre>	<p>Used only with NMAP normal output files (optional):</p> <p>Single port: <port></p> <p>Range of ports: <starting port>-<ending port></p> <p>Default ports only: <default port list></p> <p>Default Port List</p> <p>A - All ports in the file (this is the default)</p> <p>B - Oracle Application Server</p> <p>C - Lotus Web Server</p> <p>D - IBM DB2</p> <p>H - HTTP Web Servers</p> <p>L - Lotus Domino Groupware Servers</p> <p>M - MSSQL Servers</p> <p>O - Oracle</p> <p>S - Sybase</p> <p>Y - MySQL server.</p>
<pre><RANGE_TO_SCAN></pre>	<pre><starting ip address>[-<ending ip address>] (<starting port>[-<ending port>]) {:<RANGE_TO_SCAN>}</pre>
<pre><SCAN_FILE_INFO></pre>	<pre>-N <NMAP File Name> -FFS <Default File Name> [-SC <SEARCH_CRITERIA>]</pre>
<pre><SEARCH_CRITERIA></pre>	<pre><port> <starting port>-<ending port> <DEFAULT_PORT_STRING></pre>
<pre><DEFAULT_PORT_STRING></pre>	<pre><DEFAULT_PORT_TYPE> [<DEFAULT_PORT_STRING>]</pre>
<pre><DEFAULT_PORT_TYPE></pre>	<pre>A (All Applications) B (Oracle Application Server) C (Lotus Web Server) D (IBM DB2) H (HTTP Web Server) L (Lotus Groupware Server) M (Microsoft SQL Server) O (Oracle) S (Sybase) Y (MySQL)</pre>

Example:

```
ASIEngine.exe -PS -R 172.16.32.1-172.16.32.254 (1510-1530)
```

This command is used to Discover the IP address range from [172.16.32.1](#) through [172.16.32.254](#), ports 1510 through 1530.

RUNNING A PEN TEST FROM THE COMMAND LINE

Syntax:

```
ASISEngine.exe -PT -I <ip address> -P <port> -Y <policy to use> -L<corresponding session id> [-S <application name>] [-LO (stop on a locked account)] [-B(for silent mode)] [<REPORTS_TO_CREATE>]
```

Where	=
-PT	Pen Test.
-I	IP address.
-P	A port number.
-Y	Policy to use (Policy name), which you can find by clicking the Policy button on the AppDetectivePro toolbar.
-L	Corresponding Session ID. Hint: To Find Session ID, click the Open button on the AppDetectivePro toolbar.
-S	Application name. For: <ul style="list-style-type: none"> • Oracle, specify the Oracle System ID (SID) • IBM DB2, specify the IBM DB2 instance. The <code>-s</code> command is not available for applications beside Oracle and IBM DB2.
-LO	Stop on locked account (optional).
-B	Silent mode (optional).

Example:

```
ASISEngine.exe -PT -I 192.168.1.11 -P 1521 -Y 'Brute Force (Built-In)' -S oracle -L 1
```

This command is used to Pen Test the IP address [192.168.1.11](#), port 1521, using the Brute Force (Built-In) Policy. The SID name = `Oracle`, and the Session ID = `1`.

Example 2

```
ASISEngine.exe -PT -I 192.168.1.143 -P 50000 -Y 'Brute Force (Built-In)' -S
DB2INST1:SAMPLE -L 1
```

This command is used to Pen Test the IP address 192.168.1.143, port 5000, using the Brute Force (Built-In) Policy. The DB2 instance name = DB2INST1, the DB2 database name = SAMPLE, and the Session ID = 1.

RUNNING AN AUDIT FROM THE COMMAND LINE

Syntax:

```
ASISEngine.exe -PA <audit> -I <ip address> -P <port> -Y <policy to use> -U
<Database Account> -W <Database Password> -L <corresponding session id> [-
OP<'TELNET' or 'SSH'>] [-OPORT<port to use>] [-OU <OS user name> -OW <OS
password>] [-S<application name>] [-B(for silent mode)] [-DBA (for SYSDBA
privileges) | -OPER(for SYSOPER privileges)] [<REPORTS_TO_CREATE>] | -PARAMS
```

Where

=

-PA	Audit.
-I	IP address.
-P	Port number.
-Y	Policy to use (Policy name) To find a Policy name, click the Policy button on the AppDetectivePro toolbar.
-U	Database account.
-W	Database password.
-L	Corresponding Session ID. To find the Session ID, click the Open button on the AppDetectivePro toolbar.
-OU	OS user name (optional).
-OW	OS password (optional).
-S	Application name. For: <ul style="list-style-type: none"> • Oracle, specify the Oracle System ID (SID) • IBM DB2, specify the IBM DB2 instance. The -s command is not available for applications beside Oracle and IBM DB2.
-B	Silent mode (optional).

Where

=

- DBA Use SYSDBA privileges (optional). Oracle only.
You can also use -PARAMS to specify the privilege (see -PARAMS section below for details).
- OPER Use SYSOPER privileges (optional). Oracle only.
You can also use -PARAMS to specify the privilege (see -PARAMS section below for details).
- OP Protocol to use, for example, TELNET or SSH. Used for connecting to Unix machines (optional).

Where

=

- `-OPORT` Port to connect to when connecting to the operating system (optional).
- `-PARAMS` For directly passing the new parameters via the command line, the user has to pass the new parameters in a specific format as part of the `-PARAMS` flag. This is in addition to the existing flags necessary for an audit.

In addition to existing flags required to perform an audit, the `-PARAMS` flag allows you to pass the following parameters via the command line:

- `RemConnPvtKeyFilePath`. The path to the client private key file in Windows path format.
- `RemConnPvtKeyCipher`. The cipher used for the private key. Valid values are `0` (RSA) or `1` (DSA).
- `RemConnPvtKeyPassPhrase`. The pass phrase, if any, used when the client private key was created.
- `RemConnTimeout`. The connection time out value in seconds for the SSH connection. The default value is `30` seconds. This is different from the time out value specified from the AppDetective GUI property sheet. This parameter is optional.
- `RemSessionPrompt`. The Session prompt that will be used for the session. Example: `bash-2.05$`. This parameter is optional.
- `Privileges`. The account privileges to use for the Audit. Valid values are `SYSDBA` or `SYSOPER`. Oracle Only. You may alternatively use the `-DBA` or `-OPER` flags to specify the privilege (See `-DBA` or `-OPER` sections above).

See *Example 3*, below, for an example of a command that uses the `-PARAMS` flag.

Example 1:

```
ASISEngine.exe -PA -I 192.168.1.11 -P 1521 -Y 'Base Line (Built-in)' -U  
system -W manager -S oracle -L 1
```

This command is used to Audit the IP address `192.168.1.11`, port `1521`, using the Base Line (Built-In) Policy. The user name = `system`, the password = `manager`, the SID name = `oracle`, and the Session ID = `1`.

Example 2:

```
ASISEngine.exe -PA -I 192.168.1.10 -P 50000 -Y 'Base Line (Built-in)' -U  
db2admin -W db2admin -S DB2INST1:SAMPLE -L 1
```

This command is used to Audit the IP address `192.168.1.10`, port `50000`, using the Base Line (Built-In) Policy. The user name = `db2admin`, the password = `db2admin`, the DB2 instance name = `DB2INST1`, the DB2 database name = `SAMPLE`, and the Session ID = `1`.

Example 3:

All the parameters that follow `-PARAMS` must be on a single line without any spaces or line breaks. If the parameter has no value, the value should be empty. For example:

```
-PARAMS  
(RemConnPvtKeyFilePath=C:\\test.txt) (RemConnPvtKeyCipher=0)  
(RemConnPvtKeyPassPhrase=) (RemConnTimeout=30) (RemSessionPrompt  
=bash-2.05$)
```

Note the value of `RemConnPvtKeyPassPhrase` is empty.

CREATING REPORTS FROM THE COMMAND LINE

You can add reporting options to any of the commands discussed in this sub-topic.

Syntax:

```
<REPORTS_TO_CREATE>: <EMAIL_INFO> | <SAVE_DIRECTORY_INFO>
```

Specifying Where to Send Reports

Where (for email): =

-RE	Email address (enclose in single quotes).
-RSMTPIP	SMTP server.
-RSMTPPORT	SMTP server port.
-RSMTPUSE	User name.
-RSMTPPWD	Password.

Where (for a file): =

-RD	Path of file to use as output (enclose in single quotes).
-----	---

Report Output Types

Where	=
-RHTML	Create report as HTML (.mht format).
-RXML	Create report as XML.

If you do not specify an output type, AppDetectivePro generates your report as an Adobe PDF.

Discovery Reports

Where	=
-RGP - RY	Syntax: [(<policy id to print out> '<policy name to print out>') (Policy Report)]
-RGAI	Application Inventory Report. Use with -L option.

Discovery (and Associated Tests) Reports

Where	=
-RMCS	Prints a Check Status Report for all applications and latest test. Use with the <code>-L</code> option.
-RMVD	Prints a Vulnerability Details Report for all applications and latest tests. Use with the <code>-L</code> option.
-RMVS	Prints a Vulnerability Summary Report for all applications and latest tests. Use with the <code>-L</code> option.
-RMAB	Prints an Application Banner Report . Use with the <code>-L</code> option.

Reports on a Single Test

Where	=
-RSCS	Prints a Check Status Report for all applications and latest test. Use with the <code>-L</code> option.
-RSUI	Prints a User Information Report for a single test. Use with <code>-T testid -I ipaddress -P port -S appname</code> options. Use <code>-s</code> option only if available.
-RSVD	Prints a Vulnerability Details Report for a single test. Use with <code>-T testid -I ipaddress -P port -S appname</code> options. Use <code>-s</code> option only if available.
-RSVS	Prints a Vulnerability Summary Report for a single test. Use with <code>-T testid -I ipaddress -P port -S appname</code> options. Use <code>-s</code> option only if available.

Example 1:

```
ASISEngine.exe -PS -R (192.168.1.1-192.168.1.254) (1510-1530) " -RGAI -RXML -L 13 -RD 'c:\'
```

This command is used to Discover the range of IP addresses from 192.168.1.1 to 192.168.1.254, ports 1510 to 1530, placing the results into Session #13. It creates an Application Inventory Report in XML format, and saves it in the `c:\` directory.

Example 2:

```
ASIEngine.exe -PT -Y 'Demo (Built-in)' -I 192.168.1.52 -P 1433 -RMVD -RHTML
-L 42 -RE 'admin@staff.com' -RSMTPIP 'mail.staff.com' -RSMTTPORT 25 -
RSMTTPUSER 'user@staff.com' -RSMTTPWD 'blank'
```

This command is used to Pen Test the database on the IP address 192.168.1.52, port 1433, using the Demo Policy. It places the results into Session #42, and generates a Vulnerability Details Report in HTML single file format, including all the applications in Session #42. The report is emailed to the user admin@staff.com via the SMTP server listening on port 25 of mail.staff.com. AppDetectivePro authenticates to mail.staff.com as user@staff.com with the password blank.

PURGING TESTS AND SESSIONS FROM THE COMMAND LINE

Note: These command line options should be placed after the program AppDetective.exe. The AppDetective.exe executable file is located, by default, at the following location: <installation directory>\Program Files\AppSecInc\AppDetective\AppDetective.exe.

Where	=
-PUT -T <test id>	Purges a specified test.
-PUST -L <session id>	Purges all tests in a specified Session.
-PUS -L <session id>	Purges a specified Session.
-PUAT	Purge all tests in all Sessions.
-PUAS	Purges all Sessions.
-EAS -FILE <export file name>	Exports all Sessions.
-IAS -FILE <import file name>	Imports all Sessions.

Scheduling AppDetectivePro Tasks

You can use the `AT` command in conjunction with the Windows 2000 Task Scheduler service in order to perform AppDetectivePro tasks at any given time or interval. In order to schedule an AppDetectivePro task, you must configure the Task Scheduler, and establish a command with parameters.

This topic consists of the following sub-topics:

- Configuring the Task Scheduler
- Establishing Command Parameters.

CONFIGURING THE TASK SCHEDULER

Note:	If the Task Scheduler service is already started, you do not need to complete this step.
--------------	---

To configure the Task Scheduler:

Step	Action
1	From your desktop, choose Start > Settings > Control Panel > Administrative Tools .
2	Double click the Services icon.
3	Select Task Scheduler from the Services list.
4	Click Startup . The service window appears.
5	Select Automatic in the Startup Type portion of the window.
6	Select System Account in the Log on as portion of the window.
7	Click the OK button.

ESTABLISHING COMMAND PARAMETERS

Open a command line and enter `help at` to display Windows help on the `AT` command.

Step	Action
1	Open a command prompt window.
2	Change directories to the AppDetectivePro installation folder. For example: <code>cd C:\Program Files\AppSecInc\AppDetective</code>
3	At the command prompt, enter <code>AT</code> and enter the necessary command line parameters to perform the AppDetectivePro task. For more information on specifying the proper parameters, see Command Line Usage.

Command Line Test Configuration

This topic consists of the following sub-topics:

- Understanding the Command Line Flags
- Test Configuration File
- Test Log File
- Application Information File.

UNDERSTANDING THE COMMAND LINE FLAGS

The first two command line flags (i.e., test configuration file and test log file) allow you to specify:

- the applications on which you want to perform tests (using a configuration file)
- a text file in which results of your tests are written.

The third command line flag (i.e., application information file) allows you to input specific application information via a text file.

Note:	Currently, this command line flag only allows you to input DB2 database patch-level information required for DB2 audits.
--------------	--

Specifically, the command line flags adhere to the following formats:

- `test_cfg_file <TEST CONFIG FILE>`. The specific format for the test configuration file; for more information, see Test Configuration File.
- `test_log <OUTPUT FILE>`. You can only use this command line flag in conjunction with the `-test_cfg_file` command line flag.
- `db_info_file <FILE>`. Provides the ability to input application information via a text file.

Currently, the only feature will be to input DB2 patch level information that is needed for DB2 database audits.

TEST CONFIGURATION FILE

Overview

Command line flag name: `-test_cfg_file <TEST CONFIG FILE>`

The first option allows you to test multiple applications by specifying test information in a single configuration file. Performing a Discovery prior to test execution is not necessary. AppDetectivePro automatically verifies application information specified. The configuration file must include the following parameters:

- **Policy to use.** Only one Policy allowed per configuration file.
- **Optional session ID to use.** If the session ID is not specified or invalid, AppDetectivePro will use the latest session.
- **Application information.** Contains necessary information AppDetectivePro uses to perform the test:
 - IP address, port
 - Application type
 - Application name
 - Operating system (for example, **SOLARIS** or **WINDOWS**)
 - If executing an Audit Policy:
 - *Application authentication information (username/pwd)
 - *If the Policy contains operating systems checks, OS username/ password.

The format of the test configuration file is similar to an `.INI` file format. It contains two sections:

- `TEST_PARAMETERS`

- APPLICATION

Sections are delimited in square brackets, i.e., []. There can only be one [TEST_PARAMETERS] section per configuration file, and there must be at least one [APPLICATION] section. Also, each section must contain at least one key/value (KEY=VALUE) pair.

[TEST_PARAMETERS] Section

The following table explains the required and optional [TEST_PARAMETERS] keys.

Required Keys	<ul style="list-style-type: none"> • POLICY. Valid values for the POLICY key are either the Policy name or the Policy ID number.
Optional Keys	<ul style="list-style-type: none"> • SESSION_ID. If SESSION_ID is not specified, or if it is invalid (i.e., it doesn't exist), AppDetectivePro uses the latest Session ID. If Sessions do not exist, AppDetectivePro creates a Session.

[APPLICATION] Section

The following table explains the required and optional [APPLICATION] keys.

Required Keys	<ul style="list-style-type: none"> • IP. Can either be a hostname or a numeric IP address. • PORT. Must be a single number between 1 and 65536. • APP_TYPE. Application type, for example, ORACLE. For more information, see Possible Values for the APP_TYPE and APP_NAME Keys. • APP_NAME. Valid values depend on the APP_TYPE. For example, if testing against an Oracle database, the APP_NAME is be the SID of the Oracle database. For more information, see Possible Values for the APP_TYPE and APP_NAME Keys.
Optional Keys (General)	<ul style="list-style-type: none"> • PLATFORM. For more information, see Possible Values for the PLATFORM Key.

Optional Keys: Pen Test- Specific

- `STOP_ON_LOCKED_ACCT`. Value can be `TRUE` or `FALSE`. This flag controls whether AppDetectivePro stops testing if an account becomes "locked" because of AppDetectivePro.

The Audit-specific optional keys, in addition to `PLATFORM`, are required if the Audit policy contains operating system checks; for more information, see Possible Values for the `PLATFORM` Key.

- `APP_LOGIN`. The username used to authenticate to the application being tested. Required if the Policy used is an Audit Policy.
- `APP_PASSWD`. The cleartext password used to authenticate to the application being tested. Required if the Policy used is an Audit Policy.
- `OS_LOGIN`. The username used to authenticate to the operating system the application resides on.
- `OS_PASSWD`. The cleartext password used to authenticate to the operating system the application resides on.
- `OS_PROTOCOL`. Valid values are `Telnet` and `SSH` (case-sensitive).
- `OS_PORT`. Specifies which port to connect to on the remote host when attempting to log in to the operating system.
- `PRIVILEGES`. Used only in conjunction with Oracle Audits, this key designates whether to connect to an application using `Normal`, `SYSDBA`, or `SYSOPER` privileges. These values are case-sensitive.
- `SSH_KEY_FILE`. The path to the client private key file in Windows path format.
- `SSH_KEY_PASSPHRASE`. The pass phrase, if any, used when the client private key was created.
- `SSH_KEY_CIPHER`. The cipher used for the private key. Valid values are `0` (RSA) or `1` (DSA).
- `REM_CONN_TIMEOUT`. The connection time out value in seconds for the SSH connection. The default value is 30 seconds. This is different from the time out value specified from the AppDetective GUI property sheet. This parameter is optional.
- `SESSION_PROMPT`. The session prompt that will be used for the session. Example: `bash-2.05$`. This parameter is optional.

Example 2, below, is an example of a configuration file used to Audit an Oracle application, employing a custom Policy called `SSH_Test` that uses public key authentication.

Optional Keys: Audit-Specific

Example 1:

A sample Audit configuration file follows:

```
[TEST_PARAMETERS]
POLICY=Base Line (Built-In)
[APPLICATION]
IP=172.16.0.45
PORT=50000
PLATFORM=Solaris
APP_TYPE=IBM DB2
APP_NAME=db2inst1:SAMPLE
APP_LOGIN=db2auditacct
APP_PASSWD=db2auditacct_pwd
OS_LOGIN=db2instowner
OS_PASSWD=db2instowner_pwd
```

Example 2:

Below is an example of a configuration file used to Audit an Oracle application, employing a custom Policy called `SSH_Test` that uses public key authentication:

```
[TEST_PARAMETERS]
POLICY=SSH_TEST
[APPLICATION]
IP=sunny10
PORT=1521
PLATFORM=Solaris
APP_TYPE=ORACLE
APP_NAME=dev901
APP_LOGIN=sys
APP_PASSWD=admin123
OS_LOGIN=oracle
OS_PASSWD=
OS_PROTOCOL=SSH
OS_PORT=22
PRIVILEGES=sysdba
SSH_KEY_FILE=C:\testkeys\testkey1.ppk
SSH_KEY_PASSPHRASE=
SSH_KEY_CIPHER=0
REM_CONN_TIMEOUT=30
SESSION_PROMPT=bash-2.05$
```


Possible Values for the APP_TYPE and APP_NAME Keys

The following table explains possible values for the APP_TYPE and APP_NAME keys.

APP_TYPE	APP_NAME
IBM DB2	<instance>:<database>
IBM DB2 z/OS	<subsystem name>:<location name>
Oracle	<SID>
Microsoft SQL Server	Not used
MySQL	<db name>
Sybase	Not used

Possible Values for the PLATFORM Key

Possible values for the PLATFORM key follow.

- Alpha OpenVMS
- Data General
- DEC Alpha
- Fujitsu
- Hitachi
- HP Unix
- IBM AIX
- IBM NUMA
- IBM OS/390
- Intel Solaris
- Linux
- Microsoft Windows
- NCR
- Novell Netware
- SCO Unix
- Seimens
- Sequent Dynix
- SGI IRIX
- Solaris
- TRU-64

- UnixWare.

TEST LOG FILE

Optional command line flag: `-test_log <OUTPUT FILE>`

In addition to passing the configuration file to the AppDetectivePro engine, an optional flag of specifying a file that will contain session and application test result information will be added. The log file is a simple text file that contain messages regarding the tests being run. Information that will be written to the log file will contain:

- Date/time stamp of message
- PID of the process that is writing the message
- Message string.

The following message types can be written:

- Session start time
- Session completion time
- Start time of application test along with IP, port, application type, application name, and policy ID being used
- Completion time of application test as well as the detailed status of the test (for example, "SUCCESS" or "FAILURE: Invalid login information").

Sample Test Log File

```
[ 03:48:47.564 4/20/2005 ][ 1336 ] Test started
[ 03:48:48.003 4/20/2005 ][ 1336 ] Audit started on 172.16.0.45:50000 on DB2
Database:
db2inst1:SAMPLE using policy ID 19
[ 03:48:49.313 4/20/2005 ][ 1336 ] Audit started on 192.168.1.40:1433 on
Microsoft SQL
Server 2000: DEFAULTINSTANCE using policy ID 19
[ 03:49:00.033 4/20/2005 ][ 1336 ] Audit completed on 192.168.1.40:1433 on
Microsoft SQL
Server 2000: DEFAULTINSTANCE status: FAILURE - Invalid login information
[ 03:50:18.000 4/20/2005 ][ 1336 ] Audit completed on 172.16.0.45:50000 on
DB2 Database:
db2inst1:SAMPLE status: SUCCESSFUL
[ 04:01:15.298 4/20/2005 ][ 1336 ] Test completed
```

APPLICATION INFORMATION FILE

Command line flag: `-db_info_file <FILE>`

This file provides database information (that otherwise must be supplied to the OS login) in order for AppDetectivePro to perform certain tests. Currently, only DB2 Audit requires providing this information that will be used in FixPak check. The file should contain the following information.

- IP address
- Port
- DB2 instance name
- DB2 database name
- Service Level (for Windows platform), or Build Level (for UNIX platform).

Detailed File Format

The format of the test configuration file is similar to an `.INI` file format. It contains one section:

- `DB2_FIXPAK_DATA`.

Sections are delimited in square brackets, i.e., `[]`. There can only be one `[DB2_FIXPAK_DATA]` section per configuration file, and there must be at least one `[APPLICATION]` section. The section must contain at least one key/value (`KEY=VALUE`) pair.

[DB2_FIXPAK_DATA] Section

The following table explains possible values for the `DB2_FIXPACK_DATA` key.

Required Keys	<ul style="list-style-type: none"> • <code>IP</code>. Can either be a hostname or a numeric IP address. • <code>PORT</code>. Must be a single number that is between 1 and 65536. • <code>INSTANCE_NAME</code>. The DB2 instance name. • <code>DATABASE_NAME</code>. The DB2 database name. • <code>SERVICE_LEVEL</code> or <code>BUILD_LEVEL</code>. On Windows, <code>SERVICE_LEVEL</code> is required. The value is the registry value of Service Level on the DB2 database machine. The registry paths follow:
---------------	---

For DB2 v7.x

```
$HKEY_LOCAL_MACHINE\SOFTWARE\IBM\DB2\DB2 Universal
Database Enterprise Edition\CurrentVersion\Service Level
```

For Other DB2 Versions

```
$HKEY_LOCAL_MACHINE\SOFTWARE\IBM\DB2\CurrentVersion\Service Level
```

On UNIX, `BUILD_LEVEL` is required. This value comprises the contents of the `bllevel` file on the DB2 database machine. The file path is: `$HOME/sql1lib/cfg/bllevel`, where `$HOME` is home directory of the DB2 instance owner.

Sample Database Information File

For Windows:

```
[DB2_FIXPAK_DATA]
IP_ADDRESS=152.12.0.100
PORT=50000
INSTANCE_NAME=db2inst1
DATABASE_NAME=WINDOWS_SAMPLE
SERVICE_LEVEL=WR2133
```

For Unix:

```
[DB2_FIXPAK_DATA]
IP_ADDRESS=152.12.0.200
PORT=50002
INSTANCE_NAME=db2inst2
DATABASE_NAME=UNIX_SAMPLE
BUILD_LEVEL=s031208
```

Appendix B: Viewing Check Descriptions

This appendix consists of the following topics:

- How to View Check Descriptions
- How to View Checks Contained Within Policies.

How to View Check Descriptions

To view and print Pen Test and Audit check descriptions:

Step	Action
1	Click the Policy button on the toolbar.
2	If you want to view: <ul style="list-style-type: none"> • Pen Test checks, click the Pen Test tab • Audit checks, click the Audit Policies tab.
3	Click the New Policy button. The Policy Editor appears.
4	Click the + signs next to the descriptions to view the respective check descriptions.
5	Click the checks to view their details. Hint: To print a check description, right click the description, and choose Print .

How to View Checks Contained Within Policies

To view and print Pen Test and Audit check details within AppDetectivePro Policies:

Step	Action
1	Click the Policy button on the AppDetectivePro toolbar.
2	If you want to view: <ul style="list-style-type: none"> • Pen Test Policies, click the Pen Test tab • Audit policies, click the Audit tab.

Step	Action
3	Click the Policy you want to view.
4	Click the View Selected button. The Policy Editor appears.
5	Click the + signs next to the descriptions to view the active checks in the Policy.
6	Click the checks to view their details. To print a check description, right click the description, and choose Print .

Appendix C: Troubleshooting

This appendix consists of the following topics:

- Port Discovery
- False Positives
- Oracle Advanced Security
- Personal Firewalls
- Running User Rights Review With an Access Back-End.

Port Discovery

AppDetectivePro has been designed to be efficient at finding servers and their IP addresses. However, Discovering large numbers of ports on each particular IP address will take a long time to finish. For example, Discovering 60,000 ports on a single IP address takes a significant amount more time than scanning a class C network for active servers.

False Positives

False positives can occur when inconclusive version information is gathered from an application. Below is an example of a false positive that occurs while conducting an Oracle check.

Oracle versions are formatted as such: 8.1.6.3.5, where:

- 8 = the major version
- 1 = the minor version, in this case 8i
- 6 = the release, in this case release 2 of Oracle8i
- 3 = the patch set applied
- 5 = the patch applied.

Oracle advertises its version as 8.1.6.3.0 even if patch 5 is installed as shown above. From a network perspective, or even from a valid database connection, it is inconclusive if the exact patch is installed. AppDetectivePro behaves in the following way:

- If the version were clearly vulnerable, as version 8.1.6.1 would be, the check would record the vulnerability.
- If the version were clearly not vulnerable, as version 8.1.6.4 would not be, the check would not record the vulnerability.
- If there is a patch for the specific version, as would be for 8.1.6.3, we know that the vulnerability exists, but can't be 100% sure the patch is installed. In this situation, AppDetectivePro records this as a vulnerability and in the details of the vulnerability, specifies `Status=Patch available for patch set, can not detect if patch is installed`, informing you there may be a vulnerability.

You can verify the exact version of the patch installed by connecting to the operating system and accessing the file system to verify the version of the files included with the patch. This functionality is being added to the audit mode of AppDetectivePro, but doesn't currently exist.

Oracle Advanced Security

If your Oracle database is configured using ASO encryption or check summing is enabled on the network traffic, AppDetectivePro will not be able to Pen Test the Oracle database. Auditing the Oracle database will work as expected.

Personal Firewalls

AppDetectivePro runs significantly faster if a personal firewall is not installed on the local machine. Application Security, Inc. recommends you disable all personal firewalls (such as Zone Alarm, Blackice Defender, and Norton Personal Firewall) when using AppDetectivePro.

Running User Rights Review With an Access Back-End

If your AppDetectivePro back-end database is Microsoft Access, you may receive the following error while purging a User Rights Review:

```
File sharing lock count exceeded. Increase MaxLocksPerFile registry entry.
```

This error is caused by limitation of Microsoft's Jet driver when trying to perform an operation (in this case, a delete) that affects many rows in the database.

To work around this issue, you must set the registry key `HKEY_LOCAL_MACHINE\Software\Microsoft\Jet4.0\Engines\Jet 4.0\MaxLockPerFile` to at least 100000 (the default setting is 9500).

For more information on purging data, see *Purging Data*.

Appendix D: Using Default and Custom Dictionaries

This appendix consists of the following topics:

- Default Dictionaries
- Custom Dictionaries.

Default Dictionaries

AppDetectivePro includes several default dictionaries. These are used in various AppDetectivePro security checks. These files are located, by default, in: [<installation directory>](#)\Program Files\AppSecInc\Common Files\.

This topic consists of the following sub-topics:

- Password-Cracking Algorithms and Server Performance
- Oracle Default Dictionaries
- Sybase Default Dictionaries
- Lotus Domino Default Dictionaries
- Microsoft SQL Server 2000 Default Dictionaries
- IBM DB2 Default Dictionaries
- IBM DB2 z/OS Default Dictionaries
- MYSQL Default Dictionaries.

PASSWORD-CRACKING ALGORITHMS AND SERVER PERFORMANCE

Any password-cracking performed on the client has no effect on the performance of your server. Specifically, for:

- **MSSQL 2000 password-cracking.** Hashes are downloaded to the client and verified.
- **MSSQL 7 password-cracking.** Testing is performed on the database server. Large dictionaries can slow down the database.
- **Sybase ASE password-cracking.** Hashes are downloaded to the client and verified.

- **Oracle password-cracking.** Hashes are downloaded to the client and verified; each account takes approximately 30 seconds to compare against a 50,000 word dictionary.
- **DB2 password-cracking.** Performed during Pen Tests only.

ORACLE DEFAULT DICTIONARIES

For Pen Tests

- Easily-guessed database password - `basic.txt`
- Easily-guessed database username - `large-familynames.txt`
- Easily-guessed password for internal account - `medium-dictionary.txt`
- Easily-guessed password for listener - `medium-dictionary.txt`
- Easily-guessed password SYS as SYSDBA - `medium-dictionary.txt`
- Easily-guessed password SYSTEM as SYSDBA - `medium-dictionary.txt`

For Audits

- Easily-guessed database password - `large-dictionary.txt`
- Easily-guessed password for SYSDBA - `large-dictionary.txt`
- Easily-guessed password SYSOPER - `large-dictionary.txt`
- Easily-guessed role password - `large-dictionary.txt`

SYBASE DEFAULT DICTIONARIES

For Pen Tests

- Easily-guessed sa password - `sybase-basic.txt`
- Easily-guessed mon_user password - `sybase-basic.txt`
- Easily-guessed probe password - `sybase-basic.txt`
- Easily-guessed sybmail password - `sybase-basic.txt`
- Easily-guessed username (12.0+ only) - `sybase-fast-familynames.txt`
- Easily-guessed password (12.0+ only - works on accounts found in previous check) - `sybase-basic.txt`

For Audits

- Easily-guessed password - `sybase-fast-dictionary.txt`
- Easily-guessed sa password - `sybase-fast-dictionary.txt`

LOTUS DOMINO DEFAULT DICTIONARIES

For Pen Tests

- Easily-guessed username through mail databases - lotus-medium-familynames.txt
- Easily-guessed known-user password for basic authentication - lotus-fast-dictionary.txt
- Easily-guessed known-user password for SSO - lotus-brute-force.txt
- Easily-guessed username/password for basic authorization:
 - UserNames: lotus-veryfast-usernames.txt
 - Passwords: lotus-brute-force.txt
- Easily-guessed username/password for SSO:
 - UserNames: lotus-veryfast-usernames.txt
 - Passwords: lotus-brute-force.txt

For Audits

- Easily-guessable Notes password: lotus-medium-dictionary.txt
- Easily-guessed password for sa - sqlsvr-fast-dictionary.txt
- Easily-guessed password for well-known logins - sqlsvr-fast-dictionary.txt

MICROSOFT SQL SERVER 2000 DEFAULT DICTIONARIES

For Pen Tests

- Blank password - sqlsvr-medium-familynames.txt
- Password same as login - sqlsvr-medium-familynames.txt
- Easily-guessed password – attempt each login in sqlsvr-fast-familynames.txt with each password in mssql-basic.txt

IBM DB2 DEFAULT DICTIONARIES

For Audits

- Easily-guessed database password - `sqlsvr-large-dictionary.txt`
- Easily-guessed password for sa - `sqlsvr-large-dictionary.txt`
- Easily-guessed password for well-known logins - `sqlsvr-fast-dictionary.txt`

For Pen Tests

- Easily-guessed password for well-known account - `db2_medium-dictionary.txt`
- Password same as username for account - `db2_medium-familynames.txt`
- Password same as username for well-known account - `db2_default_accts.asi` used for both usernames and passwords

IBM DB2 z/OS DEFAULT DICTIONARIES

For Audits

- Easily-guessed usernames and passwords - Usernames are taken from `db2_medium-familynames.txt` and passwords from `db2_medium-dictionary.txt`.

Note:	In AppDetectivePro 5.0.6 and greater, you can set your own dictionary file for the easily-guessed usernames and passwords Audit check.
--------------	--

Password same as username for account - Does not require a dictionary; usernames collected from the database are used as passwords.

MYSQL Default Dictionaries

FOR AUDITS

- Easily guessed password - `mysql-basic.txt` used for passwords
- Easily guessed root password - `mysql_fast-familynames.txt` used for passwords

FOR PEN TESTS

- Easily guessed password - `mysql_fast-familynames.txt` used for account names and `mysql_basic.txt` used for passwords

- Blank password check - `mysql_fast-familynames.txt` used for account names
- Easily guessed root password - `mysql-basic.txt` used for passwords
- Password same as username - `mysql_large-familynames.txt` used for both usernames and passwords

Custom Dictionaries

AppDetectivePro allows you to include custom dictionaries for brute force checks. The topic consists of the following sub-topics:

- Creating a Custom Dictionary
- Including a Custom Dictionary in a Policy.

CREATING A CUSTOM DICTIONARY

To create a custom dictionary:

Step	Action
1	<p>Create a <code>.txt</code> file containing your word list (custom dictionary). Each word must be on its own line. In other words, there must be a “hard” return between every word.</p> <p>Correct:</p> <pre>apple bamboo carrot</pre> <p>Incorrect:</p> <pre>apple, bamboo, carrot</pre>
2	<p>Save the <code>.txt</code> file (custom dictionary).</p>

INCLUDING A CUSTOM DICTIONARY IN A POLICY

To include a custom dictionary in a Policy:

Step	Action
1	Click the Policy button on the toolbar.
2	Click the Pen Test tab.
3	Click Brute Force Policy .
4	Click the View Selected button.
5	Expand the Password Attacks section by clicking the + sign.
6	Customize Easily-Guessed checks to use personal dictionaries.
7	Select Dictionary Name and browse to choose the dictionary you would like to use.
8	Choose the Save As button to save your changes.

Appendix E: Using NMAP

This appendix consists of the following topics:

- What is NMAP?
- Prerequisites
- NMAP Command Line Syntax
- Creating an NMAP-Generated Output File
- Using Your NMAP-Generated File with AppDetectivePro.

What is NMAP?

NMAP is an open source utility which has become the industry standard for discovering large networks. NMAP can be used to Discover host ip addresses, open ports, as well as operating system versions.

AppDetectivePro can use the output generated by NMAP during a Discovery. This saves time in the Discovery scan because AppDetectivePro already “knows” which ip addresses and ports to probe.

Important! AppDetectivePro **only** supports NMAP normal output files when you use the `-sS` or `-sT` options.

For more information on:

- NMAP, see <http://www.nmap.org>
- using NMAP output files with AppDetectivePro tasks, see *Part II. AppDetectivePro Tasks*.

Prerequisites

To customize AppDetectivePro to use NMAP-generated output files, you must have the following:

- AppDetectivePro version 5.1.0 and greater
- A working installation of NMAP to create NMAP-generated output files.

NMAP is on most Unix machines and is now available for Windows. You can download versions from <http://www.nmap.org>.

NMAP Command Line Syntax

The following table explains the tested/supported NMAP command line syntax.

nmap	sS	<hostname>	-oN Normal.	output.nmap
	sT		-oG Greppable.	output.gnmap
			-oA Both formats.	output This creates three output files: output.nmap, output.gnmap, and output.txt).

Consequently, you can enter any one of the following supported/tested commands in Step 2 of Creating an NMAP-Generated Output File:

- `nmap -sS <hostname> -oN output.nmap`

- `nmap -sT <hostname> -oN output.nmap`
- `nmap -sS <hostname> -oG output.gnmap`
- `nmap -sT <hostname> -oG output.gnmap`
- `nmap -sS <hostname> -oA output`
- `nmap -sT <hostname> -oA output`

Creating an NMAP-Generated Output File

Note: These instructions were tested using AppDetectivePro version 5.1.6 and NMAP version 4.01 for Windows.

To create an NMAP-generated output file:

Step	Action
1	Log into the workstation where NMAP is available.
2	<p>At the command line, you can run a command any of the following supported/tested commands to generate a scan and to place the results into an NMAP file on your <code>c:</code> drive:</p> <ul style="list-style-type: none"> • <code>nmap -sS <hostname> -oN output.nmap</code> • <code>nmap -sT <hostname> -oN output.nmap</code> • <code>nmap -sS <hostname> -oG output.gnmap</code> • <code>nmap -sT <hostname> -oG output.gnmap</code> • <code>nmap -sS <hostname> -oA output</code> • <code>nmap -sT <hostname> -oA output.</code>
3	Once the NMAP scan is complete, transfer the file over to your machine where AppDetectivePro is installed.
4	Optionally, you can open your NMAP-generated file in a text editor (such as Microsoft WordPad).

Using Your NMAP-Generated File with AppDetectivePro

To use your NMAP-generated file with AppDetectivePro:

Step	Action
1	Choose Start > Programs > AppSecInc > AppDetective to start AppDetectivePro.
2	Do one of the following: <ul style="list-style-type: none">• choose Session > New from the menu• click the New button on the toolbar• press <CTRL>+N. The Session wizard appears.
3	Click the Next button. The next page of the Session wizard appears.
4	Select Load list of live network IPs and ports from a file.
5	Click the Next button. The Which file would you like to use? page of the Session wizard appears.
6	Use the drop-down to select NMAP .
7	Click the Next button. The Open pop-up appears.
8	Locate the NMAP-generated file on the machine where AppDetectivePro is installed, as specified in Step 3 of Creating an NMAP-Generated Output File.
9	Highlight the NMAP-generated file and click the Open button. The Open pop-up closes.

Step	Action
10	<p>Check one or more of the following application types to Discover:</p> <ul style="list-style-type: none">• HTTP Web Servers• IBM DB2 z/OS• IBM DB2• Lotus Domino• Microsoft SQL Server• MySQL• Oracle (All Components or Database Only)• Sybase Advance Server Enterprise.
11	<p>Click the Next button.</p> <p>The next page of the Session wizard appears.</p>
12	<p>Enter the:</p> <ul style="list-style-type: none">• Session name (required)• Session description (optional). <p>The next page of the Session wizard appears.</p>
13	<p>Click the Next button.</p> <p>The next page of the Session wizard displays your Session summary information.</p>
14	<p>Run a Discovery; for more information, see <i>Discovery</i>.</p> <p>The network tree is populated with valid applications Discovered by AppDetectivePro. You can Pen Test or Audit any Discovered applications; for more information, see <i>Pen Tests, Audits, and User Rights Reviews</i>.</p>

Appendix F: Clearing Sybase Application Logs

Sybase application logs can become full when AppDetectivePro conducts brute force attacks. This appendix explains how to clear the full Sybase application logs.

Note: You need **Administrator**-level access to perform this task.

To clear Sybase application logs:

Step	Action
1	Enter <code>isql -Usa -S<servername></code> at the command line to connect to the database.
2	Enter your password at the prompt.
3	Enter the <code>dump transaction</code> log command at the prompt: <code>dump transaction <database_name> with no_log</code>
4	Enter the <code>go</code> command. The Sybase application logs are cleared.
5	Exit your interactive SQL connection.

Appendix G: Audit and User Rights Review Privileges

This appendix consists of the following topics:

- IBM DB2 Audit Privileges
- IBM DB2 z/OS Audit Privileges
- Lotus Domino Groupware Audit Privileges
- Microsoft SQL Server Audit Privileges and User Creation Scripts
- MySQL Audit Privileges
- Oracle Audit Privileges and User Creation Script
- Sybase Audit Privileges

- Operating System Considerations (for Audits)
- Microsoft SQL Server User Rights Review Privileges
- Oracle User Rights Review Privileges

IBM DB2 Audit Privileges

Note:	For more information on IBM DB2 OS check requirements, see Operating System Considerations (for Audits).
--------------	--

To conduct a full IBM DB2 Audit, you need the following privileges. Make sure the account you are using has rights to use the following tables, views, and functions:

- CONNECT
- GET DATABASE MANAGER CONFIGURATION & LIST DATABASE DIRECTORY
- Service Info (on Windows only)
- SYSIBM.SYSCOLAUTH
- SYSIBM.SYSINDEXAUTH
- SYSIBM.SYSPASSTHROUGH
- SYSIBM.SCHEMAAUTH
- SYSIBM.SYSDBAUTH
- SYSIBM.SYSTABAUTH
- SYSIBM.SYSFUNCTIONS
- SYSIBM.SYSPROCEDURES
- SYSIBM.SYSVERSIONS
- SYSPROC.SNAPSHOT_DATABASE

Note:	<code>SYSPROC.SNAPSHOT_DATABASE</code> requires the Audit user to have <code>SYSMON</code> authority. Users with <code>SYSADM</code> , <code>SYSCTRL</code> , or <code>SYSMAINT</code> authority automatically inherit <code>SYSMON</code> authority.
--------------	---

Below is a list of checks within AppDetectivePro for an IBM DB2 Audit, and the tables and views they need permission to access in order to function properly:

- CLIENT authentication: GET DATABASE MANAGER CONFIGURATION & LIST DATABASE DIRECTORY
- SERVER authentication: GET DATABASE MANAGER CONFIGURATION & LIST DATABASE DIRECTORY

- DCS authentication: GET DATABASE MANAGER CONFIGURATION & LIST DATABASE DIRECTORY
- Trust All Client: GET DATABASE MANAGER CONFIGURATION & LIST DATABASE DIRECTORY
- Authentication type: GET DATABASE MANAGER CONFIGURATION & LIST DATABASE DIRECTORY
- Service runs as LocalSystem: Windows Management Instrumentation (WMI) with Admin privileges (Windows ONLY)
- Permissions granted to PUBLIC: SYSIBM.SYSCOLAUTH, SYSIBM.SYSINDEXAUTH, SYSIBM.SYSPASSTHROUGH, SYSIBM.SCHEMAAUTH, SYSIBM.SYSDBAUTH, SYSIBM.SYSTABAUTH
- Permissions granted to user: SYSIBM.SYSCOLAUTH, SYSIBM.SYSINDEXAUTH, SYSIBM.SYSPASSTHROUGH, SYSIBM.SCHEMAAUTH, SYSIBM.SYSDBAUTH, SYSIBM.SYSTABAUTH
- Permissions grantable: SYSIBM.SYSCOLAUTH, SYSIBM.SYSINDEXAUTH, SYSIBM.SYSPASSTHROUGH, SYSIBM.SCHEMAAUTH, SYSIBM.SYSDBAUTH, SYSIBM.SYSTABAUTH
- Permissions on system catalog: SYSIBM.SYSDBAUTH, SYSIBM.SYSTABAUTH
- Permissions to list users: SYSIBM.SYSDBAUTH, SYSIBM.SYSTABAUTH
- db2ckpwd buffer overflow (Version verify): SYSIBM.SYSVERSIONS
- Query Compiler DoS (Verify version): SYSIBM.SYSVERSIONS
- Date/Varchar DoS (Verify version): SYSIBM.SYSVERSIONS
- Latest FixPak not installed: SYSIBM.SYSVERSIONS
- Control Center buffer overflow (Verify version): SYSIBM.SYSVERSIONS
- Excessive DBADM connections

For the `Excessive DBADM connections` check, the IBM DB2 OS user must have:

- `SELECT` or `CONTROL` privilege on the `APPLICATIONS` and `SNAPAPPL_INFO` administrative views
- `SYSMON`, `SYSCTRL`, `SYSMAINT`, or `SYSADM` authority which is required to access snapshot monitor data.

Some DB2 Audit checks need to differentiate between fixpaks such as 4/4a, 6/6a, etc. These checks require specific permissions. Specifically, the checks affected are:

- Arbitrary code execution in a federated system (Verify version)
- Arbitrary code execution when processing connection messages (Verify version)
- Arbitrary file creation in XML Extender functions (Verify version)
- Buffer overflow in CALL statement (Verify version)
- Buffer overflow in db2fmp (Verify version)
- Buffer overflow in generate_distfile procedure (Verify version)
- Buffer overflow in REC2XML function (Verify version)
- Buffer overflow in SATADMIN.SATENCRYPT function (Verify version)
- Buffer overflow in the JDBC listener (Verify version)
- Buffer overflows in XML Extender functions (Verify version)
- DoS in string formatting functions (Verify version)
- Latest FixPak not installed
- Multiple Buffer overflows in libdb2.so.1 library (Verify version)
- Multiple critical vulnerabilities in IBM DB2 (Verify version)
- Multiple DoS vulnerabilities in SQLJRA protocol

The IBM DB2 OS user must have access to the [db2greg](#) command on all Unix platforms for the following IBM DB2 LUW checks:

- [Permission on files](#)
- [Setuid bit enabled](#)
- [Setgid bit enabled](#)

In order for AppDetectivePro to work properly with any of these checks, you must set special permissions, depending on what version of DB2 is running on your server.

The following table explains which permissions are required for which versions of DB2:

If your server is running DB2 version:	Requirements:
9.10 or later	<p><code>SELECT</code> or <code>CONTROL</code> privilege on the <code>ENV_INST_INFO</code> administrative view.</p> <p>OR</p> <p><code>SYSADM</code> and/or <code>ATTACH</code> privileges.</p> <p>AND</p> <p><code>EXECUTE</code> privilege on the <code>ENV_GET_INST_INFO</code> table function (required for IBM DB2 LUW v 8.2.2 and later).</p>
8.2.2 or later	<code>EXECUTE</code> privilege on the <code>ENV_GET_INST_INFO</code> table function.
8.1.0 or later	<code>SYSADM</code> or <code>ATTACH</code> privileges.
7	Registry access or OS access.

IBM DB2 z/OS Audit Privileges

This topic consists of the following sub-topics:

- Full IBM DB2 z/OS Audit Requirements
- Per Check IBM DB2 z/OS Audit Requirements.

FULL IBM DB2 z/OS AUDIT REQUIREMENTS

You require the following permissions (which `SYSADM` has by default) in order to conduct a full IBM DB2 z/OS Audit with all checks enabled:

- **SELECT** privileges on the following catalog tables:
 - SYSIBM.SYSCOLAUTH
 - SYSIBM.SYSDBAUTH
 - SYSIBM.SYSPACKAUTH
 - SYSIBM.SYSPLANAUTH
 - SYSIBM.SYSROUTINEAUTH
 - SYSIBM.SYSSCHEMAAUTH
 - SYSIBM.SYSTABAUTH
 - SYSIBM.SYSUSERAUTH
 - SYSIBM.GETVARIABLE
- Permission to call the following function: `SYSIBM.GETVARIABLE`
- Permission to call the following stored procedure: `SYSPROC.DSNWZP`

PER CHECK IBM DB2 z/OS AUDIT REQUIREMENTS

To conduct an IBM DB2 z/OS Audit with selected checks enabled, the following permissions are required in a per-check basis:

- All checks require permission to call the following function:
`SYSIBM.GETVARIABLE`
- The following IBM DB2 z/OS Audit checks require permission to call the stored procedure `SYSPROC.DSNWZP`:
 - Dual logging not enabled
 - Dual archiving not enabled
 - SMF accounting is not set to start automatically
 - Audit Trace is not set to start automatically
 - SMF statistics not set to start automatically
 - Authorization checking disabled
 - Collection interval for statistics
 - System install administrators and operators

Note:	If the <code>SYSPROC.DSNWZP</code> and <code>SYSPROC.ADMIN_DS_LIST</code> stored procedures are not enabled, you must enable them and set up the proper environments so they can function correctly.
--------------	---

- The IBM DB2 z/OS Audit check [Connection and sign-on exits](#) requires permission to call the stored procedure `SYSPROC.ADMIN_DS_LIST`.
- The following table lists IBM DB2 z/OS Audit checks which **must** have `SELECT` privileges on the corresponding IBM DB2 z/OS tables:

Check	Corresponding IBM DB2 z/OS tables requiring <code>SELECT</code> privileges
Access list of authorization IDs	SYSIBM.SYSTABAUTH
Administrative authorities on DB2 Subsystem	SYSIBM.SYSUSERAUTH
Privileges granted to PUBLIC on packages	SYSIBM.SYSPACKAUTH
Administrative authorities for DB2 catalog database	SYSIBM.SYSDBAUTH
Administrative authorities over databases	SYSIBM.SYSDBAUTH
Privileges granted to PUBLIC on plans	SYSIBM.SYSPLANAUTH
PUBLIC granted Administrative authorities on DB2 Subsystem	SYSIBM.SYSUSERAUTH
Privileges granted to PUBLIC on columns	SYSIBM.SYSCOLAUTH
Privileges granted to PUBLIC on routines	SYSIBM.SYSROUTINEAUTH
<ul style="list-style-type: none"> • Easily-guessed usernames and passwords • No permission is required • Privileges granted to PUBLIC on databases 	SYSIBM.SYSDBAUTH
Privileges granted to PUBLIC on DB2 subsystem	SYSIBM.SYSUSERAUTH

Check	Corresponding IBM DB2 z/OS tables requiring SELECT privileges
Password same as username for account	SYSIBM.SYSDBAUTH SYSIBM.SYSTABAUTH SYSIBM.SYSPLANAUTH SYSIBM.SYSCOLAUTH SYSIBM.SYSSCHEMAAUTH SYSIBM.SYSPACKAUTH SYSIBM.SYSROUTINEAUTH SYSIBM.SYSUSERAUTH
Privileges on the DB2 catalog	PSYSTABAUTH
Privileges granted to PUBLIC on schemas	SYSIBM.SYSSCHEMAAUTH
Privileges granted to PUBLIC on DB2 catalog tables	SYSTABAUTH
Privileges granted to PUBLIC on tables	SYSTABAUTH
Administrative authority for database granted to PUBLIC	SYSIBM.SYSDBAUTH
Default User IDs	SYSIBM.SYSTABAUTH SYSIBM.SYSCOLAUTH SYSIBM.SYSDBAUTH SYSIBM.SYSPACKAUTH SYSIBM.SYSPLANAUTH SYSIBM.SYSRESAUTH SYSIBM.SYSROUTINEAUTH SYSIBM.SYSUSERAUTH SYSIBM.SYSSCHEMAAUTH SYSIBM.SYSSEQUENCEAUTH

Lotus Domino Groupware Audit Privileges

Note: For more information on Lotus Domino OS check requirements, see Operating System Considerations (for Audits).

To conduct a full Lotus Domino Groupware Audit, you need the following privileges. Make sure the account you are using has rights to use the following tables and views:

- Read all databases
- Read decsadm.nsf and all of its documents
- Read names.nsf and all of its documents
- Execute commands on the server
- Read all user documents

At a document level, AppDetectivePro checks certain fields, including: `$Author`, `$Readers`, `RM_MapFrom`, `$Readers`, and fields of type `LNRTTYPE_AUTHORS_FIELD`.

AppDetectivePro also verifies certain Lotus Domino Groupware properties (for example, if you have attachments and if they are encrypted). If any of the required fields listed above are encrypted and the id does not have access to it, then some of the checks below will not work properly.

Caution! **Depositor** access that **only** has access to read public documents is sufficient to run a Lotus Domino Groupware Audit, with the exception of the `names.nsf` database which requires **Reader** access.

Besides `SHOW` commands, the following Lotus Domino Groupware commands are also executed:

- `TELL HTTP SHOW FILE ACCESS`
- `SET SECURE`

Below is a list of checks within the AppDetectivePro for a Lotus Domino Audit, and the tables and views they need permission to access in order to function properly:

- Anonymous can create documents: Read all databases
- Anonymous granted Designer or higher access: Read all databases
- Anonymous user in Authors field: Read all databases
- Default has Editor or higher access: Read all databases
- Encrypted field full-text indexed: Read all databases
- Unspecified user type in ACL: Read all databases
- DECS password unencrypted: Read deccsadm.nsf and all of its documents
- Anonymous ACL missing: Read all databases, Read names.nsf and all of its documents
- Access server unrestricted: Read names.nsf and all of its documents
- All people can use monitors: Read names.nsf and all of its documents
- All users can run personal agents: Read names.nsf and all of its documents
- Anonymous access via HTTPS: Read names.nsf and all of its documents
- Anonymous access via Notes RPC: Read names.nsf and all of its documents
- Bindsock arbitrary file creation: Read names.nsf and all of its documents
- CGI directory leak: Read names.nsf and all of its documents
- Check passwords on Notes IDs: Read names.nsf and all of its documents
- Create databases unrestricted: Read names.nsf and all of its documents
- Enumerate groups: Read names.nsf and all of its documents
- Failed access control on file attachments: Read names.nsf and all of its documents
- iNotes client ActiveX control buffer overflow: Read names.nsf and all of its documents
- iNotes s_ViewName buffer overflow: Read names.nsf and all of its documents
- Latest maintenance release not applied: Read names.nsf and all of its documents
- Long POST request DoS: Read names.nsf and all of its documents
- Maximum number of request headers: Read names.nsf and all of its documents
- Maximum size of request contents: Read names.nsf and all of its documents
- Maximum size of request headers: Read names.nsf and all of its documents
- Maximum URL length: Read names.nsf and all of its documents
- Maximum URL path segments: Read names.nsf and all of its documents
- Non-admins can use monitors: Read names.nsf and all of its documents

- Notes RPC buffer overflow: Read names.nsf and all of its documents
- Notes_ExecDirectory buffer overflow: Read names.nsf and all of its documents
- Password change interval for user: Read names.nsf and all of its documents
- PATH buffer overflow: Read names.nsf and all of its documents
- Public keys compared to directory: Read names.nsf and all of its documents
- Restricted agents runlist: Read names.nsf and all of its documents
- Restricted Java/COM runlist: Read names.nsf and all of its documents
- Saved email not encrypted: Read names.nsf and all of its documents
- Servlets disabled: Read names.nsf and all of its documents
- Unrestricted agents runlist: Read names.nsf and all of its documents
- Unrestricted Java/COM runlist: Read names.nsf and all of its documents
- User can create new databases: Read names.nsf and all of its documents
- Administration over HTTP: Read names.nsf and all of its documents, Execute a command on the server
- Anonymous access via HTTP: Read names.nsf and all of its documents, Execute a command on the server
- Anonymous access via IIOP: Read names.nsf and all of its documents, Execute a command on the server
- Anonymous access via IIOPS: Read names.nsf and all of its documents, Execute a command on the server
- Anonymous access via LDAP: Read names.nsf and all of its documents, Execute a command on the server
- Anonymous access via LDAPS: Read names.nsf and all of its documents, Execute a command on the server
- ESMTTP buffer overflow: Read names.nsf and all of its documents, Execute a command on the server
- Expired certificates allowed: Read names.nsf and all of its documents, Execute a command on the server
- HTTP authenticate buffer overflow: Read names.nsf and all of its documents, Execute a command on the server
- HTTP database browsing: Read names.nsf and all of its documents, Execute a command on the server
- HTTP logging not enabled: Read names.nsf and all of its documents, Execute a command on the server
- HTTP methods excluded from logging: Read names.nsf and all of its documents, Execute a command on the server
- HTTP MIME types excluded from logging: Read names.nsf and all of its documents, Execute a command on the server

- HTTP return codes excluded from logging: Read names.nsf and all of its documents, Execute a command on the server
- HTTP user agents excluded from logging: Read names.nsf and all of its documents, Execute a command on the server
- HTTPS allows anonymous access: Read names.nsf and all of its documents, Execute a command on the server
- Inadequate amgr process logging: Read names.nsf and all of its documents, Execute a command on the server
- Incomplete POST DoS: Read names.nsf and all of its documents, Execute a command on the server
- Interface address leak in banner: Read names.nsf and all of its documents, Execute a command on the server
- LDAP buffer overflow: Read names.nsf and all of its documents, Execute a command on the server
- LDAP format string: Read names.nsf and all of its documents, Execute a command on the server
- MS-DOS device web path leak: Read names.nsf and all of its documents, Execute a command on the server
- Personal agents runlist: Read names.nsf and all of its documents, Execute a command on the server
- Redirected host/location buffer overflow: Read names.nsf and all of its documents, Execute a command on the server
- Routing loop DoS (Verify version): Read names.nsf and all of its documents, Execute a command on the server
- SMTP buffer overflow: Read names.nsf and all of its documents, Execute a command on the server
- Unencrypted HTTP: Read names.nsf and all of its documents, Execute a command on the server
- Unencrypted IIOP: Read names.nsf and all of its documents, Execute a command on the server
- Unencrypted IMAP: Read names.nsf and all of its documents, Execute a command on the server
- Unencrypted LDAP: Read names.nsf and all of its documents, Execute a command on the server
- Unencrypted NNTP: Read names.nsf and all of its documents, Execute a command on the server
- Unencrypted POP3: Read names.nsf and all of its documents, Execute a command on the server
- Web retriever HTTP status buffer overflow: Read names.nsf and all of its documents, Execute a command on the server
- Web Retriever logging: Read names.nsf and all of its documents, Execute a command on the server

- Easily-guessed Internet password: Read all user documents
- Easily-guessed Notes password: Read all user documents
- Agent manager debugging not enabled: Execute a command on the server
- Ambiguous webnames allowed: Execute a command on the server
- Console password not set: Execute a command on the server
- Inadequate console logging: Execute a command on the server
- NDS password present: Execute a command on the server
- NDS userid present: Execute a command on the server
- Phone line logging not enabled: Execute a command on the server

Microsoft SQL Server Audit Privileges and User Creation Scripts

Note:	For more information on Microsoft SQL Server OS check requirements, see Operating System Considerations (for Audits).
-------	---

This topic consists of the following sub-topics:

- [Microsoft SQL Server 2000 and MSDE Audit Privileges](#)
- [Running the Microsoft SQL Server 2000 User Creation Script](#)
- [Running the Microsoft SQL Server 2000 with Sysadmin User Creation Script](#)
- [Microsoft SQL Server 2005 and Microsoft SQL Server 2008 Audit Privileges](#)
- [Credentials for Microsoft SQL Server Audits](#)
- [Running the Microsoft SQL Server 2005 and 2008 User Creation Script](#)
- [Registry Access for Microsoft SQL Server 2000, 2005, and 2008](#)

MICROSOFT SQL SERVER 2000 AND MSDE AUDIT PRIVILEGES

To conduct a full Microsoft SQL Server 2000 or MSDE Audit, you need the following privileges. Make sure the account you are using has rights to use the following tables and views:

Check	Privileges Required
master.dbo.xp_loginconfig	EXECUTE
master.dbo.xp_regread	
exec <db name>.dbo.sp_helpprotect	
msdb.dbo.sp_get_sqlagent_properties	
master.dbo.xp_cmdshell	

```

@@VERSION
master.dbo.syslogins (MSSQLSysLogins)
master.dbo.sysxlogins
master.dbo.sysdatabases
master.dbo.sysconfigures
master.dbo.syscurconfigs
master.dbo.syscharsets
<db name>.dbo.sysusers
<db name>.dbo.sysobjects
<db name>.dbo.syscomments
    
```

In addition, certain Microsoft SQL Server 2000 DISA-STIG Database Security Configuration checks require you to be a member of the `sysadmin` fixed server role or the `db_owner` fixed database role on the publication database. The following table provides specific information about which checks require which roles (and why):

Microsoft SQL Server 2000 DISA-STIG checks:	Use:	To run these checks, you must be a member of:
DBMS replication account privileges Replication snapshot folder protection	Replication system stored procedures.	The <code>sysadmin</code> fixed server role or the <code>db_owner</code> fixed database role on the publication database.
Database auditing Auditing of Security Events Startup Stored Procedures	<code>fn_trace_getinfo</code> and <code>fn_trace_geteventinfo</code> functions.	The <code>sysadmin</code> fixed server role.

Below is a list of checks within the AppDetectivePro for a Microsoft SQL Server 2000 Audit, and the tables and views they need permission to access in order to function properly.

Note: To learn more about enabling registry access for Microsoft SQL Server 2000, see [Registry Access for Microsoft SQL Server 2000, 2005, and 2008](#).

- Agent jobs privilege escalation: `exec <db name>.dbo.sp_helpprotect, master.dbo.sysdatabases`
- Auditing of failed logins: `master.dbo.xp_loginconfig`
- Auditing of successful logins: `master.dbo.xp_loginconfig`
- Blank password: `master.dbo.sysxlogins`
- Blank password for sa: `master.dbo.sysxlogins`
- Blank password for well-known login: `master.dbo.sysxlogins`
- BULK INSERT buffer overflow: `@@VERSION`
- C2 Audit Mode: `@@VERSION, master.dbo.sysconfigures, master.dbo.syscurconfigs`
- Case-insensitive sort order: `master.dbo.syscharsets, master.dbo.sysconfigures, master.dbo.syscurconfigs`
- Changing mode may leave sa password blank: `@@VERSION`
- Cleartext password written by installation: `@@VERSION, master.dbo.xp_cmdshell`
- Computed Column UDF DoS: `@@version`
- Database ownership chaining not disabled: `sysconfigures, syscurconfigs`
- DBCC addextendedproc buffer overflow: `@@VERSION`
- DBCC BUFFER buffer overflow: `@@VERSION`
- DBCC CHECKCONSTRAINTS buffer overflow: `@@VERSION`
- DBCC CLEANABLE buffer overflow: `@@VERSION`
- DBCC INDEXDEFRAG buffer overflow: `@@VERSION`
- DBCC PROCBUF buffer overflow: `@@VERSION`
- DBCC SHOWCONTIG buffer overflow: `@@VERSION`
- DBCC SHOWTABLEAFFINITY buffer overflow: `@@VERSION`
- DBCC UPDATEUSAGE buffer overflow: `@@VERSION`
- DBMS remote system credential use and access: `master.dbo.sysxlogins, [master].dbo.sys.servers`
- Default login enabled: `@@VERSION, master.dbo.syslogins, master.dbo.xp_loginconfig`
- Direct updates on data dictionary: `master.dbo.sysconfigures, master.dbo.syscurconfigs`
- DTS package procedures granted to public: `sp_helpprotect`
- DTS package password publicly viewable: `msdb.dbo.sysuser, exec msdb.dbo.sp_helpprotect`
- DTS password exposed in properties dialog: `@@VERSION`
- DTS passwords publicly viewable: `<db name>.dbo.sysuser, exec <db name>.dbo.sp_helpprotect, master.dbo.sysdatabases`
- Easily-guessed password: `@@VERSION`
- Easily-guessed password for sa: `@@VERSION`
- Easily-guessed password for well-known login: `@@VERSION`

- Encoded password written by installation: @@VERSION, master.dbo.xp_cmdshell
- Enterprise Manager improperly revokes proxy account: @@VERSION
- [Error logs can be overwritten: Registry access](#)
- Escalated privileges in heterogeneous joins: @@VERSION
- Extended stored proc privilege upgrade: exec <db name>.dbo.sp_helprotect, master.dbo.sysdatabases
- Fixed server role granted: master.dbo.syslogins
- Format string in C runtime DoS: @@VERSION
- Format string vuln in xp_sprintf: @@VERSION
- FORMATMESSAGE buffer overflow: @@VERSION
- Global temporary stored proc exists: sysobjects,sysusers
- Guest user exists in database: <db name>.dbo.sysuser, master.dbo.sysdatabases
- Hello buffer overflow: @@VERSION
- Infected with Spida worm: <db name>.dbo.sysobjects, master.dbo.sysdatabases, master.dbo.xp_cmdshell
- [Jet running in sandbox Mode: Registry access](#)
- Job output file handling: @@VERSION
- Latest service pack applied: @@VERSION
- Lumigent Log Explorer buffer overflow: <db name>.dbo.sysobjects, master.dbo.sysdatabases
- Malformed RPC request DoS: @@VERSION
- Malformed TDS packet header DoS: @@VERSION
- MDX Query buffer overflow: @@VERSION
- Objects not owned by dbo: <db name>.dbo.sysobjects, master.dbo.sysdatabases, <db name>.dbo.sysuser
- [OLEDB ad hoc queries allowed: Registry access](#)
- Orphaned user: @@VERSION, <db name>.dbo.sysuser, master.dbo.sysdatabases, master.dbo.syslogins
- Password same as login name: @@VERSION
- Permission grantable: exec <db name>.dbo.sp_helprotect, master.dbo.sysdatabases
- Permissions granted to public: <db name>.dbo.sp_helprotect
- Permission on mswebtasks: exec <db name>.dbo.sp_helprotect, master.dbo.sysdatabases
- Permission on registry extended proc: exec <db name>.dbo.sp_helprotect, master.dbo.sysdatabases
- Permission on sp_MSsetalertinfo: exec <db name>.dbo.sp_helprotect, master.dbo.sysdatabases
- Permission on sp_MSSetServerProperties: exec <db name>.dbo.sp_helprotect, master.dbo.sysdatabases

- Permission on `sp_readwebtask`: `exec <db name>.dbo.sp_helprotect, master.dbo.sysdatabases`
- Permission on `sp_runwebtask`: `exec <db name>.dbo.sp_helprotect, master.dbo.sysdatabases`
- Permission on `xp_readerrorlog`: `exec <db name>.dbo.sp_helprotect, master.dbo.sysdatabases`
- Permission to select from `syslogins`: `exec <db name>.dbo.sp_helprotect, master.dbo.sysdatabases`
- Permission to select from system table: `<db name>.dbo.sysobjects, exec <db name>.dbo.sp_helprotect, master.dbo.sysdatabases`
- **Permissions granted on `sp_add_dtspackage`: `msdb.dbo.sysuser, exec msdb.dbo.sp_helprotect`**
- Permissions granted on `xp_cmdshell`: `@@VERSION, exec <db name>.dbo.sp_helprotect, master.dbo.sysdatabases`
- Permissions granted to user: `<db name>.dbo.sysuser, exec <db name>.dbo.sp_helprotect, master.dbo.sysdatabases`
- Public can create Agent jobs: `exec <db name>.dbo.sp_helprotect, master.dbo.sysdatabases`
- `pwdencrypt` buffer overflow: `@@VERSION`
- `RAISERROR` buffer overflow: `@@VERSION`
- Registry extended proc not removed: `<db name>.dbo.sysobjects, master.dbo.sysdatabases`
- Remote access allowed: `master.dbo.sysconfigures, master.dbo.syscurconfigs`
- Remote data source function unchecked buffer: `@@VERSION`
- Replication password publicly viewable: `xp_regread, sysobjects, @@version, sp_helprotect`
- Resolution service DoS: `@@VERSION`
- Resolution service heap overflow: `@@VERSION`
- Resolution service stack overflow: `@@VERSION`
- Reusable cached administrator connection: `@@VERSION`
- Service runs as LocalSystem: Windows Management Instrumentation (WMI) with Admin privileges.
- `sp_attachsubscription` command injection: `@@VERSION, <db name>.dbo.sysobjects, master.dbo.sysdatabases`
- `sp_MScopyscriptfile` command injection: `<db name>.dbo.sysobjects, master.dbo.sysdatabases, @@VERSION`
- SQL Agent password publicly viewable: `@@version, msdb.dbo.sp_get_sqlagent_properties, sp_helprotect`
- SQL Agent procedures granted to public: `sp_helprotect`
- SQLServerAgent password in registry: `@@VERSION, <db name>.dbo.sysobjects, master.dbo.sysdatabases`

- `srv_paraminfo` buffer overflow in `sp_OACreate`: @@VERSION
- `srv_paraminfo` buffer overflow in `sp_OADestroy`: @@VERSION
- `srv_paraminfo` buffer overflow in `sp_OAGetProperty`: @@VERSION
- `srv_paraminfo` buffer overflow in `sp_OAMethod`: @@VERSION
- `srv_paraminfo` buffer overflow in `sp_OASetProperty`: @@VERSION
- `srv_paraminfo` buffer overflow in `xp_displayparamstmt`: @@VERSION
- `srv_paraminfo` buffer overflow in `xp_execresultset`: @@VERSION
- `srv_paraminfo` buffer overflow in `xp_peekqueue`: @@VERSION
- `srv_paraminfo` buffer overflow in `xp_printstatements`: @@VERSION
- `srv_paraminfo` buffer overflow in `xp_proxiedmetadata`: @@VERSION
- `srv_paraminfo` buffer overflow in `xp_SetSQLSecurity`: @@VERSION
- `srv_paraminfo` buffer overflow in `xp_showcolv`: @@VERSION
- `srv_paraminfo` buffer overflow in `xp_sqlagent_monitor`: @@VERSION
- `srv_paraminfo` buffer overflow in `xp_sqlinventory`: @@VERSION
- `srv_paraminfo` buffer overflow in `xp_updatecolvbm`: @@VERSION
- Standard SQL Server authentication allowed: @@VERSION, <db name>.dbo.sysobjects, master.dbo.sysdatabases, master.dbo.xp_loginconfig
- Statement permission granted: master.dbo.sysdatabases, exec <db name>.dbo.sp_helpprotect
- SysAdmin only for CmdExec job steps: @@VERSION, <db name>.dbo.sysobjects, master.dbo.sysdatabases
- sysadmin role granted: master.dbo.syslogins
- Table to store DTS passwords publicly viewable: <db name>.dbo.sysuser, master.dbo.sysdatabases, exec <db name>.dbo.sp_helpprotect
- Temporary stored procedures bypass permissions: @@VERSION
- UDB broadcast buffer overflow: master.dbo.xp_cmdshell
- Unauthorized object permission grants: <db name>.dbo.sysuser, exec <db name>.dbo.sp_helpprotect, master.dbo.sysdatabases
- Windows account name shown as hostname: @@VERSION, master.dbo.xp_loginconfig
- XMLHTTP control allows local file access: <db name>.dbo.sysobjects, master.dbo.sysdatabases, @@VERSION
- `xp_cmdshell` not removed: <db name>.dbo.sysobjects, master.dbo.sysdatabases replace for `xp_cmdshell` not removed/not disabled: `select object_id()`
- `xp_controlqueueservice` buffer overflow: <db name>.dbo.sysobjects, master.dbo.sysdatabases
- `xp_createprivatequeue` buffer overflow: @@VERSION, <db name>.dbo.sysobjects, master.dbo.sysdatabases
- `xp_createqueue` buffer overflow: @@VERSION, master.dbo.sysdatabases, <db name>.dbo.sysobjects

- `xp_decodequeuecmd` buffer overflow: @@VERSION, <db name>.dbo.sysobjects, master.dbo.sysdatabases
- `xp_deleteprivatequeue` buffer overflow: @@VERSION, <db name>.dbo.sysobjects, master.dbo.sysdatabases
- `xp_deletequeue` buffer overflow: @@VERSION, <db name>.dbo.sysobjects, master.dbo.sysdatabases
- `xp_dirtree` buffer overflow: @@VERSION, <db name>.dbo.sysobjects, master.dbo.sysdatabases
- `xp_displayqueueemesgs` buffer overflow: @@VERSION, master.dbo.sysdatabases, <db name>.dbo.sysobjects
- `xp_dsninfo` buffer overflow: <db name>.dbo.sysobjects, @@VERSION, master.dbo.sysdatabases
- `xp_mergelineages` buffer overflow: @@VERSION, master.dbo.sysdatabases, <db name>.dbo.sysobjects
- `xp_oledbinfo` buffer overflow: @@VERSION, <db name>.dbo.sysobjects, master.dbo.sysdatabases
- `xp_proxiedmetadata` buffer overflow: master.dbo.sysdatabases, <db name>.dbo.sysobjects, @@VERSION
- `xp_readpkfromqueue` buffer overflow: @@VERSION, <db name>.dbo.sysobjects, master.dbo.sysdatabases
- `xp_readpkfromvarbin` buffer overflow: @@VERSION, <db name>.dbo.sysobjects, master.dbo.sysdatabases
- `xp_repl_encrypt` buffer overflow: @@VERSION, <db name>.dbo.sysobjects, master.dbo.sysdatabases
- `xp_resetqueue` buffer overflow: @@VERSION, <db name>.dbo.sysobjects, master.dbo.sysdatabases
- `xp_sprintf` buffer overflow: @@VERSION
- `xp_sqlagent_param` buffer overflow: @@VERSION, <db name>.dbo.sysobjects, master.dbo.sysdatabases
- `xp_sqlinventory` buffer overflow: @@VERSION, master.dbo.sysdatabases, <db name>.dbo.sysobjects
- `xp_unpackcab` buffer overflow: @@VERSION, <db name>.dbo.sysobjects, master.dbo.sysdatabases
- `xstatus` backdoor: @@VERSION, master.dbo.sysxlogins

RUNNING THE MICROSOFT SQL SERVER 2000 USER CREATION SCRIPT

Application Security Inc. has written a convenient Microsoft SQL Server 2000 user creation script ([CreateUserSQLServer2k.sql](#)) which creates an account with the minimum privileges necessary to perform Audits on a Microsoft SQL 2000 instance.

The contents of the `CreateUserSQLServer2k.sql` script follow:

```
set implicit_transactions off
set cursor_close_on_commit off

--create login
use [master]
EXEC sp_addlogin 'aduser', 'Admin123', 'master'
GO

--add user to each database
EXEC sp_MSforeachdb '
USE [?]
DECLARE @isUpdateable sql_variant

SELECT @isUpdateable = databasePropertyEx(name,'Updateability') FROM
master.dbo.sysdatabases where databasePropertyEx(name,'Status')='ONLINE' and name = '?'

IF @isUpdateable = 'READ_WRITE'
BEGIN
    EXEC sp_adduser 'aduser'
END'
GO

--assign privileges needed for audit
USE [master]
GO
GRANT EXECUTE ON dbo.xp_loginconfig TO [aduser]
GRANT SELECT ON dbo.syslogins TO [aduser]
GRANT SELECT ON dbo.sysxlogins TO [aduser]
GRANT SELECT ON dbo.sysaltfiles TO [aduser]
GRANT SELECT ON dbo.sysdatabases TO [aduser]
GRANT SELECT ON dbo.sysconfigures TO [aduser]
GRANT SELECT ON dbo.syscurconfigs TO [aduser]
GRANT SELECT ON dbo.sysservers TO [aduser]
```

```
GRANT SELECT ON dbo.sysmembers TO [aduser]
GRANT SELECT ON dbo.sysprotects TO [aduser]
GRANT SELECT ON dbo.spt_values TO [aduser]
GRANT EXECUTE ON sp_helpreplicationdboption TO [aduser]
GRANT EXECUTE ON sp_helpsrvrolemember TO [aduser]
GRANT EXECUTE ON sp_helprolemember TO [aduser]
GRANT SELECT ON dbo.sysoledbusers TO [aduser]

EXEC sp_MSforeachdb '
DECLARE @isUpdateable sql_variant

SELECT @isUpdateable = databasePropertyEx(name, 'Updateability') FROM mas-
ter.dbo.sysdatabases where databasePropertyEx(name, 'Status')='ONLINE' and name
= '?'

IF @isUpdateable = 'READ_WRITE'
BEGIN
    GRANT EXECUTE ON [?].dbo.sp_helpprotect TO [aduser]
    GRANT EXECUTE ON [?].dbo.sp_helpuser TO [aduser]
END
'

EXEC sp_MSforeachdb '
USE [?]

DECLARE @isUpdateable sql_variant

SELECT @isUpdateable = databasePropertyEx(name, 'Updateability') FROM mas-
ter.dbo.sysdatabases where databasePropertyEx(name, 'Status')='ONLINE' and name
= '?'

IF @isUpdateable = 'READ_WRITE'
BEGIN
    GRANT SELECT ON dbo.sysusers TO [aduser]
    GRANT SELECT ON dbo.sysobjects TO [aduser]
```

```

GRANT SELECT ON dbo.syscomments TO [aduser]
END
'
```

```

use [msdb]
GRANT SELECT ON dbo.sysjobs TO [aduser]
GRANT SELECT ON dbo.sysjobhistory TO [aduser]
```

```
print 'all done.'
```

RUNNING THE MICROSOFT SQL SERVER 2000 WITH SYSADMIN USER CREATION SCRIPT

Application Security Inc. has written a convenient Microsoft SQL Server 2000 user creation script ([CreateUserSQLServer2kwithSA.sql](#)) which creates an account with the minimum privileges necessary to perform Audits on a Microsoft SQL 2000 instance, and adds it to the SYSADMIN server role.

The contents of the [CreateUserSQLServer2kwithSA.sql](#) script follow:

```

USE master
GO
EXEC sp_addlogin 'aduser', 'Admin123'
GO

EXEC sp_MSforeachdb '
USE [?]
DECLARE @isUpdateable sql_variant

SELECT @isUpdateable =
databasePropertyEx(name, 'Updateability') FROM
master.dbo.sysdatabases where
databasePropertyEx(name, 'Status')='ONLINE' and name =
'?'

IF @isUpdateable = 'READ_WRITE'
BEGIN EXEC sp_grantdbaccess 'aduser', 'aduser'
END'
GO

EXEC sp_addsrvrolemember "aduser", SYSADMIN
```


MICROSOFT SQL SERVER 2005 AND MICROSOFT SQL SERVER 2008 AUDIT PRIVILEGES

Important!

Application Security Inc. wrote a convenient **Microsoft SQL Server 2005 and Microsoft SQL Server 2008 user creation script** ([CreateUserSQLServer2k52k8PublicRevoked.sql](#)) that creates an account with the minimum privileges necessary to perform an Audit on a Microsoft SQL Server instance. If you want to run this script, just make sure whatever account you use to conduct your Audit has at least the **SELECT** privileges listed in the script. For more information, see [Running the Microsoft SQL Server 2005 and 2008 User Creation Script](#).

Any Audit check for Microsoft SQL Server 2005 and Microsoft SQL Server 2008 queries the following views:

- `sys.databases`
- `sys.configurations`
- `sys.server_principals`
- `sys.server_role_members`

In Microsoft SQL Server 2005 and Microsoft SQL Server 2008 the public group can select from these views but, due to metadata visibility concept, AppDetectivePro may not return all records. For this reason, each of the checks listed below requires the following permissions in order to retrieve data: `VIEW DEFINITION`, `VIEW ANY DEFINITION`, and `CONTROL SERVER`.

In addition, you must have permission to select from `system table: select all rows from master.sys.database_permissions, <dbname>.sys.system_objects` views which implies `VIEW DEFINITION` on database scope permission.

For the check `Symmetric Keys: encrypting mechanism` to work properly, the auditing user should have access to all keys. The user must be a privileged user have been granted access to all the keys. You can use one of the following statements to grant access:

```
for every database
GRANT VIEW DEFINITION TO [aduser]
or
in master database
GRANT VIEW ANY DEFINITION TO [aduser]
```

In addition, certain Microsoft SQL Server 2005 and 2008 DISA-STIG Database Security Configuration checks require you to be a member of the `sysadmin` fixed server role or the `db_owner` fixed database role on the publication database. The following table provides specific information about which checks require which roles (and why):

Microsoft SQL Server 205 and 2008 DISA-STIG checks:	Use:	To run these checks, you must be a member of:
DBMS replication account privileges Replication snapshot folder protection	Replication system stored procedures.	The <code>sysadmin</code> fixed server role or the <code>db_owner</code> fixed database role on the publication database

Below is a list of AppDetectivePro checks used to run a Microsoft SQL Server 2005 or Microsoft SQL Server 2008 Audit, including the tables and views they need permission to access in order to function properly:

- `Agent XPs enabled`: `select from sys.configurations view.`
- `Application user access to external objects`: `select from <dbname>.sys.objects, <dbname>.sys.database_permissions.`
- `Asymmetric Keys: private key encryption type`: `select from master.dbo.sysdatabases, select from <dbname>.sys.asymmetric_keys, VIEW DEFINITION on database scope permission.`
- `Auditing of failed logins`: `master.dbo.xp_loginconfig.`
- `Auditing of failed/successful logins`: `execute xp_loginconfig.`
- `Audit trace status`: `select from fn_trace_getinfo, fn_trace_geteventinfo.`
- `Blank password checks`: `select password_hash column of sys.sql_logins for all sql logins which implies CONTROL SERVER permission.`
- `BUILTIN\Administrators not removed`: `select all rows from sys.server_principals view which implies VIEW ANY DEFINITION permission.`
- `C2 Audit Mode`: `select from sys.configurations view.`
- `CLR objects allowed`: `select from sys.configurations view.`
- `Common criteria compliance disabled`: `select from sys.configurations view.`

- Database job/batch queue monitoring: select from master.sys.procedures, select name, job_id columns from msdb.dbo.sysjobs and select job_id column from msdb.dbo.sysjobhistory.
- Database Master Key: access control: select from master.dbo.sysdatabases, <dbname>.sys.database_principals, <dbname>.sys.database_permissions.
- Database Master Key: encryption password: select from master.dbo.sysdatabases, <dbname>.sys.key_encryptions, <dbname>.sys.symmetric_keys, VIEW DEFINITION on database scope permission.
- Database Master Key: is_master_key_encrypted_by_server: select from sys.databases.
- Database Master Key: password storage: select from sys.master_key_passwords.
- Database ownership chaining not disabled: select from sys.configurations view.
- DBA OS privilege assignment: execute sp_helpsrvrolemember.
- DBMS account password expiration: select from sys.sql_logins.
- DBMS administration OS accounts: execute sp_helpsrvrolemember.
- DBMS audit log backups: select from fn_trace_getinfo.
- DBMS audit record access: select from sys.server_permissions, master.dbo.syslogins and master.dbo.sysusers, execute sp_helpsrvrolemember.
- DBMS Password Policy Enforced: execute xp_loginconfig, select from sys.sql_logins.
- DBMS remote system credential use and access: select from dbo.sysservers, sys.linked_logins.
- DBMS services dedicated custom account: Registry access.
- DBMS software file backups: Registry access.
- DBMS dedicated software directory and partition: Registry access.
- DBMS network port, protocol, and services (PPS) configuration: Registry access*.

Note:	To learn more about enabling registry access for Microsoft SQL Server 2005 and 2008, see Registry Access for Microsoft SQL Server 2000, 2005, and 2008.
--------------	---

- Dedicated data file directories: select from sys.master_files, sys.databases, Registry access*.
- Default password for well-known login: makes connection attempts.
- Default Trace Disabled: select from sys.configurations view.

- DTS package password publicly viewable: select all rows from msdb.sys.database_permissions, sys.types, sys.all_objects, sys.certificates, sys.fulltext_catalogs, sys.routes, sys.remote_service_bindings, sys.services, sys.service_contracts, sys.service_message_types, sys.xml_schema_collections, sys.assemblies views which implies VIEW DEFINITION on database scope permission.
- DTS package procedures granted to public: select from msdb.sys.database_permissions view.
- DTS procedures granted to PUBLIC: select from msdb.sys.database_principals, msdb.sys.database_permissions.
- Easily-guessed password checks: select password_hash column of sys.sql_logins for all sql logins which implies CONTROL SERVER permission.
- Encryption of DBMS sensitive data in transit: Registry access.
- Error logs can be overwritten: Registry access.
- Event forwarding not disabled: Registry access.
- Fixed server role granted: select all rows from sys.server_principals, sys.server_role_members views which implies VIEW ANY DEFINITION permission.
- Global temporary stored proc exists: select from tempdb.sys.all_objects.
- Guest user exists in database: select all rows from sys.databases and <dbname>.sys.database_principals, and <dbname>.sys.database_permissions views.
- Integration Services OS account least privileges: Windows Management Instrumentation (WMI).
- Latest service pack/hot fix not applied: uses @@version - requires no privileges.
- Linked Servers Definitions: select from sys.servers view. Permissions granted on sp_add_dtspackage: select all rows from msdb.sys.database_permissions, sys.types, sys.all_objects, sys.certificates, sys.fulltext_catalogs, sys.routes, sys.remote_service_bindings, sys.services, sys.service_contracts, sys.service_message_types, sys.xml_schema_collections, sys.assemblies views which implies VIEW DEFINITION on database scope permission.
- Lumigent Log Explorer buffer overflow: select all rows from master.sys.objects view which implies VIEW DEFINITION on master database permission.
- Not using NTFS partition: execute xp_instance_regread.
- OLEDB ad hoc queries allowed: select from sys.configurations view, Registry access.

- Password same as login name: select password_hash column of sys.sql_logins view for all sql logins which implies CONTROL SERVER permission.
- Permission grantable: select all rows from sys.databases, <dbname>.sys.database_permissions views which implies VIEW DEFINITION on database scope permission.
- Permission on OLE automation procs: select all rows from master.sys.database_permissions view which implies VIEW DEFINITION on database scope permission.
- Permission on registry extended proc: select all rows from master.sys.database_permissions view which implies VIEW DEFINITION on database scope permission.
- Permission to select from system table: select all rows from master.sys.database_permissions view which implies VIEW DEFINITION on database scope permission.
- Permissions granted on xp_cmdshell: select all rows from master.sys.database_permissions view which implies VIEW DEFINITION on database scope permission.
- Permissions granted to PUBLIC: select all rows from sys.databases, <dbname>.sys.database_permissions views.
- Permissions granted to user: select all rows from sys.databases, <dbname>.sys.database_permissions, sys.types, sys.all_objects, sys.certificates, sys.fulltext_catalogs, sys.routes, sys.remote_service_bindings, sys.services, sys.service_contracts, sys.service_message_types, sys.xml_schema_collections, sys.assemblies views which implies VIEW DEFINITION on database scope permission.
- Permissions on files: execute xp_instance_regread.
- Protection of DBMS asymmetric encryption keys: select from master.dbo.sysdatabases, <dbname>.sys.asymmetric_keys, <dbname>.sys.database_principals, <dbname>.sys.database_permissions, VIEW DEFINITION on database scope permission.
- Proxy account subsystem privileges: select subsystem, subsystem_id columns from msdb.dbo.syssubsystems.
- Registry extended proc not removed: select from master.sys.system_objects view.
- Registry permissions: execute xp_instance_regread.
- Remote access allowed: select from sys.configurations view.
- Remote admin connections allowed: select from sys.configurations view.
- Replication filters: member of the sysadmin fixed server role or the db_owner fixed database role on the publication database.
- Replication filters not employed: member of the sysadmin fixed server role or the db_owner fixed database role on the publication database.

- Sample database not removed: select all rows from sys.databases view.
- Service Broker Endpoints exist: select from sys.service_broker_endpoints.
- Service runs as LocalSystem: Windows Management Instrumentation (WMI) with Admin privileges.
- SMO and DMO XPs enabled: select from sys.configurations view.
- SQL Server Agent account user rights: Windows Management Instrumentation (WMI).
- SQL Server Agent proxy accounts are not dedicated: execute sp_enum_login_for_proxy.
- SQL Server component service account user rights: Windows Management Instrumentation (WMI).
- SQL Server file permissions: Registry access*, OS access (Permission to read files in the installation directory of the database) also Windows Management Instrumentation (WMI).
- SQL Server service account: Windows Management Instrumentation (WMI).
- SQL Server service account user rights: Windows Management Instrumentation (WMI).
- Standard SQL Server authentication allowed: execute xp_instance_regread.
- Statement permission granted: select all rows from sys.databases, <dbname>.sys.database_permissions views which implies VIEW DEFINITION on database scope permission.
- Symmetric Keys: allowed encryption algorithms: select from master.dbo.sysdatabases, <dbname>.sys.symmetric_keys, VIEW DEFINITION on database scope permission.
- Symmetric Keys: encrypting mechanism: select from master.dbo.sysdatabases, <dbname>.sys.symmetric_keys, <dbname>.sys.key_encryptions, VIEW DEFINITION on database scope permission.
- sysadmin role granted: select all rows from sys.server_principals, sys.server_role_members views which implies VIEW ANY DEFINITION permission.
- Unauthorized object permission grants: select all rows from sys.databases, <dbname>.sys.database_permissions, sys.types, sys.all_objects, sys.certificates, sys.fulltext_catalogs, sys.routes, sys.remote_service_bindings, sys.services, sys.service_contracts, sys.service_message_types, sys.xml_schema_collections, sys.assemblies views which implies VIEW DEFINITION on database scope permission.
- XML web service access: select from sys.http_endpoints.
- Web assistant procedures enabled: select from sys.configurations view.

- `xp_cmdshell` not removed/not disabled: `select from sys.configurations view.`

CREDENTIALS FOR MICROSOFT SQL SERVER AUDITS

If you are unable to Audit a Microsoft SQL Server database using Windows Authentication, you may be using an account that lacks the proper credentials. There are a number of different ways to supply the proper credentials for Microsoft SQL Server. The appropriate method depends on your circumstances.

The following table explains how to change your credentials under different scenarios when you attempt to perform an Audit on the Microsoft SQL Server `TARGET` machine from another machine (`HOST`). Once you have valid credentials on the target `HOST`, you should be able to perform your Audit.

Part	If	Then
1	<code>TARGET</code> and <code>HOST</code> are in the same or trusted domain.	<ul style="list-style-type: none"> • If you are logged in to <code>HOST</code> as a user that has Administrative access to <code>TARGET</code>, you do not need to supply additional credentials. <p>Or...</p> <ul style="list-style-type: none"> • If you are logged in as user without Administrative access, you will need to supply <code>TARGET</code>'s <code>sa</code> credentials.

Part	If	Then
2	<p>TARGET is in WORKGROUP_X and HOST is in DOMAIN_A</p> <p>Or...</p> <p>TARGET is in WORKGROUP_X and HOST is in WORKGROUP_Y</p> <p>Or...</p> <p>TARGET is in WORKGROUP_X and HOST is in WORKGROUP_X</p>	<ul style="list-style-type: none"> • You can supply sa credentials in AppDetectivePro. <p>Or...</p> <ul style="list-style-type: none"> • You can create a local user on TARGET and a local user on HOST with matching user names and passwords. You cannot use Domain names here. <p>Or...</p> <ul style="list-style-type: none"> • Select the Properties branch option Connect to Microsoft SQL Servers via Named Pipes in the AppDetectivePro Properties branch, then use the Net Use technique to establish credentials on TARGET. You must select this option to force AppDetectivePro to use named pipes. You must check this option if you want to Audit a Microsoft SQL Server database (using Windows Authentication) against a machine on a different or untrusted domain. Additional steps are required. For more information, see <i>Auditing Microsoft SQL Server (Using Windows Authentication) Against a Machine on a Different or Untrusted Domain</i>. <p>To use the Net Use technique:</p> <ul style="list-style-type: none"> -Open a command prompt. -Enter the <code>net use</code> command to log in to the target server with valid credentials. -The command should adhere to the following format: <code>net use \\computerIP / user:[domainname\]username</code> -AppDetectivePro prompts you for a valid password on the TARGET. -Verify access by re-entering <code>net use</code>. <p>AppDetectivePro does not support Pen Testing any Microsoft SQL Server instances which use named pipes for connection.</p>

Part	If	Then
3	TARGET is in DOMAIN_A and HOST is either in an untrusted DOMAIN_B or in WORKGROUP_X	<ul style="list-style-type: none"> • You can use any of the methods listed in Part 2, above. Or... • You can add HOST to DOMAIN_A.

RUNNING THE MICROSOFT SQL SERVER 2005 AND 2008 USER CREATION SCRIPT

Application Security Inc. has written a convenient Microsoft SQL Server 2005 and Microsoft SQL Server 2008 user creation script ([CreateUserSQLServer2k52k8PublicRevoked.sql](#)) which creates an account with the minimum privileges necessary to perform Audits on either a Microsoft SQL Server 2005 or a Microsoft SQL Server 2008 instance.

Caution! If you want to run this script, make sure whatever account you use to conduct your Audit has at least the [SELECT](#) privileges listed in the script (see below).

The contents of the [CreateUserSQLServer2k52k8PublicRevoked.sql](#) script follow:

```
CREATE LOGIN [aduser] WITH PASSWORD=N'Admin123', DEFAULT_DATABASE=[master]
GO

EXEC sp_MSforeachdb '
USE [?]
DECLARE @isUpdateable sql_variant

SELECT @isUpdateable = databasePropertyEx(name,"Updateability") FROM
master.dbo.sysdatabases where databasePropertyEx(name,"Status")="ONLINE"
and name = "?"

IF @isUpdateable = "READ_WRITE"
BEGIN
    CREATE USER [aduser] FOR LOGIN [aduser] WITH DEFAULT_SCHEMA=[dbo]
END'
```

GO

USE [master]

GO

GRANT EXECUTE ON dbo.xp_loginconfig TO [aduser]

GRANT SELECT ON dbo.syslogins TO [aduser]

GRANT SELECT ON dbo.sysdatabases TO [aduser]

GRANT SELECT ON dbo.sysconfigures TO [aduser]

GRANT SELECT ON dbo.syscurconfigs TO [aduser]

GRANT SELECT ON dbo.syscharsets TO [aduser]

GRANT SELECT ON sys.configurations TO [aduser]

GRANT SELECT ON sys.server_principals TO [aduser]

GRANT SELECT ON sys.server_role_members TO [aduser]

GRANT ALTER TRACE TO [aduser]

GRANT SELECT ON sys.fn_trace_getinfo TO [aduser]

EXEC sp_MSforeachdb '

DECLARE @isUpdateable sql_variant

SELECT @isUpdateable = databasePropertyEx(name,"Updateability") FROM
master.dbo.sysdatabases where databasePropertyEx(name,"Status")="ONLINE"
and name = "?"

IF @isUpdateable = "READ_WRITE"

BEGIN

GRANT EXECUTE ON [?].dbo.sp_helprotect TO [aduser]

END'

GRANT SELECT ON sys.servers TO [aduser]

GRANT EXECUTE ON dbo.sp_helpsrvrolemember TO [aduser]

```
GRANT SELECT ON dbo.fn_trace_geteventinfo TO [aduser]
GRANT SELECT ON dbo.fn_trace_getinfo TO [aduser]
GRANT SELECT ON sys.databases TO [aduser]
GRANT SELECT ON sys.master_key_passwords TO [aduser]
GRANT SELECT ON sys.sql_logins TO [aduser]
GRANT SELECT ON sys.master_files TO [aduser]
GRANT SELECT ON sys.procedures TO [aduser]
GRANT SELECT ON sys.server_permissions TO [aduser]
GRANT SELECT ON sys.all_objects TO [aduser]
GRANT SELECT ON sys.certificates TO [aduser]
GRANT SELECT ON sys.fulltext_catalogs TO [aduser]
GRANT SELECT ON sys.routes TO [aduser]
GRANT SELECT ON sys.remote_service_bindings TO [aduser]
GRANT SELECT ON sys.services TO [aduser]
GRANT SELECT ON sys.service_contracts TO [aduser]
GRANT SELECT ON sys.service_message_types TO [aduser]
GRANT SELECT ON sys.xml_schema_collections TO [aduser]
GRANT SELECT ON sys.assemblies TO [aduser]
GRANT SELECT ON sys.http_endpoints TO [aduser]
GRANT SELECT ON dbo.sysservers TO [aduser]
GRANT SELECT ON dbo.sysservers TO [aduser]
GRANT SELECT ON sys.linked_logins TO [aduser]
GRANT SELECT ON sys.service_broker_endpoints TO [aduser]
GRANT SELECT ON sys.credentials TO [aduser]
GRANT EXECUTE ON dbo.sp_helppublication TO [aduser]
GRANT EXECUTE ON dbo.sp_helpmergepublication TO [aduser]
GRANT EXECUTE ON dbo.sp_helpmergesubscription TO [aduser]
GRANT EXECUTE ON dbo.sp_helpsubscription TO [aduser]
GRANT EXECUTE ON dbo.sp_help_publication_access TO [aduser]
GRANT EXECUTE ON dbo.sp_helpuser TO [aduser]
GRANT SELECT ON sys.dm_os_cluster_nodes TO [aduser]
```

```
GRANT SELECT ON sys.database_files TO [aduser]
GRANT EXECUTE ON dbo.sp_helpreplicationdboption TO [aduser]
GRANT EXECUTE ON dbo.sp_helprolemember TO [aduser]
GRANT SELECT ON dbo.sysprocesses TO [aduser]
grant view any definition to [aduser]
GRANT VIEW SERVER STATE TO [aduser]
GO

USE [msdb]
GO
GRANT EXECUTE ON dbo.sp_get_sqlagent_properties TO [aduser]
GRANT SELECT ON dbo.sysproxysubsystem TO [aduser]
GRANT SELECT ON dbo.sysproxies TO [aduser]
GRANT EXECUTE ON dbo.sp_enum_login_for_proxy TO [aduser]
GRANT SELECT ON dbo.sysjobs ([name],[job_id]) TO [aduser]
GRANT SELECT ON dbo.sysjobhistory ([job_id]) TO [aduser]
GRANT SELECT ON dbo.syssubsystems ([subsystem],[subsystem_id]) TO [aduser]
GRANT SELECT ON [dbo].[sysjobsteps] ([proxy_id],[subsystem],[job_id]) TO
[aduser]
GRANT SELECT ON dbo.sysjobs TO [aduser]
GO

EXEC sp_MSforeachdb '
USE [?]
DECLARE @isUpdateable sql_variant
SELECT @isUpdateable = databasePropertyEx(name,"Updateability") FROM
master.dbo.sysdatabases where databasePropertyEx(name,"Status")="ONLINE"
and name = "?"
```

```
IF @isUpdateable = "READ_WRITE"  
BEGIN  
GRANT SELECT ON dbo.sysusers TO [aduser]  
GRANT SELECT ON dbo.sysobjects TO [aduser]  
GRANT SELECT ON dbo.syscomments TO [aduser]  
GRANT VIEW DEFINITION TO [aduser]  
GRANT SELECT ON sys.database_permissions TO [aduser]  
GRANT SELECT ON sys.objects TO [aduser]  
GRANT SELECT ON sys.asymmetric_keys TO [aduser]  
GRANT SELECT ON sys.database_principals TO [aduser]  
GRANT SELECT ON sys.key_encryptions TO [aduser]  
GRANT SELECT ON sys.symmetric_keys TO [aduser]  
GRANT SELECT ON sys.types TO [aduser]  
GRANT SELECT ON sys.systemmembers TO [aduser]  
GRANT SELECT ON sys.database_role_members TO [aduser]  
GRANT SELECT ON sys.schemas TO [aduser]  
GRANT SELECT ON sys.system_objects TO [aduser]  
END '  
GO
```

REGISTRY ACCESS FOR MICROSOFT SQL SERVER 2000, 2005, AND 2008

Some Microsoft SQL Server 2000, 2005, and 2008 Audit privileges require you to have remote registry access in order to perform Audits on Microsoft SQL Server instances. These required Audit privileges are listed in:

- Microsoft SQL Server 2000 and MSDE Audit Privileges (for all applicable **Microsoft SQL Server 2000** Audit privileges)
- Microsoft SQL Server 2005 and Microsoft SQL Server 2008 Audit Privileges (for all applicable **Microsoft SQL Server 2005 and 2008** Audit privileges).

Depending on your version of Microsoft SQL Server 2000, 2005, and 2008 (and whether you are using Microsoft SQL Server Authentication or Windows Authentication), you can get the remote registry value in either of the following two ways:

1. Via the `xp_regread` extended stored procedure (explained in the following table).

If your version of Microsoft SQL Server is:	And you are using:	Detail
Microsoft SQL Server 2000 (service pack prior to SP4)	Microsoft SQL Server Authentication Windows Authentication	Grant <code>execute</code> on <code>xp_regread</code> to the AppDetectivePro user or the <code>Public</code> role. Grant <code>execute</code> on <code>xp_regread</code> to the Windows user or to the <code>Public</code> role, and permissions on the key being accessed.

If your version of Microsoft SQL Server is:	And you are using:	Detail
Microsoft SQL Server 2000 SP4 and Microsoft SQL Server 2005 or 2008	Microsoft SQL Server Authentication Windows Authentication	Grant <code>execute</code> on <code>xp_regread</code> to the AppDetectivePro user or the <code>Public</code> role. Grant <code>execute</code> on <code>xp_regread</code> to Windows user or the <code>Public</code> role, and permissions on the key being accessed.
	Microsoft SQL Server Authentication or Windows Authentication	<p>Although authentication mode (i.e., Microsoft SQL Server Authentication or Windows Authentication) is used, AppDetectivePro requires an entry on the target <code>(HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft SQL Server\<INSTANCE>\MSSQLServer\ExtendedProcedures\Xp_regread Allowed Paths)</code> of the requested registry subkey. (Reference: http://support.microsoft.com/kb/887165)</p> <p>Since the Microsoft SQL Server installation program pre-populates the <code>Xp_regread Allowed Paths</code> registry entry with the extended stored procedures that Microsoft SQL Server can access, you only need to add the following registry entries:</p> <ul style="list-style-type: none"> • <code>HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft SQL Server\Instance Names\SQL</code> • <code>HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSSQLServerOLAPService</code> • <code>HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ReportServer</code>

2. Get the remote registry value via the Windows Remote Registry API, and provide a valid Windows account with remote registry access.

MySQL Audit Privileges

Note: For more information on MySQL Server OS check requirements, see Operating System Considerations (for Audits).

To conduct a full MySQL Audit, you need the following privileges. Make sure the account you are using has rights to use the following tables and views:

- Anonymous user exists: SELECT on user table
- Blank account passwords: SELECT on user table
- Blank root password: SELECT on user table
- Default passwords for test accounts: SELECT on user table
- Easily-guessed account passwords: SELECT on user table
- Easily-guessed root password: SELECT on user table
- FILE privileges granted: SELECT on user table
- General log file not enabled: execute SHOW VARIABLES
- Password for user same as username: SELECT on user table
- Permissions grantable: SELECT on the user table, SELECT on the db table, SELECT on the host table, SELECT on the tables_priv table, and SELECT on the procs_priv table
- Permissions on GRANT tables: SELECT on the user table, SELECT on the db table, SELECT on the host table, SELECT on the tables_priv table, SELECT on the procs_priv table, and SELECT on the columns_priv' table
- Permissions on user table: SELECT on the user table, SELECT on the db table, SELECT on the host table, SELECT on the tables_priv table, and SELECT on the columns_priv table.
- PROCESS privileges granted: SELECT on user table
- Sample database not removed: execute SHOW DATABASES
- SSL encryption not enabled: execute SHOW VARIABLES
- Grant SELECT on procs_priv

The Grant SELECT on procs_priv privilege is only required on the Permissions on GRANT tables and Permissions grantable MySQL Audit checks on MySQL 5.0 and greater.

MYSQL CHECKS

MySQL Audit

- Easily-guessed root password
- Easily-guessed passwords
- Blank password
- Blank root password
- Universal access
- SSL is enabled
- Grant tables privileges
- Ensure sample databases have been removed
- Permissions on [User] table
- Permissions granted directly to user
- Logging not enabled
- MySQL mysqld Privilege Escalation Vulnerability
- MySQL libmysqlclient Library Read_One_Row Buffer Overflow Vulnerability
- MySQL COM_CHANGE_USER Password Memory Corruption Vulnerability
- MySQL Double Free Heap Corruption Vulnerability
- MySQL COM_CHANGE_USER Password Length Account Compromise Vulnerability
- MySQL libmysqlclient Library Read_Rows Buffer Overflow Vulnerability
- MySQL COM_TABLE_DUMP Memory Corruption Vulnerability
- MySQL COM_TABLE_DUMP Memory Corruption Vulnerability
- MySQL Bind Address Not Enabled Weak Default Configuration Vulnerability
- MySQL Null Root Password Weak Default Configuration Vulnerability
- WinMySQLadmin Plain Text Password Storage Vulnerability
- MySQL Root Operation Symbolic Link File Overwriting Vulnerability
- MySQL SHOW GRANTS Password Hash Disclosure Vulnerability
- MySQL Local Buffer Overflow Vulnerability
- MySQL Authentication Algorithm Vulnerability
- MySQL GRANT Global Password Changing Vulnerability
- MySQL Unauthenticated Remote Access Vulnerability
- [Permissions on GRANT tables](#)
- [Permissions grantable](#)

The Grant SELECT on procs_priv privilege is only required on the Permissions on GRANT tables and Permissions grantable MySQL Audit checks on MySQL 5.0 and greater.

MySQL Pen Test

- Easily-guessed root password
- Easily-guessed password
- Blank password
- Blank root password
- MySQL mysqld Privilege Escalation Vulnerability
- MySQL libmysqlclient Library Read_One_Row Buffer Overflow Vulnerability
- MySQL COM_CHANGE_USER Password Memory Corruption Vulnerability
- MySQL Double Free Heap Corruption Vulnerability
- MySQL COM_CHANGE_USER Password Length Account Compromise Vulnerability
- MySQL libmysqlclient Library Read_Rows Buffer Overflow Vulnerability
- MySQL COM_TABLE_DUMP Memory Corruption Vulnerability
- MySQL COM_TABLE_DUMP Memory Corruption Vulnerability
- MySQL Bind Address Not Enabled Weak Default Configuration Vulnerability
- MySQL Null Root Password Weak Default Configuration Vulnerability
- WinMySQLadmin Plain Text Password Storage Vulnerability
- MySQL Root Operation Symbolic Link File Overwriting Vulnerability
- MySQL SHOW GRANTS Password Hash Disclosure Vulnerability
- MySQL Local Buffer Overflow Vulnerability
- MySQL Authentication Algorithm Vulnerability
- MySQL GRANT Global Password Changing VulnerabilityMySQL
- MySQL Unauthenticated Remote Access Vulnerability

Oracle Audit Privileges and User Creation Script

Note: For more information on Oracle OS check requirements, see Operating System Considerations (for Audits) and Appendix O: Oracle Critical Patch Update Detection.

This section consists of the following topics:

- [Oracle Audit Privileges](#)
- [Running the Oracle User Creation Script](#)

ORACLE AUDIT PRIVILEGES

To conduct a full Oracle Audit, you need the following privileges. Make sure the account you are using has rights to use the following tables, views, and functions:

- `$PWFIL``_USERS`
- `ALTER USER username TEMPORARY TABLESPACE TEMP`
- `DBA_OBJ_AUDIT_OPTS`
- `DBA_OBJECTS`
- `DBA_PROFILES`
- `DBA_ROLES`
- `DBA_ROLE_PRIVS`
- `DBA_STMT_AUDIT_OPTS`
- `DBA_SYS_PRIVS`
- `DBA_TABLES`
- `DBA_TAB_PRIVS`
- `DBA_USERS`
- `DBA_VIEWS`
- `DBMS_UTILITY.PORT_STRING`
- `PRODUCT_COMPONENT_VERSION`
- `SYS.LINK$`
- `SYS.USER$`
- `SYS.REGISTRY$HISTORY`
- `SYS.DBA_DB_LINKS`
- `SYS.DBA_LIBRARIES`
- `SYS.DBA_OBJECTS`
- `SYS.DBA_ROLE_PRIVS`

- `SYS.DBA_SOURCE`
- `SYS.DBA_USERS`
- `SYS.DBA_DB_LINKS`
- `SYS.V_$INSTANCE`
- `SYS.DBA_TS_QUOTAS`
- `V$LOG`
- `V$PWFILE_USERS`
- `V$VERSION`
- `V_$DATABASE`
- `V_$DATAFILE`
- `V_$LOGFILE`
- `V_$SESSION`
- `V_$PARAMETER` (AppDetectivePro selects from `V$PARAMETER` but you must grant `SELECT` on `V_$PARAMETER`)

Note:	The user account must have the <code>CREATE SESSION</code> privilege. In addition, the user account used for Audits needs a temporary table space assigned, which you can create with the following command: <code>ALTER USER user-name TEMPORARY TABLESPACE TEMP</code>
--------------	--

The following is a list of checks within the AppDetectivePro for Oracle Security Audit, and the tables and views to which they must have permission in order to function properly:

- `_TRACE_FILES_PUBLIC` undocumented configuration parameter is NOT set to `FALSE` (Note that this check must have `sysdba` privileges.)
- Account associated with `DEFAULT` profile: `DBA_USERS`
- Account granted the predefined role `CONNECT`: `DBA_ROLE_PRIVS`
- Account granted the predefined role `DBA`: `DBA_ROLE_PRIVS`
- Account granted the predefined role `RESOURCE`: `DBA_ROLE_PRIVS`
- Accounts with `SYSTEM` as default tablespace: `DBA_USERS`
- `ANSI` join syntax bypasses object privileges: `PRODUCT_COMPONENT_VERSION`
- ANY system privilege applies to data dictionary: `V$PARAMETER`
- Auditing Not Enabled: `V$PARAMETER`
- Auditing of `CREATE SESSION` not enabled: `DBA_STMT_AUDIT_OPTS`
- `BFILENAME` buffer overflow (Verify version): `PRODUCT_COMPONENT_VERSION`
- Brute-force database password: `DBA_USERS`
- Brute-force role password: `SYS.USER$`

- Cleartext password stored with database link: SYS.LINK\$
- Create library privilege: DBA_SYS_PRIVS, PRODUCT_COMPONENT_VERSION
- Database link buffer overflow (Verify version):PRODUCT_COMPONENT_VERSION
- Database user allows remote authentication: DBA_USERS, V\$PARAMETER
- DBLINK_ENCRYPT_LOGIN not enabled: SYS.LINK\$, V\$PARAMETER
- DBMS data files are not dedicated to support individual applications: SELECT permission for views SYS.DBA_DATA_FILES, SYS.DBA_INDEXES
- DBMS dedicated software directory and partition: V\$DATAFILE, V\$LOGFILE, V\$PARAMETER
- Default database password: DBA_USERS
- Easily-guessed database password: DBA_USERS
- Easily-guessed role password: SYS.USER\$
- Expired password: DBA_USERS, PRODUCT_COMPONENT_VERSION
- Kick Listener DoS (Verify version): PRODUCT_COMPONENT_VERSION
- Label Security row label improperly assigned: PRODUCT_COMPONENT_VERSION
- Label Security SQL predicates bypassed: PRODUCT_COMPONENT_VERSION
- Label Security unauthorized higher level read: PRODUCT_COMPONENT_VERSION
- Listener debug DoS (Verify version): PRODUCT_COMPONENT_VERSION
- Listener format string buffer overflow (Verify version): PRODUCT_COMPONENT_VERSION
- Locked account: DBA_USERS, PRODUCT_COMPONENT_VERSION
- MTDS DoS (Verify version): PRODUCT_COMPONENT_VERSION
- NERP DoS (Verify version): PRODUCT_COMPONENT_VERSION
- Non-standard account with DBA role: DBA_ROLE_PRIVS
- NSPTCN buffer overflow (Verify version): PRODUCT_COMPONENT_VERSION
- NSPTCN data offset DoS (Verify version): PRODUCT_COMPONENT_VERSION
- Object privilege grantable: DBA_TAB_PRIVS
- Object privilege granted to account: DBA_TAB_PRIVS, DBA_USERS
- Object privilege granted to PUBLIC: DBA_TAB_PRIVS
- Oracle Configuration Manager: DBA_USERS
- Oracle DIAGNOSTIC_DEST parameter: V\$PARAMETER
- Oracle file overwrite: PRODUCT_COMPONENT_VERSION
- Oracle LOG_ARCHIVE_DEST parameter: V\$DATABASE, V\$PARAMETER
- OS authentication prefix: V\$PARAMETER

- Overdue password change: sys.user\$
- Password for database user same as username: DBA_USERS
- Privilege granted to SELECT from data dictionary: DBA_TABLES, DBA_TAB_PRIVS
- Privilege on audit trail table: DBA_TAB_PRIVS
- Privilege on database link table: DBA_TAB_PRIVS, DBA_USERS
- Privilege to execute UTL_FILE granted to PUBLIC: DBA_TAB_PRIVS
- Privilege to execute UTL_HTTP granted to PUBLIC: DBA_TAB_PRIVS
- Privilege to execute UTL_SMTP granted to PUBLIC: DBA_TAB_PRIVS
- Privilege to execute UTL_TCP granted to PUBLIC: DBA_TAB_PRIVS
- Profile settings - Failed Login Attempts: DBA_PROFILES, PRODUCT_COMPONENT_VERSION
- Profile settings - Password Grace Time: DBA_PROFILES, PRODUCT_COMPONENT_VERSION
- Profile settings - Password Life Time: DBA_PROFILES, PRODUCT_COMPONENT_VERSION
- Profile settings - Password Lock Time: DBA_PROFILES, PRODUCT_COMPONENT_VERSION
- Profile settings - Password Reuse Maximum: DBA_PROFILES, PRODUCT_COMPONENT_VERSION
- Profile settings - Password Reuse Time: DBA_PROFILES, PRODUCT_COMPONENT_VERSION
- Profile settings - Password Verify Function: DBA_PROFILES, PRODUCT_COMPONENT_VERSION
- Remote login password file not disabled: V\$PARAMETER
- Remote OS Authentication enabled: V\$PARAMETER
- Remote OS Roles enabled: V\$PARAMETER
- Requestor version DoS (Verify version): PRODUCT_COMPONENT_VERSION
- Role without password: DBA_ROLES
- Roles granted WITH ADMIN OPTION: DBA_ROLE_PRIVS
- SERVICE_CURLOAD DoS (Verify version): PRODUCT_COMPONENT_VERSION
- SERVICE_NAME buffer overflow (Verify version): PRODUCT_COMPONENT_VERSION
- Service runs as LocalSystem: Windows Management Instrumentation (WMI) with Admin privileges (Windows ONLY).
- SNMP DoS (Verify version): PRODUCT_COMPONENT_VERSION
- SQL92_SECURITY parameter not enabled: V\$PARAMETER

- SYSDBA auditing bug: `PRODUCT_COMPONENT_VERSION`
- [SYSDBA privilege assignments](#)
- System privilege granted to account: `DBA_SYS_PRIVS, DBA_USERS`
- System privilege granted to PUBLIC: `DBA_SYS_PRIVS`
- System privilege granted WITH ADMIN OPTION: `DBA_SYS_PRIVS`
- System privilege with ANY clause: `DBA_SYS_PRIVS`
- TCL debugger installs with setUID root: `DBA_SYS_PRIVS`
- TCL debugger installs with setUID root: `PRODUCT_COMPONENT_VERSION`
- `TO_TIMESTAMP_TZ` buffer overflow (Verify version):`PRODUCT_COMPONENT_VERSION`
- `TZ_OFFSET` buffer overflow (Verify version):`PRODUCT_COMPONENT_VERSION`
- Trace reporting buffer overflow: `PRODUCT_COMPONENT_VERSION`
- `UTL_FILE_DIR` unrestricted: `V$PARAMETER`
- XSQL Servlet stylesheet as URL parameter: `PRODUCT_COMPONENT_VERSION`
- Auditing of Schema Objects: `DBA_OBJ_AUDIT_OPTS, DBA_VIEWS`
- `PITRIG_DROPMETADATA` Buffer Overflow: `DBA_PROCEDURES` and Oracle Critical Patch Update Detection requirements (see Appendix O: Oracle Critical Patch Update Detection)
- Object ownership: `DBA_OBJECTS, DBA_ROLE_PRIVS`
- Application user role privileges: `DBA_TAB_PRIVS, DBA_ROLE_PRIVS, DBA_OBJECTS`

RUNNING THE ORACLE USER CREATION SCRIPT

Application Security Inc. has written a convenient Oracle user creation script ([CreateUserOracle.sql](#)) which creates an account with the minimum privileges necessary to perform Audits on an Oracle instance.

The contents of the [CreateUserOracle.sql](#) script follow:

```
DROP USER aduser cascade;
CREATE USER aduser IDENTIFIED BY AD123;
GRANT SELECT ON SYS.DBA_DB_LINKS TO aduser;
GRANT SELECT ON SYS.DBA_DATA_FILES TO aduser;
GRANT SELECT ON SYS.DBA_OBJECTS TO aduser;
GRANT SELECT ON SYS.DBA_OBJ_AUDIT_OPTS TO aduser;
GRANT SELECT ON SYS.DBA_PROCEDURES TO aduser;
GRANT SELECT ON SYS.DBA_PROFILES TO aduser;
```

```
GRANT SELECT ON SYS.DBA_ROLES TO aduser;
GRANT SELECT ON SYS.DBA_ROLE_PRIVS TO aduser;
GRANT SELECT ON SYS.DBA_STMT_AUDIT_OPTS TO aduser;
GRANT SELECT ON SYS.DBA_SYS_PRIVS TO aduser;
GRANT SELECT ON SYS.DBA_TABLES TO aduser;
GRANT SELECT ON SYS.DBA_INDEXES TO aduser;
GRANT SELECT ON SYS.DBA_TAB_PRIVS TO aduser;
GRANT SELECT ON SYS.DBA_TS_QUOTAS TO aduser;
GRANT SELECT ON SYS.DBA_USERS TO aduser;
GRANT SELECT ON SYS.DBA_SOURCE TO aduser;
GRANT SELECT ON SYS.DBA_VIEWS TO aduser;
GRANT SELECT ON SYS.PRODUCT_COMPONENT_VERSION TO aduser;
GRANT SELECT ON SYS.LINK$ TO aduser;
GRANT SELECT ON SYS.USER$ TO aduser;
GRANT SELECT ON SYS.V_$PARAMETER TO aduser;
GRANT SELECT ON SYS.V_$LOG TO aduser;
GRANT SELECT ON SYS.V_$PWFILERS TO aduser;
GRANT SELECT ON SYS.V_$INSTANCE TO aduser;
GRANT SELECT ON SYS.V_$DATABASE TO aduser;
GRANT SELECT ON SYS.DBA_PRIV_AUDIT_OPTS TO aduser;
GRANT SELECT ON SYS.DBA_REPCATLOG TO aduser;
GRANT SELECT ON SYS.DEFPROPAGATOR TO aduser;
GRANT SELECT ON SYS.V_$DATAFILE TO aduser;
GRANT SELECT ON SYS.V_$LOGFILE TO aduser;
GRANT SELECT ON SYS.V_$SESSION TO aduser;

GRANT SELECT ON SYS.REGISTRY$HISTORY TO aduser;

GRANT CREATE SESSION TO aduser;
declare temp number;
begin
```



```
SELECT count(*) into temp FROM DBA_VIEWS WHERE OWNER='LBACSYS' AND
VIEW_NAME='DBA_SA_USERS';
if (temp>0) then
    execute immediate 'GRANT SELECT ON LBACSYS.DBA_SA_USERS TO aduser';
end if;
end;
/
```

Sybase Audit Privileges

To conduct a full Sybase Audit, you need the following privileges. Make sure the account you are using has rights to use the following tables and views:

- SELECT @@VERSION
- master.dbo.syslogins
- master.dbo.sysrvroles
- master.dbo.sysdatabases
- master.dbo.sysconfigures
- master.dbo.syscurconfigs
- master.dbo.sysroles
- master.dbo.sysloginroles
- master.dbo.sysattributes
- master.dbo.sysservers
- [exec sp_server_info](#)
- [exec sp_loginconfig](#)
- [exec sp_displayaudit](#) (if it's >= 11.5)
- [sp_auditoption](#) (if it's < 11.5 and >= 11.0)
- master.dbo.syblicenseslog
- master.dbo.syscharsets
- <db name>.dbo.sysusers
- <db name>.dbo.sysobjects
- <db name>.dbo.syscomments
- [exec <db name>.dbo.sp_help_resource_limit](#) (if it's >= 11.5)

The following is a list of checks within AppDetectivePro for a Sybase Security Audit, and the tables and views to which they must have permission in order to function properly:

- Audit database owned by sa_role member: master.dbo.syslogins, master.dbo.sysloginroles, master.dbo.syssrvroles, <dbname>.dbo.sysusers
- Auditing of security not enabled: must have sso_role granted.
- Auditing of sso_role not enabled: must have sso_role granted.
- Auditing of sa_role not enabled: must have sso_role granted.
- Guest user exists in sybsecurity: master.dbo.syslogins, master.dbo.syssrvroles, <dbname>.dbo.sysusers
- Login granted sa_role: master.dbo.syslogins, master.dbo.sysloginroles, master.dbo.syssrvroles, <dbname>.dbo.sysusers
- Login granted sso_role: master.dbo.syslogins, master.dbo.sysloginroles, master.dbo.syssrvroles, <dbname>.dbo.sysusers
- Objects not owned by dbo: master.dbo.syslogins, master.dbo.syssrvroles, <dbname>.dbo.sysusers, <dbname>.dbo.sysobjects
- Permission granted in sybsecurity: master.dbo.syslogins, master.dbo.syssrvroles, <dbname>.dbo.sysobjects
- Permission granted on system table: master.dbo.syslogins, master.dbo.syssrvroles, <dbname>.dbo.sysobjects
- Permission granted on xp_cmdshell: master.dbo.syslogins, master.dbo.syssrvroles, <dbname>.dbo.sysobjects
- Permission to select from syslogins: master.dbo.syslogins, master.dbo.syssrvroles
- Permissions granted to public: master.dbo.syslogins, master.dbo.syssrvroles, <dbname>.dbo.sysusers
- Permissions granted to user: master.dbo.syslogins, master.dbo.syssrvroles, <dbname>.dbo.sysusers
- Remote access allowed: master.dbo.syslogins, master.dbo.syssrvroles
- Roles revoked from the sa login: master.dbo.syslogins, master.dbo.sysloginroles, master.dbo.syssrvroles
- Server configured with remote server: master.dbo.syslogins, master.dbo.syssrvroles
- Statement permission granted: master.dbo.syslogins, master.dbo.syssrvroles, <dbname>.dbo.sysusers
- Unrestricted access to syscomments: master.dbo.syslogins, master.dbo.syssrvroles
- Updates allowed to system tables: master.dbo.syslogins, master.dbo.syssrvroles

- With grant option: master.dbo.syslogins, master.dbo.sysserverroles, <dbname>.dbo.sysusers
- xp_cmdshell context: master.dbo.syslogins, master.dbo.sysserverroles, <dbname>.dbo.sysobjects
- Absolute value of numeric DoS (Verify version): master.dbo.syslogins, master.dbo.sysserverroles
- Allow resource limit: master.dbo.syslogins, master.dbo.sysserverroles
- Application schema owner must not be assigned DBA credentials: master.dbo.sysloginroles
- Audit logout not set: sybsystemprocs.dbo.sp_loginconfig, sso_role
- Audit queue size: master.dbo.syslogins, master.dbo.sysserverroles
- Audit subsystem not installed: master.dbo.syslogins, master.dbo.sysserverroles
- Auditing disabled: sybsystemprocs.dbo.sp_loginconfig, sso_role
- Auditing of failed logins not enabled: sybsystemprocs.dbo.sp_loginconfig, sso_role
- Auditing of successful logins not enabled: sybsystemprocs.dbo.sp_loginconfig, sso_role
- Current audit table: master.dbo.syslogins, master.dbo.sysserverroles
- Database replication disabled: master.dbo.sysloginroles
- DBCC CHECKVERIFY buffer overflow: master.dbo.syslogins, master.dbo.sysserverroles
- DROP DATABASE buffer overflow: master.dbo.syslogins, master.dbo.sysserverroles
- Event log computer name: master.dbo.syslogins, master.dbo.sysserverroles
- Event logging: master.dbo.syslogins, master.dbo.sysserverroles
- Exceeded licensing limitations: master.dbo.sysblicenseslog
- Excessive DBA connections: master.dbo.sysloginroles
- Latest patch not applied: master.dbo.syslogins, master.dbo.sysserverroles
- List resource limits: master.dbo.syslogins, master.dbo.sysserverroles
- Log audit logon failure: master.dbo.syslogins, master.dbo.sysserverroles
- Log audit logon success: master.dbo.syslogins, master.dbo.sysserverroles
- No patches available for version: master.dbo.syslogins, master.dbo.sysserverroles
- Password array buffer overflow: master.dbo.syslogins, master.dbo.sysserverroles
- Privileges of database owners: master.dbo.sysloginroles
- Require message confidentiality with encryption: master.dbo.syslogins, master.dbo.sysserverroles
- Require message integrity: master.dbo.syslogins, master.dbo.sysserverroles

- Select all DoS (Verify version): master.dbo.syslogins, master.dbo.sysssrvroles
- Select/Into DoS (Verify version): master.dbo.syslogins, master.dbo.sysssrvroles
- SSL enabled: master.dbo.syslogins, master.dbo.sysssrvroles
- Start mail session: master.dbo.syslogins, master.dbo.sysssrvroles
- Suspend audit when full disabled: master.dbo.syslogins, master.dbo.sysssrvroles
- Vulns for v12.5.3 ESD#1 (Verify version): master.dbo.syslogins, master.dbo.sysssrvroles
- xp_cmdshell not removed: master.dbo.syslogins, master.dbo.sysssrvroles, <dbname>.dbo.sysobjects
- xp_freedll buffer overflow: master.dbo.syslogins, master.dbo.sysssrvroles, <dbname>.dbo.sysobjects
- Blank password for sa: master.dbo.syslogins, master.dbo.sysssrvroles
- Check password for digit: master.dbo.syslogins, master.dbo.sysssrvroles
- Default login exists: sybssystemprocs.dbo.sp_loginconfig, sso_role
- Default login granted role: sybssystemprocs.dbo.sp_loginconfig, sso_role
- Default password for dba repository user: master.dbo.syslogins, master.dbo.sysssrvroles
- Default password for entldbdb: master.dbo.syslogins, master.dbo.sysssrvroles
- Default password for entldbreader: master.dbo.syslogins, master.dbo.sysssrvroles
- Default password for jagadmin: master.dbo.syslogins, master.dbo.sysssrvroles
- Default password for PIAdmin: master.dbo.syslogins, master.dbo.sysssrvroles
- Default password for pkiuser: master.dbo.syslogins, master.dbo.sysssrvroles
- Default password for PortalAdmin: master.dbo.syslogins, master.dbo.sysssrvroles
- Default password for pso: master.dbo.syslogins, master.dbo.sysssrvroles
- Default port used: master.dbo.syslisteners
- Default SAP password: master.dbo.syslogins, master.dbo.sysssrvroles
- Easily-guessed password: master.dbo.syslogins, master.dbo.sysssrvroles
- Easily-guessed sa password: master.dbo.syslogins, master.dbo.sysssrvroles
- Expired logins: master.dbo.syslogins, master.dbo.sysssrvroles
- Guest user exists in database: master.dbo.syslogins, master.dbo.sysssrvroles, <dbname>.dbo.sysusers
- Locked logins: master.dbo.syslogins, master.dbo.sysssrvroles

- Login attributes less restrictive: master.dbo.syslogins, master.dbo.sysssrvroles
- Login mode: sybssystemprocs.dbo.sp_loginconfig, sso_role
- Maximum failed logins: master.dbo.syslogins, master.dbo.sysssrvroles
- Minimum password length: master.dbo.syslogins, master.dbo.sysssrvroles
- Orphaned user: master.dbo.syslogins, master.dbo.sysssrvroles, <dbname>.dbo.sysusers
- Password same as login name: master.dbo.syslogins, master.dbo.sysssrvroles
- Per login password expiration: master.dbo.syslogins, master.dbo.sysssrvroles
- Roles without passwords: master.dbo.syslogins, master.dbo.sysssrvroles
- Secure default login exists: master.dbo.syslogins, master.dbo.sysssrvroles
- System-wide password expiration: master.dbo.syslogins, master.dbo.sysssrvroles
- Unified login required: master.dbo.syslogins, master.dbo.sysssrvroles
- Unlocked sa login: master.dbo.syslogins, master.dbo.sysssrvroles
- Use security services: master.dbo.syslogins, master.dbo.sysssrvroles
- Not using NTFS partition: master.dbo.syslogins, master.dbo.sysssrvroles
- Permissions on files: master.dbo.syslogins, master.dbo.sysssrvroles
- Registry permissions: master.dbo.syslogins, master.dbo.sysssrvroles
- Service runs as LocalSystem: Windows Management Instrumentation (WMI) with Admin privileges (Windows ONLY).
- Setgid bit enabled: master.dbo.syslogins, master.dbo.sysssrvroles
- Setuid bit enabled: master.dbo.syslogins, master.dbo.sysssrvroles

Operating System Considerations (for Audits)

Some AppDetectivePro Audit checks require more than just a valid database account to perform correctly. They have different requirements depending upon whether the operating system (OS) is Windows or UNIX. (The checks are listed in the Audit category [OS Integrity](#).) They only run if the target database has the appropriate OS.

This topic consists of the following sub-topics:

- Windows OS Audit Check Requirements
- UNIX OS Audit Check Requirements.

WINDOWS OS AUDIT CHECK REQUIREMENTS

AppDetectivePro performs Windows OS checks via Windows authentication. Make sure the account and computer you are running AppDetectivePro from has the appropriate permissions for the corresponding checks:

- **Not Using NTFS Partition.** Permission to read the installation disk type.
- **Registry Permissions.** Remote registry access.
- **Service Runs as Local System.** Permission to list the system services.
- **Permissions on Files.** Permission to read files in the installation directory of the database.

UNIX OS AUDIT CHECK REQUIREMENTS

AppDetectivePro performs Unix OS checks via a Telnet or SSH account. Your account must have the appropriate read and directory listing permissions activated on the database installation and running directories.

If you run the following checks:	Then you must have permission to:
Permissions on Files Setgid Bit Enabled Setuid Bit Enabled	List files in the installation directories of the database.

Properly-Configured Environment Variables

AppDetectivePro can Audit platforms that use system variables to specify the location of the database instances. In UNIX, you must set the environment variables correctly in order to use SSH or Telnet to access the accounts. Specific requirements follow.

If you want to Audit the following platform:	Then you must have permission to:
Oracle	Make sure the <code>\$ORACLE_HOME</code> variable is correct.

Sybase	Make sure the <code>\$SYBASE</code> variable is correct.
MySQL	Define a <code>datadir</code> or <code>basedir</code> variable to point to the database root.

Microsoft SQL Server User Rights Review Privileges

This topic consists of the following sub-topics:

- Microsoft SQL Server 2000 User Rights Review Privileges
- Microsoft SQL Server 2005 and Microsoft SQL Server 2008 Audit Privileges

MICROSOFT SQL SERVER 2000 USER RIGHTS REVIEW PRIVILEGES

To conduct a User Rights Review on a Microsoft SQL Server 2000 database, you need the privileges listed below:

Note: Privileges including the tag `<DATABASE>` apply to **every** database in the Microsoft SQL Server instance.

Object | Type | Columns | Privilege

- `<DATABASE>.dbo.sysobjects | table | * | SELECT`
- `<DATABASE>.dbo.systemmembers | table | groupuid, memberuid | SELECT`
- `<DATABASE>.dbo.syscolumns | table | * | SELECT`
- `<DATABASE>.dbo.sysprotects | table | * | SELECT`
- `<DATABASE>.dbo.sysusers | table | uid, name, sid, isapprole, issqlrole, isntgroup, isntuser, isntname | SELECT`
- `master.dbo.syscurconfigs | table | comment, value | SELECT`
- `master.dbo.syslogins | table | loginname, isntname, isntuser, isntgroup, sid, name | SELECT`
- `master.dbo.sysdatabases | table | dbid, name | SELECT`
- `master.dbo.spt_values | table | * | SELECT`
- `master.dbo.sysxlogins | table | name, srvid, xstatus | SELECT`

MICROSOFT SQL SERVER 2005 AND MICROSOFT SQL SERVER 2008 USER RIGHTS REVIEW PRIVILEGES

Important!	While having access to the system views and stored procedures listed below allows you to perform a User Rights Review, Microsoft SQL Server 2005 and Microsoft SQL Server 2008 permissions-based metadata will cause returned data to be filtered to return only data that the account in use should have access to. To make sure that the User Rights Review can see all data available, the account running the review should be granted the server-level VIEW ANY DEFINITION privilege. However, this privilege can still be overridden at the database, schema, and object level by DENYs. The only way to avoid the effect of these DENYs is to run a User Rights Review with an account that's granted the sysadmin server role, which negates the effect of any DENYs. For more information on SQL Server 2005's and Microsoft SQL Server 2008's permissions-based metadata, see: http://msdn.microsoft.com/en-us/library/ms187113.aspx .
-------------------	--

To conduct a User Rights Review on a Microsoft SQL Server 2005 or Microsoft SQL Server 2008 database, you need the privileges listed below:

Required System Privileges:

VIEW ANY DEFINITION

Required Object Privileges:

Object | Type | Columns | Privilege

- <DATABASE>.sys.database_role_members|table|*|SELECT
- <DATABASE>.sys.columns|table|*|SELECT
- <DATABASE>.sys.all_objects|table|*|SELECT
- <DATABASE>.sys.database_principals|table|*|SELECT
- <DATABASE>.sys.database_permissions|table|*|SELECT
- master.sys.configurations|table|*|SELECT
- master.sys.sysdatabases|table|*|SELECT
- master.sys.endpoints|table|*|SELECT
- master.sys.server_principals|table|*|SELECT
- master.sys.server_permissions|table|*|SELECT
- master.sys.server_role_members|table|*|SELECT
- master.sys.sp_dbfixedrolepermission|Stored Procedure|n/a|EXECUTE
- master.sys.sp_srvrolepermission|Stored Procedure|n/a|EXECUTE

Oracle User Rights Review Privileges

To conduct an Oracle User Rights Review, you need the following privileges:

Object|Type|Columns|Privilege

- `SYS.OBJ$|table|*|SELECT`
- `SYS.V_$SYSTEM_PARAMETER|view|*|SELECT`
- `SYS.COL$|table|*|SELECT`
- `SYS.DBA_OBJECTS|view|*|SELECT`
- `SYS.OBJAUTH$|table|*|SELECT`
- `SYS.TABLE_PRIVILEGE_MAP|table|*|SELECT`
- `SYS.USER$|table|*|SELECT`
- `SYS.SYSAUTH$|table|*|SELECT`
- `SYS.SYSTEM_PRIVILEGE_MAP|table|*|SELECT`

Note: The user account must have the `CREATE SESSION` privilege.

Appendix H: Using Microsoft SQL Server with AppDetectivePro

AppDetectivePro can use Microsoft SQL Server, MSDE 2000 SP4, or Microsoft SQL Server 2005/2008 as its back-end database, allowing for a more robust database for use in larger AppDetectivePro installations. The AppDetectivePro installer installs Microsoft Access by default during installation, which is a viable solution for small-to-medium AppDetectivePro installations.

This appendix consists of the following topics:

- [Microsoft SQL Server 2000](#)
- [Microsoft SQL Server 2000 and MSDE 2000 SP 4](#)
- [Microsoft SQL Server 2005/2008 on Windows Vista/Windows 7/Windows Server 2008](#)

Microsoft SQL Server 2000

When using Microsoft SQL Server 2000 as your AppDetective Pro database, be aware of the following login and service pack information.

Caution!	Ensure that the SA administrator password is not left blank.
-----------------	--

CHANGING THE SA LOGIN PASSWORD FROM THE COMMAND PROMPT

To change the `sa` login password from the command prompt:

1. On the AppDetectivePro host, open a command prompt.
2. Enter the command: `sp_password NULL, [newpassword], 'sa'`

CHANGING THE SA LOGIN PASSWORD FROM ENTERPRISE MANAGER

To change the `sa` login password from Enterprise Manager (i.e., the Microsoft SQL Server GUI console):

1. Open the **Security** node under the server name.
2. Click the **Logins** node.
3. Double click the **sa login** in the list on the right.
4. Enter a new password in the **Password** field.
5. Click **OK**.

SERVICE PACKS

Microsoft releases service packs on a regular basis that provide various fixes including security fixes. Stay up-to-date on the latest service pack to minimize your vulnerability to buffer overflows and other attacks.

Because Microsoft SQL Server service packs are cumulative, you do not need to install previous service packs. Each service pack includes all fixes from previously released service packs, and can be applied to an original installation or to one where previous service packs have been applied.

Hint:	To verify what version of Microsoft SQL Server you have installed, run the following command against the database: <code>SELECT @@Version</code>
--------------	--

Microsoft SQL Server 2000 and MSDE 2000 SP 4

If you are running Microsoft SQL Server or MSDE 2000 SP4, you should install service pack 3a. You can download this service pack from <http://www.microsoft.com/sql/downloads/2000/sp3.asp>.

MSDE 2000 SP4 uses Windows authentication. To ensure a higher level of security, make sure your Windows login account uses a strong password. Make sure that the latest service pack or hotfix is installed on your database server.

Microsoft SQL Server 2005/2008 on Windows Vista/Windows 7/Windows Server 2008

When Microsoft SQL Server 2005/2008 is installed on Windows Vista/Windows 7/Windows Server 2008, there may be an issue if the Windows account is used to connect to the database; specifically if the Windows account is granted access to the SQL Server via local Administrators group membership.

To enable members of the Windows Vista Administrators group to log in, you must explicitly add the account to the SQL Server logins. Launch SQL Server management studio as the Administrator, and add the Windows account.

Appendix I: Enabling SSL Encryption on AppDetectivePro

To secure communications between AppDetectivePro machine and the back-end database server (Microsoft SQL Server) on a remote machine, you can use SSL (Secure Sockets Layer) encryption for the database.

For SSL to work you must install Server Authentication Certificate on the database server machine. After the certificate is installed on the server, you can enable SSL encryption either on the server or on client machine, depending whether you want the encryption to be on a per server or per client machine basis.

To enable SSL encryption of AppDetectivePro:

Step	Action
1	Enable SSL encryption on the database server. All database connections from any client to the Microsoft SQL Server are encrypted.
2	Enable SSL encryption on the database client machine. All database connections from the client machine to any Microsoft SQL Server are encrypted.
3	Do <u>not</u> enable SSL on both the server and client. If you use enabling SSL on a database client machine, the client must trust the same root authority of the server certificate.

Appendix J: Default Ports

AppDetectivePro searches the following ports when the Use Default Ports option is active.

DOMINO APPLICATION SERVER

- 80
- 443

DOMINO GROUPWARE SERVER

- 80
- 1352

IBM DB2

- 446
- 523
- 3700
- 3701
- 50000
- 50001
- 50002
- 50003

- 50004
- 50005
- 50006
- 50007
- 50008
- 50009
- 50010

IBM DB2 z/OS

- 446

MICROSOFT SQL SERVER

- 1433
- 1434

MYSQL

- 3306

ORACLE

- 1520
- 1521
- 1522
- 1523
- 1524
- 1525
- 1526
- 1527
- 1528
- 1529
- 1530

SYBASE

- 4000
- 4100
- 5000

Appendix K: Fix Scripts (Detail)

The following tables list each AppDetectivePro fix script (for Microsoft SQL Server, Oracle, Sybase, IBM DB2, and MySQL); for more information on fix scripts, see *Fix Scripts*.

This appendix consists of the following topics:

- Microsoft SQL Server Fix Scripts
- Oracle Fix Scripts
- Sybase Fix Scripts
- IBM DB2 Fix Scripts
- MySQL Fix Scripts.

MICROSOFT SQL SERVER FIX SCRIPTS

Check	Script
xp_controlqueueservice buffer overflow	<pre>USE master GO DROP PROCEDURE xp_controlqueueservice GO</pre>
Password same as login name	<pre>USE master GO sp_password '<!--LOGIN--!>', '<NEW PASSWORD>', '<!--LOGIN--!>' GO</pre>
Blank password	<p>Note: The following SQL statements require sysadmin privileges in order to be performed</p> <pre>USE master GO sp_password NULL, '<NEW PASSWORD>', '<!-- LOGIN--!>' GO</pre>
Easily-guessed password for well-known login	<pre>USE master GO sp_password '<!--PASSWORD--!>', '<NEW PASSWORD>', '<!--LOGIN--!>' GO</pre>
Easily-guessed password for sa	<pre>USE master GO sp_password '<!--PASSWORD--!>', '<NEW PASSWORD>', 'sa' GO</pre>

Check	Script
Blank password for well-known login	<p>Note: The following SQL statements require sysadmin privileges in order to be performed.</p> <pre>USE master GO sp_password NULL, '<NEW PASSWORD>', '<!-- LOGIN--!!>' GO</pre>
Blank password for sa	<p>Note: The following SQL statements require sysadmin privileges in order to be performed</p> <pre>USE master GO sp_password NULL, '<NEW PASSWORD>', 'sa' GO</pre>
srv_paraminfo buffer overflow in xp_showcolv	<pre>USE master GO REVOKE EXECUTE ON master.dbo.xp_showcolv FROM public GO</pre>
Extended stored proc privilege upgrade	<pre>USE master GO REVOKE ALL ON [<!--EXTENDED STORED PROCEDURE--!!>] FROM public GO</pre>
srv_paraminfo buffer overflow in xp_proxiedmetadata	<pre>USE master GO REVOKE EXECUTE ON master.dbo.xp_proxiedmetadata FROM public GO</pre>

Check	Script
xp_dsninfo buffer overflow	<pre>USE master GO DROP PROCEDURE xp_dsninfo GO</pre>
xp_oledbinfo buffer overflow	<p>Note: Despite performing the following SQL statements, vulnerabilities may still show up in future Security Audits. To fully fix this vulnerability, please apply the latest patch.</p>
xp_repl_encrypt buffer overflow	<p>Note: Despite performing the following SQL statements, vulnerabilities may still show up in future Security Audits. To fully fix this vulnerability, please apply the latest patch.</p>
xp_dirtree buffer overflow	<p>Note: Despite performing the following SQL statements, vulnerabilities may still show up in future Security Audits. To fully fix this vulnerability, please apply the latest patch.</p>
Enterprise Manager improperly revokes proxy account	<pre>DECLARE @regread_dropped int DECLARE @regwrite_dropped int SELECT @regread_dropped=0, @regwrite_dropped=0 IF not exists (select * from master.dbo.sysobjects where name = 'xp_instance_regread') BEGIN EXECUTE master.dbo.sp_addextendedproc 'xp_instance_reg</pre>
Permission on registry extended proc	<pre>USE <!--DATABASE--!> GO REVOKE EXECUTE ON [<!--EXTENDED STORED PROCEDURE--!>] FROM <!--GRANTED TO--!> GO</pre>

Check	Script
srv_paraminfo buffer overflow in sp_OAGetProperty	Note: Despite performing the following SQL statements, vulnerabilities may still show up in future Security Audits. To fully fix this vulnerability, please apply the latest patch.
Remote access allowed	USE master GO sp_configure 'remote access', 0 GO RECONFIGURE GO
srv_paraminfo buffer overflow in xp_updatecolvbm	USE master GO REVOKE EXECUTE ON master.dbo.xp_updatecolvbm FROM public GO
Format string vuln in xp_sprintf	USE master GO REVOKE EXECUTE ON master.dbo.xp_sprintf FROM public GO
Changing mode may leave sa password blank	Note: The following SQL statements require sysadmin privileges in order to be performed USE master GO sp_password NULL, '<NEW PASSWORD>', 'sa' GO
srv_paraminfo buffer overflow in xp_sqlagent_monitor	Note: Despite performing the following SQL statements, vulnerabilities may still show up in future Security Audits. To fully fix this vulnerability, please apply the latest patch.

Check	Script
srv_paraminfo buffer overflow in sp_OACreate	Note: Despite performing the following SQL statements, vulnerabilities may still show up in future Security Audits. To fully fix this vulnerability, please apply the latest patch.
srv_paraminfo buffer overflow in xp_peekqueue	USE master GO REVOKE EXECUTE ON master.dbo.xp_peekqueue FROM public GO
Permissions granted to user	USE [<!--DATABASE--!>] GO REVOKE <!--PRIVILEGE--!> ON <!--OBJECT NAME--!> FROM [<!--GRANTED TO--!>] GO
Easily-guessed password	USE master GO sp_password '<!--PASSWORD--!>', '<NEW PASSWORD>', '<!--LOGIN--!>' GO
Permission on OLE automation procs	USE master GO REVOKE EXECUTE ON [<!--OBJECT NAME--!>] FROM [<!--USER NAME--!>] GO
srv_paraminfo buffer overflow in sp_OASetProperty	Note: Despite performing the following SQL statements, vulnerabilities may still show up in future Security Audits. To fully fix this vulnerability, please apply the latest patch.

Check	Script
srv_paraminfo buffer overflow in xp_execresultset	<pre>USE master GO REVOKE EXECUTE ON master.dbo.xp_execresultset FROM public GO</pre>
Direct updates on data dictionary	<pre>USE master GO sp_configure 'allow updates', 0 GO RECONFIGURE WITH OVERRIDE GO</pre>
srv_paraminfo buffer overflow in xp_SetSQLSecurity	<pre>USE master GO REVOKE EXECUTE ON master.dbo.xp_SetSQLSecurity FROM public GO</pre>
srv_paraminfo buffer overflow in xp_printstatements	<pre>USE master GO REVOKE EXECUTE ON master.dbo.xp_printstatements FROM public GO</pre>
srv_paraminfo buffer overflow in sp_OAMethod	<p>Note: Despite performing the following SQL statements, vulnerabilities may still show up in future Security Audits. To fully fix this vulnerability, please apply the latest patch.</p>
Unauthorized object permission grants	<pre>IF DB_ID(N'<!--DATABASE--!>') IS NOT NULL EXEC('USE [<!--DATABASE--!>] + ' REVOKE <!-- PERMISSION--!> ON [<!--OWNER--!>].[<!-- OBJECT NAME--!>] FROM [<!--GRANTEE--!>]')</pre>

Check	Script
Default trace disabled	<pre>USE master exec sp_configure 'show advanced options', 1 reconfigure exec sp_configure 'default trace enabled', 1 reconfigure</pre>
Agent jobs privilege escalation	<pre>USE <!--DATABASE--!> GO REVOKE ALL ON [<!--STORED PROCEDURE--!>] FROM public GO</pre>
Remote admin connections allowed	<pre>exec sp_configure 'remote admin connections', 0 go reconfigure go</pre>
Agent XPs enabled	<pre>USE master EXEC sp_configure 'show advanced options', 1 RECONFIGURE EXEC sp_configure 'Agent XPs', '0' RECONFIGURE</pre>
sp_replwritetovarbin limited memory overwrite vulnerability	<pre>USE master GO REVOKE ALL ON master.dbo.sp_replwritetovarbin FROM [<!--GRANTED TO--!>] GO</pre>
xp_cmdshell not removed/not disabled	<pre>USE master GO sp_dropextendedproc @funcname='xp_cmdshell' GO</pre>

Check	Script
Unauthorized object permission grants	<pre>IF DB_ID(N'<!--DATABASE--!>') IS NOT NULL EXEC('USE [<!--DATABASE--!>] + ' REVOKE <!-- PERMISSION--!> ON [<!--COLUMN--!>] FROM [<!-- -GRANTEE--!>']')</pre>
C2 Audit Mode	<pre>USE master EXEC sp_configure 'show advanced option', '1' RECONFIGURE WITH OVERRIDE EXEC sp_configure 'c2 audit mode', 1 RECONFIGURE WITH OVERRIDE</pre>
Unauthorized object permission grants	<pre>DECLARE @oldValue int SELECT @oldValue = value FROM master..syscurconfigs where config=102 We have to run SP_CONFIGURE to allow updates to the system catalogs EXEC SP_CONFIGURE 'ALLOW UPDATES', 1 RECONFIGURE WITH OVERRIDE</pre>
Unauthorized object permission grants	<pre>EXEC SP_CONFIGURE 'ALLOW UPDATES', @oldValue RECONFIGURE WITH OVERRIDE GO</pre>
Permissions granted to GUEST	<pre>IF DB_ID(N'<!--DATABASE--!>') IS NOT NULL EXEC('USE [<!--DATABASE--!>] + ' REVOKE <!-- PERMISSION--!> FROM GUEST')" Permissions granted to GUEST IF DB_ID(N'<!--DATABASE--!>') IS NOT NULL EXEC('USE [<!--DATABASE--!>] + ' REVOKE <!-- PERMISSION--!> ON [<!--OWNER--!>].[<!-- OBJECT NAME--!>] FROM GUEST')</pre>

Check	Script
Unauthorized object permission grants	<pre>IF DB_ID(N'<!--DATABASE--!>') IS NOT NULL EXEC('USE [<!--DATABASE--!>] + ' REVOKE <!-- PERMISSION--!> ON [<!--SCHEMA NAME--!>]. [<!-- OBJECT NAME--!>] FROM [<!--GRANTEE--!>]')</pre>
Permissions granted to GUEST	<pre>IF DB_ID(N'<!--DATABASE--!>') IS NOT NULL EXEC('USE [<!--DATABASE--!>] + ' REVOKE <!-- PERMISSION--!> ON [<!--SCHEMA NAME--!>]. [<!-- OBJECT NAME--!>] FROM GUEST')</pre>
Unauthorized object permission grants	<pre>IF DB_ID(N'<!--DATABASE--!>') IS NOT NULL EXEC('USE [<!--DATABASE--!>] + ' REVOKE <!-- PERMISSION--!> FROM [<!--GRANTEE--!>]')</pre>
Permission on sp_runwebtask	<pre>USE master GO REVOKE ALL ON master.dbo.sp_runwebtask FROM public GO</pre>
Statement permission granted	<pre>USE <!--DATABASE--!> GO REVOKE <!--PRIVILEGE--!> FROM <!--GRANTED TO--!> GO</pre>
Permission grantable	<pre>USE [<!--DATABASE--!>] GO REVOKE <!--PRIVILEGE--!> ON [<!--DATABASE-- !>]. [<!--SCHEMA NAME--!>]. [<!--OBJECT NAME-- !>] FROM <!--GRANTED TO--!> CASCADE GO</pre>

Check	Script
Guest user exists in database	<pre>USE <!--DATABASE--!> GO sp_dropuser guest GO</pre>
Registry extended proc not removed	<pre>USE master GO sp_dropextendedproc @funcname='<!--EXTENDED STORED PROCEDURE--!>' GO</pre>
xp_createqueue buffer overflow	<pre>USE master GO DROP PROCEDURE xp_createqueue GO</pre>
Permissions granted on xp_cmdshell	<pre>USE master GO IF exists (select * from master.dbo.sysobjects where name = 'xp_cmdshell') REVOKE EXECUTE ON [xp_cmdshell] FROM [<!-- USER NAME--!>] GO</pre>
Permission grantable	<pre>USE [<!--DATABASE--!>] GO REVOKE <!--PRIVILEGE--!> ON [<!--DATABASE-- !>]. [<!--OWNER--!>]. [<!--OBJECT NAME--!>] FROM <!--GRANTED TO--!> CASCADE GO</pre>

Check	Script
Permissions granted to user	<pre>USE [<!--DATABASE--!>] GO REVOKE <!--PRIVILEGE--!> FROM [<!--GRANTED TO--!>] GO</pre>
C2 Audit Mode	<pre>DECLARE @oldValue int SELECT @oldValue = value FROM master..syscurconfigs where config=518 --We have to run SP_CONFIGURE 'show advanced option', '1' to be able to change advanced options</pre>
Permissions granted to user	<pre>USE [<!--DATABASE--!>] GO REVOKE <!--PRIVILEGE--!> ON [<!--SCHEMA NAME--!>]. [<!--OBJECT NAME--!>] FROM [<!--GRANTED TO--!>] CASCADE GO</pre>
Permission to select from system table	<pre>USE [<!--DATABASE--!>] GO REVOKE SELECT ON [<!--DATABASE--!>]. [<!--SCHEMA NAME--!>]. [<!--TABLE NAME--!>] FROM [<!--GRANTED TO--!>] CASCADE GO</pre>
Permission to select from system table	<pre>USE [<!--DATABASE--!>] GO REVOKE SELECT ON [<!--DATABASE--!>]. [<!--OWNER--!>]. [<!--TABLE NAME--!>] FROM [<!--GRANTED TO--!>] CASCADE GO</pre>

Check	Script
Error logs can be overwritten	<p>Note: Despite performing the following SQL statements, vulnerabilities may still show up in future Security Audits. To fully fix this vulnerability, please apply the latest patch.</p> <pre> Permission to select from syslogins USE master GO REVOKE SELECT ON master.dbo.syslogins FROM <!--GRANTED TO--!> GO </pre>
Objects not owned by dbo	<pre> USE <!--DATABASE--!> GO DROP TABLE [<!--DATABASE--!>]. [<!--OWNER--!>]. [<!--OBJECT NAME--!>] GO </pre>
srv_paraminfo buffer overflow in sp_OADestroy	<p>Note: Despite performing the following SQL statements, vulnerabilities may still show up in future Security Audits. To fully fix this vulnerability, please apply the latest patch.</p>
Default password for well-known login	<pre> USE master GO sp_password <!--PASSWORD--!>, <NEW PASSWORD>, <!--LOGIN--!> GO </pre>
Permissions granted to PUBLIC	<pre> EXEC SP_CONFIGURE 'ALLOW UPDATES', @oldValue RECONFIGURE WITH OVERRIDE GO </pre>

Check	Script
sysadmin role granted "USE master	GO EXEC sp_dropsrvrolemember N'<!--LOGIN--!>', 'sysadmin' GO
xp_deletequeue buffer overflow	USE master GO DROP PROCEDURE xp_deletequeue GO
xp_displayqueuemsgs buffer overflow	USE master GO DROP PROCEDURE xp_displayqueuemsgs GO
xp_readpkfromqueue buffer overflow	USE master GO DROP PROCEDURE xp_readpkfromqueue GO
xp_sprintf buffer overflow	USE master GO REVOKE EXECUTE ON master.dbo.xp_sprintf FROM public GO
xp_unpackcab buffer overflow	USE master GO DROP PROCEDURE xp_unpackcab GO

Check	Script
Permission on sp_MSsetalertinfo	USE master GO REVOKE ALL ON master.dbo.sp_MSsetalertinfo FROM public GO
xp_mergelineages buffer overflow	USE master GO DROP PROCEDURE xp_mergelineages GO
xp_decodequeuecmd buffer overflow	USE master GO DROP PROCEDURE xp_decodequeuecmd GO
xp_resetqueue buffer overflow	USE master GO DROP PROCEDURE xp_resetqueue GO
Permissions granted to GUEST	EXEC SP_CONFIGURE 'ALLOW UPDATES', @oldValue RECONFIGURE WITH OVERRIDE GO
xp_sqlagent_param buffer overflow	Note: Despite performing the following SQL statements, vulnerabilities may still show up in future Securit Audits. To fully fix this vulnerability, please apply the latest patch.

Check	Script
xp_readpkfromvarbin buffer overflow	USE master GO DROP PROCEDURE xp_readpkfromvarbin GO
Encoded password written by installation	USE master GO sp_password <!--SQLDOMAINPWD--!>,<NEW PASSWORD>,'sa' GO
Encoded password written by installation	USE master GO sp_password <!--CONFIRMPWD--!>,<NEW PASSWORD>,'sa' GO
Encoded password written by installation	USE master GO sp_password <!--ENTERPWD--!>,<NEW PASSWORD>,'sa' GO
xp_sqlinventory buffer overflow	USE master GO DROP PROCEDURE xp_sqlinventory GO
Encoded password written by installation	USE master GO sp_password <!--AGTDOMAINPWD--!>,<NEW PASSWORD>,'sa' GO

Check	Script
Fixed server role granted	<pre>USE master GO EXEC sp_dropserverolemember N'<!--LOGIN--!>', '<!--PRIVILEGE--!>' GO</pre>
Encoded password written by installation	<pre>USE master GO sp_password <!--SVPWD--!>, <NEWPASSWORD>, 'sa' GO</pre>
Encoded password written by installation	<pre>USE master GO sp_password <!--SVPASSWORD--!>, <NEWPASSWORD>, 'sa' GO</pre>
DTS password table publicly viewable	<pre>USE msdb GO sp_dropuser guest GO REVOKE SELECT ON RTblDBMProps FROM public GO</pre>
Table to store DTS passwords publicly viewable	<pre>USE msdb GO sp_dropuser guest GO REVOKE SELECT ON RTblDBMProps FROM public GO</pre>

Check	Script
sp_MScopyscriptfile command injection	Note: Despite performing the following SQL statements, vulnerabilities may still show up in future Security Audits. To fully fix this vulnerability, please apply the latest patch.
Public can create Agent jobs	<pre>USE <!--DATABASE--!> GO REVOKE ALL ON [<!--STORED PROCEDURE--!>] FROM public GO</pre>
Permission on sp_MSSetServerProperties	<pre>USE master GO REVOKE ALL ON master.dbo.sp_MSSetServerProperties FROM public GO</pre>
xp_deleteprivatequeue buffer overflow	<pre>USE master GO DROP PROCEDURE xp_deleteprivatequeue GO</pre>
srv_paraminfo buffer overflow in xp_displayparamstmt	<pre>USE master GO REVOKE EXECUTE ON master.dbo.xp_displayparamstmt FROM public GO</pre>

Check	Script
Permissions granted to PUBLIC	<pre>IF DB_ID(N'<!--DATABASE--!>') IS NOT NULL EXEC('USE [<!--DATABASE--!>] + ' REVOKE <!--PERMISSION--!> ON [<!--OWNER--!>].[<!--OBJECT NAME--!>] FROM PUBLIC')</pre> <p>xp_proxiedmetadata buffer overflow</p> <p>Note: Despite performing the following SQL statements, vulnerabilities may still show up in future Security Audits. To fully fix this vulnerability, please apply the latest patch.</p>
xp_createprivatequeue buffer overflow	<pre>USE master GO DROP PROCEDURE xp_createprivatequeue GO</pre>
Permissions granted on sp_add_dtspackage	<pre>USE msdb GO REVOKE EXECUTE ON sp_add_dtspackage FROM public GO</pre> <p>Permissions granted to GUEST"IF DB_ID(N'<!--DATABASE--!>') IS NOT NULL</p> <pre>EXEC('USE [<!--DATABASE--!>] + ' REVOKE <!--PERMISSION--!> ON [<!--COLUMN--!>] FROM GUEST')</pre>
Permission on mswebtasks	<pre>USE msdb GO REVOKE <!--PERMISSION--!> ON msdb.dbo.mswebtasks FROM public GO</pre>

Check	Script
Permission on sp_readwebtask	<pre>USE master GO REVOKE ALL ON master.dbo.sp_readwebtask FROM public GO</pre>
Permission on xp_readerrorlog	<pre>USE master GO REVOKE ALL ON master.dbo.xp_readerrorlog FROM <!--GRANTED TO--!> GO</pre>
xstatus backdoor	<pre>EXEC SP_CONFIGURE 'ALLOW UPDATES', @oldValue RECONFIGURE WITH OVERRIDE GO</pre>
xstatus backdoor	<pre>DECLARE @oldValue int SELECT @oldValue = value FROM master..syscurconfigs where config=102 We have to run SP_CONFIGURE to allow updates to the system catalogs EXEC SP_CONFIGURE 'ALLOW UPDATES', 1 RECONFIGURE WITH OVERRIDE</pre>
DTS package procedures granted to public	<pre>USE <!--DATABASE--!> GO REVOKE ALL ON [<!--DATABASE--!>]. [<!-- OWNER--!>]. [<!--PROCEDURE NAME--!>] FROM public GO</pre>

Check	Script
Agent jobs privilege escalation	<pre>USE <!--DATABASE--!> GO REVOKE ALL ON [<!--EXTENDED STORED PROCEDURE--!>] FROM public GO</pre>
xstatus backdoor	<pre>USE master exec('delete from master.dbo.sysxlogins where [name] = "<!--LOGIN--!>"') EXEC sp_grantlogin N'<!--LOGIN--!>'</pre>
DTS package procedures granted to public	<pre>USE <!--DATABASE--!> GO REVOKE ALL ON [<!--DATABASE--!>]. [<!-- OWNER--!>]. [<!--TABLE NAME--!>] FROM public GO</pre>
SQL injection in sp_MSdropretry	<p>Note: Despite performing the following SQL statements, vulnerabilities may still show up in future Security Audits. To fully fix this vulnerability, please apply the latest patch.</p>
SQL Agent password publicly viewable	<pre>USE msdb GO sp_dropuser guest GO REVOKE ALL ON sp_get_sqlagent_properties FROM public GO</pre>

Check	Script
SQL Agent procedures granted to public	<pre>USE msdb GO sp_dropuser guest GO REVOKE ALL ON sp_get_sqlagent_properties FROM public GO</pre>
Permissions granted to GUEST	<pre>DECLARE @oldValue int SELECT @oldValue = value FROM master..syscurconfigs where config=102 We have to run SP_CONFIGURE to allow updates to the system catalogs EXEC SP_CONFIGURE 'ALLOW UPDATES', 1 RECONFIGURE WITH OVERRIDE</pre>
Permissions granted to PUBLIC	<pre>IF DB_ID(N'<!--DATABASE--!>') IS NOT NULL EXEC('USE [<!--DATABASE--!>] + ' REVOKE <!-- PERMISSION--!> ON [<!--COLUMN--!>] FROM PUBLIC') Permissions granted to PUBLIC"IF DB_ID(N'<!-- DATABASE--!>') IS NOT NULL EXEC('USE [<!--DATABASE--!>] + ' REVOKE <!-- PERMISSION--!> ON [<!--SCHEMA NAME--!>].[<!-- OBJECT NAME--!>] FROM PUBLIC')</pre>
Sample database not removed	<pre>USE master GO DROP DATABASE <!--DATABASE--!> GO</pre>

Check	Script
Permissions granted to PUBLIC	DECLARE @oldValue int SELECT @oldValue = value FROM master..syscurconfigs where config=102 We have to run SP_CONFIGURE to allow updates to the system catalogs EXEC SP_CONFIGURE 'ALLOW UPDATES', RECONFIGURE WITH OVERRIDE
Permissions granted to PUBLIC	IF DB_ID(N'<!--DATABASE--!>') IS NOT NULL EXEC('USE [<!--DATABASE--!>] + ' REVOKE <!-- PERMISSION--!> FROM PUBLIC')

ORACLE FIX SCRIPTS

Check	Script
Brute-force role password	ALTER ROLE <!--USERNAME--!!> IDENTIFIED BY <PASSWORD>;
Object privilege granted to PUBLIC	BEGIN IF UPPER('<!--PRIVILEGE--!!>') IN ('DEQUEUE', 'ENQUEUE') THEN DBMS_AQADM.REVOKE_QUEUE_PRIVILEGE('<!--PRIVILEGE--!!>', '<!--OWNER--!!>.<!--OBJECT NAME--!!>', 'PUBLIC'); ELSE EXECUTE IMMEDIATE 'REVOKE <!--PRIVILEGE--!!> ON "<!--OWNER--
Account granted the predefined role CONNECT	CREATE ROLE <NEW ROLE>; GRANT CREATE SESSION TO <NEW ROLE>;
Account granted the predefined role CONNECT	REVOKE CONNECT FROM <!--GRANTED TO--!!>; GRANT <NEW ROLE> TO <!--GRANTED TO--!!>;
Non-standard account with DBA role	REVOKE DBA FROM <!--GRANTED TO--!!>;
Account granted the predefined role RESOURCE	CREATE ROLE <NEW ROLE>; GRANT CREATE SESSION TO <NEW ROLE>;
Privilege to execute UTL_HTTP granted to PUBLIC	REVOKE EXECUTE ON SYS.UTL_HTTP FROM PUBLIC;
Easily-guessed role password	ALTER ROLE <!--USER NAME--!!> IDENTIFIED BY <PASSWORD>;
Privilege to execute UTL_SMTP granted to PUBLIC	REVOKE EXECUTE ON SYS.UTL_SMTP FROM PUBLIC;

Check	Script
Profile settings - Failed Login Attempts	ALTER PROFILE <!--PROFILE--!> LIMIT FAILED_LOGIN_ATTEMPTS 10;
Object privilege grantable	BEGIN IF UPPER('<!--PRIVILEGE--!>') IN ('DEQUEUE', 'ENQUEUE') THEN DBMS_AQADM.REVOKE_QUEUE_PRIVILEGE('<!--PRIVILEGE--!>', '<!--OWNER--!>.<!--OBJECT NAME--!>', '<!--GRANTED TO--!>'); DBMS_AQADM.GRANT_QUEUE_PRIVILEGE('<!--PRIVILEGE--!>'
Privilege on database link table	REVOKE <!--PRIVILEGE--!> ON SYS.LINK\$ FROM <!--USER NAME--!>;
Object privilege granted to account	CREATE ROLE <NEW ROLE>;
Default database password	ALTER USER <!--USER NAME--!> IDENTIFIED BY <NEW PASSWORD>;
Account granted the predefined role RESOURCE	REVOKE RESOURCE FROM <!--GRANTED TO--!>; GRANT <NEW ROLE> TO <!--GRANTED TO--!>;
System privilege granted WITH ADMIN OPTION	REVOKE <!--PRIVILEGE--!> FROM <!--GRANTED TO--!>; GRANT <!--PRIVILEGE--!> TO <!--GRANTED TO--!>;
Role without password	ALTER ROLE <!--ROLE--!> IDENTIFIED BY <PASSWORD>;
Profile settings - Password Verify Function	ALTER PROFILE <!--PROFILE--!> LIMIT PASSWORD_VERIFY_FUNCTION <NEW VERIFY FUNCTION>;
Profile settings - Password Reuse Time	ALTER PROFILE <!--PROFILE--!> LIMIT PASSWORD_REUSE_TIME 180 PASSWORD_REUSE_MAX UNLIMITED;

Check	Script
Profile settings - Password Reuse Maximum	ALTER PROFILE <!--PROFILE--!> LIMIT PASSWORD_REUSE_MAX 10 PASSWORD_REUSE_TIME UNLIMITED;
Profile settings - Password Lock Time	ALTER PROFILE <!--PROFILE--!> LIMIT PASSWORD_LOCK_TIME 1;
Profile settings - Password Life Time	ALTER PROFILE <!--PROFILE--!> LIMIT PASSWORD_LIFE_TIME 90;
Profile settings - Password Grace Time	ALTER PROFILE <!--PROFILE--!> LIMIT PASSWORD_GRACE_TIME 3;
Object privilege granted to account	BEGIN IF NOT UPPER('<!--PRIVILEGE--!>') IN ('INDEX', 'REFERENCES') THEN EXECUTE IMMEDIATE 'REVOKE <!-- PRIVILEGE--!> ON ""<!--OWNER--!>"".'""<!-- OBJECT NAME--!>"" FROM <!--GRANTED TO-- !>; EXECUTE IMMEDIATE 'GRANT <!-- PRIVILEGE--!> ON ""<!--
Privilege to execute UTL_FILE granted to PUBLIC	REVOKE EXECUTE ON SYS.UTL_FILE FROM PUBLIC;
Auditing of CREATE SESSION not enabled	AUDIT SESSION;
SQL Injection in OWF_MGR.WF_LOV	REVOKE EXECUTE ON OWF_MGR.WF_LOV FROM PUBLIC;
Password for database user same as username	ALTER USER <!--USER NAME--!> IDENTIFIED BY <NEW PASSWORD>;
Expired password	ALTER USER <!--USERNAME--!> IDENTIFIED BY <NEW PASSWORD>;
Account granted ALTER SYSTEM privilege	REVOKE ALTER SYSTEM FROM <!--GRANTED TO--!>;

Check	Script
System privilege with ANY clause	REVOKE <!--PRIVILEGE--!> FROM <!--GRANTED TO--!>;
Create library privilege	REVOKE <!--PRIVILEGE--!> FROM <!--GRANTED TO--!>;
Privilege on audit trail table	REVOKE <!--PRIVILEGE--!> ON SYS.AUD\$ FROM <!--GRANTED TO--!>;
Account associated with DEFAULT profile	ALTER USER <!--USERNAME--!> PROFILE <NEW PROFILE NAME>;
Account associated with DEFAULT profile	CREATE PROFILE <NEW PROFILE NAME> LIMIT SESSIONS_PER_USER 2 CPU_PER_SESSION unlimited CPU_PER_CALL 6000 LOGICAL_READS_PER_SESSION unlimited LOGICAL_READS_PER_CALL 100 IDLE_TIME 30 CONNECT_TIME 480;
Privilege granted to SELECT from data dictionary	REVOKE <!--PRIVILEGE--!> ON <!--TABLE NAME--!> FROM <!--GRANTED TO--!>;
Account granted the predefined role DBA	CREATE ROLE <NEW ROLE>;
System privilege granted to account	CREATE ROLE <NEW ROLE>;VARIABLE privilege_name VARCHAR2(20); VARIABLE privilege_user VARCHAR2(100);
Account can access source code as SYS	REVOKE <!--PRIVILEGE--!> FROM <!--GRANTED TO--!>;

Check	Script
System privilege granted to account"	<pre>BEGIN :privilege_user := 'Privilege: ' '<!--PRIVILEGE--!!>' ' - User: ' '<!--GRANTED TO--!!>'; END; / PRINT :privilege_user; BEGIN --UNLIMITED TABLESPACE, SYSDBA or SYSOPER privilege cannot be granted to a role. IF NOT UPPER('<!--PRIVILEGE"</pre>
Overdue password change	<pre>ALTER USER <!--USERNAME--!!> IDENTIFIED BY <PASSWORD>;</pre>
Account can grant any role	<pre>REVOKE GRANT ANY ROLE FROM <!-- GRANTED TO--!!>;</pre>
SQL Injection in PORTAL.WPG_SESSION	<pre>REVOKE EXECUTE ON PORTAL.WPG_SESSION FROM PUBLIC;</pre>
Accounts with SYSTEM as default tablespace	<pre>ALTER USER <!--USER NAME--!!> DEFAULT TABLESPACE <NEW DEFAULT TABLESPACE>;</pre>
SQL Injection in ORASSO.WPG_SESSION	<pre>REVOKE EXECUTE ON ORASSO.WPG_SESSION FROM PUBLIC;</pre>
Account granted the predefined role DBA	<pre>REVOKE DBA FROM <!--GRANTED TO--!!>; GRANT CREATE SESSION TO <NEW ROLE>; GRANT <NEW ROLE> TO <!--GRANTED TO-- !!>;</pre>
Account can replace public links	<pre>REVOKE CREATE PUBLIC DATABASE LINK FROM <!--GRANTED TO--!!>; REVOKE DROP PUBLIC DATABASE LINK FROM <!--GRANTED TO--!!>;</pre>

Check	Script
Privilege to execute DBMS_RANDOM granted to PUBLIC	REVOKE EXECUTE ON SYS.DBMS_RANDOM FROM PUBLIC;
Roles granted WITH ADMIN OPTION	REVOKE <!--ROLE--!> FROM <!--GRANTED TO--!>; GRANT <!--ROLE--!> TO <!--GRANTED TO--!>;
Account granted the JAVA_ADMIN role	REVOKE JAVA_ADMIN FROM <!--GRANTED TO--!>;
Default role password	ALTER ROLE <!--ROLE--!> IDENTIFIED BY <PASSWORD>;
System privilege granted to PUBLIC	REVOKE "<!--PRIVILEGE--!>" FROM PUBLIC;
SQL Injection in OWF_MGR.WF_EVENT_HTML	REVOKE EXECUTE ON OWF_MGR.WF_EVENT_HTML FROM PUBLIC;
Privilege to execute UTL_TCP granted to PUBLIC	REVOKE EXECUTE ON SYS.UTL_TCP FROM PUBLIC;
Account can become another user	REVOKE BECOME USER FROM <!--GRANTED TO--!>; REVOKE ALTER USER FROM <!--GRANTED TO--!>;
Account can create public synonyms	REVOKE CREATE PUBLIC SYNONYM FROM <!--GRANTED TO--!>;

SYBASE FIX SCRIPTS

Check	Script
Server configured with remote server	USE master sp_dropserver <!--SERVER NAME--!>, droplogins
Allow resource limit	USE master sp_configure 'allow resource limits', 1 RECONFIGURE
Permission granted in sybsecurity	USE <!--DATABASE--!> REVOKE <!--PRIVILEGE--!> ON <!-- DATABASE--!>.<!--OWNER--!>.<!--OBJECT-- !!>.<!--COLUMN--!> FROM <!--GRANTED TO--!>
Permission granted on xp_cmdshell	USE <!--DATABASE--!> REVOKE EXECUTE ON xp_cmdshell FROM <!--GRANTED TO--!>
Permission granted in sybsecurity	USE <!--DATABASE--!> REVOKE <!--PRIVILEGE--!> ON <!-- DATABASE--!>.<!--OWNER--!>.<!--OBJECT-- !!> FROM <!--GRANTED TO--!>
Auditing disabled	sp_auditooption 'enable auditing', 'on' sp_configure 'auditing', 1
Log audit logon failure	USE master sp_configure 'log audit logon failure', 1 RECONFIGURE
Blank password for sa	USE master sp_password <CURRENT PASSWORD>, <NEW PASSWORD>, 'sa'

Easily-guessed sa password	USE master sp_password <CURRENT PASSWORD>, <NEW PASSWORD>, 'sa'
Default password for entldbreader	USE master sp_password <CURRENT PASSWORD>, <NEW PASSWORD>, 'entldbreader'
Default password for jagadmin	USE master sp_password <CURRENT PASSWORD>, <NEW PASSWORD>, 'jagadmin'
Suspend audit when full disabled	USE master sp_configure 'suspend audit when device full', 1 RECONFIGURE
Statement permission granted	USE <!--DATABASE--!> REVOKE <!--PRIVILEGE--!> FROM <!-- GRANTED TO--!>
Default password for entldbdbo	USE master sp_password <CURRENT PASSWORD>, <NEW PASSWORD>, 'entldbdbo'
Default password for dba repository user	USE master sp_password <CURRENT PASSWORD>, <NEW PASSWORD>, 'dba'
Easily-guessed password	USE master sp_password <CURRENT PASSWORD>, <NEW PASSWORD>, <!--LOGIN--!>
Permissions granted to public	USE <!--DATABASE--!> REVOKE <!--PRIVILEGE--!> ON <!-- DATABASE--!>.<!--OWNER--!>.<!--OBJECT-- !!>.<!--COLUMN--!> FROM public

Require message integrity	USE master execute sp_configure 'msg integrity reqd', 1 execute sp_configure 'use security services', 1
Default password for pso	USE master sp_password <CURRENT PASSWORD>, <NEW PASSWORD>, 'pso'
Unrestricted access to syscomments	USE master sp_configure 'select on syscomments.text', 0 RECONFIGURE
Audit database owned by sa_role member	USE master sp_changedbowner <!---LOGIN--!> <, true >
Login attributes less restrictive	USE master sp_modifylogin <!---LOGIN--!>, 'max failed_logins', <NEW VALUE> sp_modifylogin <!---LOGIN--!>, 'passwd expiration', <NEW VALUE> sp_modifylogin <!---LOGIN--!>, 'min passwd length', <NEW VALUE> sp_modifylogin 'all overrides', 'max failed_login
Unlocked sa login	USE master sp_role ""grant"", sa_role, <NEW SA LOGIN> sp_role ""grant"", sso_role, <NEW SA LOGIN> sp_locklogin 'sa', ""lock""
With grant option	USE <!---DATABASE--!> REVOKE <!---PRIVILEGE--!> ON <!---DATABASE--!>.<!---OWNER--!>.<!---OBJECT--!> FROM <!---DATABASE--!>.<!---USER--!> CASCADE
Auditing of failed logins not enabled	sp_auditooption 'logins', 'fail' sp_audit 'login', 'all', 'all', 'fail'

Permissions granted to public	USE <!--DATABASE--!> REVOKE <!--PRIVILEGE--!> ON <!-- DATABASE--!>.<!--OWNER--!>.<!--OBJECT-- !!> FROM public
Expired logins	USE master sp_password <CURRENT PASSWORD>, <NEW PASSWORD>, <!--LOGIN--!>
Login granted sa_role	USE master REVOKE sa_role FROM <!--LOGIN--!>
Login granted sso_role	USE master REVOKE sso_role FROM <!--LOGIN--!>
Guest user exists in sybsecurity	USE sybsecurity sp_dropuser guest
Auditing of successful logins not enabled	sp_auditoption 'logins', 'ok' sp_audit 'login', 'all', 'all', 'pass'
Permissions granted to user	USE <!--DATABASE--!> REVOKE <!--PRIVILEGE--!> ON <!-- DATABASE--!>.<!--OWNER--!>.<!--OBJECT-- !!> FROM <!--GRANTED TO--!>
Event logging	USE master execute sp_configure 'event logging', 1 RECONFIGURE
Objects not owned by dbo	USE <!--DATABASE--!> DROP TABLE <!--DATABASE--!>.<!-- OWNER--!>.<!--OBJECT--!>
Remote access allowed	USE master sp_configure 'allow remote access', 0 RECONFIGURE

Roles revoked from the sa login	<pre>USE master REVOKE ROLE sa_role FROM sa REVOKE ROLE sso_role FROM sa REVOKE ROLE oper_role FROM sa REVOKE ROLE sybase_ts_role FROM sa</pre>
List resource limits	<pre>USE <!--DATABASE--!> sp_add_resource_limit <!--LOGIN--!>, <!-- APPLICATION--!>, <!--RANGE--!>, <LIMIT TYPE>, <!--LIMIT--!> <, <ENFORCED> <, <ACTION> <, <SCOPE> >>></pre>
Start mail session	<pre>USE master execute sp_configure 'start mail session', 0 RECONFIGURE</pre>
Unified login required	<pre>USE master sp_configure 'unified login required', 1 sp_configure 'use security services', 1 RECONFIGURE</pre>
Allow sendmsg	<pre>USE master execute sp_configure 'allow sendmsg', 0 RECONFIGURE</pre>
Orphaned user	<pre>USE master sp_dropuser '<!--USERNAME--!>' sp_droplogin '<CORRESPONDING LOGIN>' sp_addlogin '<CORRESPONDING LOGIN>', <LOGIN PASSWORD> sp_adduser '<CORRESPONDING LOGIN>', '<!--USERNAME--!>'</pre>
Secure default login exists	<pre>USE master execute sp_configure 'secure default login', 0, '' RECONFIGURE</pre>

Roles without passwords	USE master ALTER ROLE <!--ROLE--!> ADD PASSWD <NEW PASSWORD>
Require message confidentiality with encryption	USE master execute sp_configure 'msg confidentiality reqd', 1 execute sp_configure 'use security services', 1 RECONFIGURE
Event log computer name	USE master sp_configure 'event log computer name', 0, '<YOUR SERVER NAME>'
Use security services	USE master sp_configure 'use security services', 1 RECONFIGURE
Default SAP password"USE master	sp_password <CURRENT PASSWORD>, <NEW PASSWORD>, <!--LOGIN--!>
Audit queue size	USE master sp_configure 'audit queue size', <NEW VALUE>
Log audit logon success	USE master sp_configure 'log audit logon success', 1 RECONFIGURE
Default password for PortalAdmin	USE master sp_password <CURRENT PASSWORD>, <NEW PASSWORD>, 'PortalAdmin'
Default password for pkiuser	USE master sp_password <CURRENT PASSWORD>, <NEW PASSWORD>, 'pkiuser'
Password same as login name	USE master sp_password <CURRENT PASSWORD>, <NEW PASSWORD>, <!--LOGIN--!>

Guest user exists in database	USE <!--DATABASE--!> sp_dropuser guest
System-wide password expiration	USE master sp_configure 'systemwide password expiration', 90 RECONFIGURE
Audit logout not set	USE master sp_auditooption 'logouts', <CHOOSE 'on' 'off'> sp_audit 'logout', 'all', 'all', <CHOOSE 'on' 'fail' 'pass'>"
Permission granted on system table	USE <!--DATABASE--!> REVOKE SELECT ON <!--DATABASE--!>.<!--OWNER--!>.<!--OBJECT--!> FROM <!--GRANTED TO--!>
xp_cmdshell not removed	USE master sp_dropextendedproc xp_cmdshell
Permission to select from syslogins	USE master REVOKE <!--PRIVILEGE--!> ON master.dbo.syslogins FROM <!--GRANTED TO--!>
xp_cmdshell context	USE master sp_configure 'xp_cmdshell context', 1 RECONFIGURE
Current audit table	USE master sp_configure ""current audit table"", <CURRENT AUDIT TABLE> <, ""with truncate"">
Minimum password length	USE master sp_configure 'minimum password length', <NEW VALUE>

Maximum failed logins	USE master sp_configure 'maximum failed logins', <NEW VALUE>
Check password for digit	USE master sp_configure 'check password for digit', 1 RECONFIGURE
Default password for PIAdmin	USE master sp_password <CURRENT PASSWORD>, <NEW PASSWORD>, 'PIAdmin'
Updates allowed to system tables	USE master sp_configure 'allow updates to system tables', 0 RECONFIGURE

IBM DB2 FIX SCRIPTS

Check	Script
Permissions to list users	<pre> REVOKE CONTROL ON <!--TABLE NAME--!> TO PUBLIC REVOKE ALTER ON <!--TABLE NAME--!> TO PUBLIC REVOKE DELETE ON <!--TABLE NAME--!> TO PUBLIC REVOKE INDEX ON <!--TABLE NAME--!> TO PUBLIC REVOKE INSERT ON <!--TABLE NAME--!> TO PUBLIC REVOKE SELECT ON </pre>
Permissions granted to PUBLIC	<pre> REVOKE <!--PRIVILEGE--!> FROM publicthx </pre>
Permissions granted to PUBLIC	<pre> REVOKE <!--PRIVILEGE--!> ON <!--TABLE--!> FROM public </pre>
Permissions granted to PUBLIC	<pre> REVOKE <!--PRIVILEGE--!> ON <!--SCHEMA-- !> FROM public </pre>
CREATE_NOT_FENCED privilege granted	<pre> REVOKE CREATE_NOT_FENCED ON DATABASE FROM PUBLIC REVOKE CREATE_NOT_FENCED ON DATABASE FROM USER <!--GRANTED TO--!> REVOKE CREATE_NOT_FENCED ON DATABASE FROM GROUP <!--GRANTED TO-- !> </pre>
Permissions granted to PUBLIC	<pre> REVOKE <!--PRIVILEGE--!> ON <!--INDEX--!> FROM public </pre>
Permissions granted to PUBLIC	<pre> REVOKE <!--PRIVILEGE--!> ON <!--COLUMN- !> FROM public </pre>

Check	Script
Permissions to list users	REVOKE CONTROL ON <!--TABLE NAME--!> TO PUBLIC REVOKE ALTER ON <!--TABLE NAME--!> TO PUBLIC REVOKE DELETE ON <!--TABLE NAME--!> TO PUBLIC REVOKE INDEX ON <!--TABLE NAME--!> TO PUBLIC REVOKE INSERT ON <!--TABLE NAME--!> TO PUBLIC REVOKE SELECT ON
Auditing buffer size	UPDATE DATABASE MANAGER CONFIGURATION USING AUDIT_BUF_SZ <NEW VALUE>
Permissions granted to user	REVOKE <!--PRIVILEGE--!> ON INDEX <!-- INDEX--!> FROM <!--GRANTED TO--!>
Permissions granted to user	REVOKE <!--PRIVILEGE--!> ON SCHEMA <!-- SCHEMA--!> FROM <!--GRANTED TO--!>
Permissions granted to user	REVOKE <!--PRIVILEGE--!> ON <!--TABLE--!> FROM <!--GRANTED TO--!>
Permissions granted to user	REVOKE <!--PRIVILEGE--!> FROM <!-- GRANTED TO--!>
AUTHENTICATION parameter type	UPDATE DBM CFG USING AUTHENTICATION <NEW METHOD>
AUTHENTICATION parameter set to DCS	UPDATE DBM CFG USING AUTHENTICATION DCS_ENCRYPT

Check	Script
Permissions to list users	<pre> REVOKE CONTROL ON <!--TABLE NAME--!> TO PUBLIC REVOKE ALTER ON <!--TABLE NAME--!> TO PUBLIC REVOKE DELETE ON <!--TABLE NAME--!> TO PUBLIC REVOKE INDEX ON <!--TABLE NAME--!> TO PUBLIC REVOKE INSERT ON <!--TABLE NAME--!> TO PUBLIC REVOKE SELECT ON </pre>
Permissions on system catalog	<pre> REVOKE CONTROL ON <!--TABLE NAME--!> TO PUBLIC REVOKE ALTER ON <!--TABLE NAME--!> TO PUBLIC REVOKE DELETE ON <!--TABLE NAME--!> TO PUBLIC REVOKE INDEX ON <!--TABLE NAME--!> TO PUBLIC REVOKE INSERT ON <!--TABLE NAME--!> TO PUBLIC REVOKE SELECT ON </pre>
AUTHENTICATION parameter set to SERVER	<pre> UPDATE DBM CFG USING AUTHENTICATION SERVER_ENCRYPT </pre>
AUTHENTICATION parameter set to CLIENT	<pre> UPDATE DBM CFG USING AUTHENTICATION SERVER_ENCRYPT </pre>
Permissions granted to user	<pre> REVOKE <!--PRIVILEGE--!> ON <!--COLUMN- !> FROM <!--GRANTED TO--!> </pre>

MYSQL FIX SCRIPTS

Check	Script
Easily-guessed root password	UPDATE user SET Password=PASSWORD('<NEW PASSWORD>') WHERE user='root'; FLUSH PRIVILEGES;
FILE privileges granted	REVOKE FILE ON *.* FROM ' <!--USER--!>'@' <!--HOST--!>'; FLUSH PRIVILEGES;
PROCESS privileges granted	REVOKE PROCESS ON *.* FROM ' <!--USER--!>'@' <!--HOST--!>'; FLUSH PRIVILEGES;
Password for user same as username	UPDATE user SET Password=PASSWORD('<NEW PASSWORD>') WHERE user=' <!--USER--!>'@' <!--HOST--!>'; FLUSH PRIVILEGES;
Sample database not removed	DROP DATABASE <!--SAMPLE DATABASE--!>
Easily-guessed account passwords	UPDATE user SET Password=PASSWORD('<NEW PASSWORD>') WHERE user=' <!--USER--!>'@' <!--HOST--!>'; FLUSH PRIVILEGES;
Blank root password	UPDATE user SET Password=PASSWORD('<NEW PASSWORD>') WHERE user='root'; FLUSH PRIVILEGES;
Default passwords for test accounts	REVOKE ALL ON *.* FROM ' <!--USER--!>'@' <!--HOST--!>'; DELETE FROM user WHERE User=' <!--USER--!>'@' <!--HOST--!>'; FLUSH PRIVILEGES;

Blank account passwords	<pre>UPDATE user SET Password=PASSWORD('<NEW PASSWORD>') WHERE user='<!--USER--!!>'@'<!-- HOST--!!>'; FLUSH PRIVILEGES;</pre>
Anonymous user exists	<pre>DELETE FROM mysql.user WHERE User = '<!-- USER--!!>'@'<!--HOST--!!>';</pre>

Appendix L: Check Point Logging Properties Installation

AppDetectivePro 5.0 and greater includes new functionality that forwards AppDetectivePro Pen Test and Audit results to a Check Point® Event Logging Server (SmartCenter Server™). This appendix explains how to enable this functionality in AppDetectivePro, and send events to your Check Point SmartCenter Server.

This appendix consists of the following topics:

- Environment
- Check Point Setup
- AppDetectivePro Setup
- Testing AppDetectivePro Integration with Check Point.

Environment

You must install or obtain the following:

- AppDetectivePro 5.0 or greater, which includes `Opsec_Pull_Cert.exe` and `Opsec_putkey.exe`
- Check Point NG™ .

Check Point Setup

This topic explains how to prepare the Check Point server to receive log events from the AppDetectivePro host.

To set up Check Point:

Step	Action
1	<p>The Check Point suite includes a firewall. Subsequently, you must create a:</p> <ul style="list-style-type: none"> • firewall policy that accepts AppDetectivePro traffic. The policy should allow the traffic between AppDetectivePro node and the Check Point node. • rule that allows the service <code>FW1_e1a</code> (TCP port 18187). The service <code>FW1_ica_pull</code> (TCP port 18210) is needed to allow the <code>opsec_pull_cert</code> in Step 6, below. <p>After creating the policy, you must install the policy on the Check Point SmartDashboard.</p> <p>AppDetectivePro traffic can now reach your Check Point SmartCenter Server.</p>
2	<p>On the Check Point SmartDashboard, under the Network Objects branch in the left pane, right click Nodes > New Nodes > Host. In this example, the Check Point node is named checkpoint and the AppDetectivePro node is g-unit.</p> <p>The Host Node pop-up appears.</p>
3	<p>Do the following:</p> <ul style="list-style-type: none"> • In the Name field, enter the hostname where AppDetectivePro is installed. • Click the Get Address button. <p>Check Point populates the IP Address field.</p> <ul style="list-style-type: none"> • Click the OK button.
4	<p>On the Check Point SmartDashboard, under the Servers and OPSEC Applications branch in the left pane, right click OPSEC Applications and choose OPSEC Application.</p> <p>The OPSEC Application Properties pop-up appears.</p>

Step	Action
5	<p>Do the following:</p> <ul style="list-style-type: none"> • In the Name field of the OPSEC Application Properties pop-up, enter a name for the object (for example, <code>ela_client2</code>). You will need this in Step 6. • Use the Host drop-down to select the node where AppDetectivePro is installed (i.e., g-unit). • In the Client Entities section, check ELA. • Click the Communications button. <p>The Communication pop-up appears.</p> <ul style="list-style-type: none"> • Enter your activation key in the Activation Key field. • Confirm your activation key in the Confirm Activation Key field. • Click the Initialize button. • Click the Close button.
6	<p>Retrieve a certificate from Check Point's internal Certificate Authority (CA).</p> <ul style="list-style-type: none"> • On the AppDetectivePro host (for example, g-unit), open a command prompt window. • Change the directory to the Check Point folder under which AppDetectivePro is installed. Make sure utility <code>opsec_pull_certificate.exe</code> is there. • Enter: <code>opsec_pull_cert -h host -n object_name -p password</code> <p>where:</p> <ul style="list-style-type: none"> - <code>host</code> is the location where Check Point is installed. - <code>object_name</code> was created in Step 5. - <code>password</code> was created in Step 6. <p>Communication is established. Check Point is now ready to receive events from AppDetectivePro.</p>

AppDetectivePro Setup

On the AppDetectivePro side, you must enable the sending of events to Check Point after a Pen Test or Audit.

To set up AppDetectivePro to send events to Check Point after a Pen Test or Audit:

Step	Action
1	In AppDetectivePro, choose Edit > Properties . The Properties dialog box appears.
2	Check Enable Checkpoint SmartCenter Server logging .

Step	Action
3	<p>Configure the following parameters:</p> <ul style="list-style-type: none"> • Authentication Type. By default, Check Point servers use SSLCA to communicate with their objects. However, you can use this drop-down to select Clear Text, if necessary. <p>Contact Check Point Tech Services for assistance with changing the ELA server to accept clear connections. SIC Name and the P12 Key File, explained below, are only needed if you select SSLCA.</p> <ul style="list-style-type: none"> • Target Server IP Address. Enter the hostname or IP address where the Check Point SmartCenter Server is located. • Target Server Port. By default, a Check Point SmartCenter Server uses port 18187. • Target SIC Name. To locate the target Secure Internal Communication (SIC) name (example: <code>cn=cp_mgmt,o=checkpoint.abc.com.48tcd4</code>): <ul style="list-style-type: none"> -Under the Network Objects branch (in the left pane of the Check Point SmartDashboard), double click the Check Point node to display its properties. -Copy the value in the DN field (Secure Internal Communication portion). -Paste the value into the Target SIC Name field in the AppDetectivePro Properties dialog box. • Client SIC Name. To locate the target Secure Internal Communication (SIC) name: <ul style="list-style-type: none"> -Under the Servers and OPSEC Applications branch (in the left pane of the Check Point SmartDashboard), double click the node to which AppDetectivePro is mapped to display its properties. -Copy the value in the DN field (Secure Internal Communication portion). -Paste the value into the Target SIC Name field in the AppDetectivePro Properties dialog box. • P12 Key File. Specify the location of the .p12 file that was generated when you executed the <code>opsec_pull_cert.exe</code>; for more information, see Step 6 in Check Point Setup. By default, this file should be located under the directory where AppDetectivePro is installed.
4	<p>Click OK.</p> <p>AppDetectivePro PenTest or Audit results are sent to Check Point.</p>

Step	Action
5	<p>On the SmartDashboard:</p> <ul style="list-style-type: none"> • Choose Policy > Install. • Select the Check Point target. • Click the OK button. <p>You can use the Check Point SmartView Tracker to view all AppDetectivePro event logs.</p>

Testing AppDetectivePro Integration with Check Point

To test AppDetectivePro integration with Check Point:

Step	Action
1	<p>Do the following:</p> <ul style="list-style-type: none"> • Create an AppDetectivePro query. • Right-click the Product field. • On the Product Filter pop up, add Equal to AppDetectivePro.
2	<p>Save the custom query, by choosing Query > Save As... and entering: AppDetectivePro.</p>

Appendix M: Customizing Reports with Your Company Logo

This appendix explains how to customize your AppDetectivePro reports. Specifically, it explains how to replace the default Application Security Inc. logo with your company logo. This appendix consists of the following topics:

- Assumptions
- Customizing Reports with Your Company Logo.

Assumptions

This appendix assumes you have a working installation of AppDetectivePro, which you can download from the Application Security, Inc. website (www.appsecinc.com). You can evaluate a fully-functional version of AppDetectivePro for 30 days without obligation. AppDetectivePro

Customizing Reports with Your Company Logo

To customize reports with your company logo:

Step	Action
1	Choose Edit > Properties from the menu. The Properties dialog box appears.
2	Click the Reports branch in the left tree view. The Reports portion of the Properties dialog box appears.
3	Check Select a logo for use on the reports .
4	Click the Browse button. The Save As pop-up appears.

Step	Action
5	Locate your logo image file (.bmp format only) and click the Save button. Your selected image file name displays in the Company Logo field of the Properties dialog box. AppDetectivePro automatically resizes your image to fit in the Crystal Reports format. However, in HTML reports your image displays as the actual size. Application Security, Inc. recommends a pixel size of 154 x 46 for HTML, and 278 x 54 for Crystal Reports.
6	Click OK . Your AppDetectivePro reports display your company logo.

Appendix N: Integrating a Custom Dictionary to Uncover Easily-Guessed Passwords

This appendix explains how to integrate a customized dictionary into AppDetectivePro in order to uncover easily-guessed passwords during a Pen Test or Audit of your applications.

EXAMPLE

This appendix describes an example of integrating a dictionary of Spanish words (which can be obtained for free from the Web) to create an Audit Policy that employs a check to uncover easily-guessed Spanish passwords. You can replicate this example whether you are using your own password dictionary in a different language, or a Policy that employs multiple checks.

This appendix consists of the following topics:

- Assumptions
- Sample Database and Dictionary Used
- Creating a New Policy and Integrating a Custom Dictionary
- Using Your New Custom Dictionary Policy.

Assumptions

This appendix assumes you have a working installation of AppDetectivePro, which you can download from the Application Security, Inc. website (www.appsecinc.com). You can evaluate a fully-functional version of AppDetectivePro for 30 days without obligation.

Sample Database and Dictionary Used

The example in this appendix uses:

- Microsoft SQL Server for the database
- a Spanish word list for the custom dictionary file.

Creating a New Policy and Integrating a Custom Dictionary

To create a new Policy and integrate a custom dictionary:

Step	Action
1	<p>Do one of the following:</p> <ul style="list-style-type: none"> • choose Edit > Policies from the menu • click the Policy button on the toolbar • press <CTRL>+L. <p>The Policies dialog box appears. The Pen Test Policies tab is selected by default.</p> <ul style="list-style-type: none"> • Click the Audit Policies tab. <p>Your built-in and user-defined Audit Policies display.</p>
2	<p>Click the New Policy button.</p> <p>The Policy Editor page appears. The Oracle tab is selected by default. Oracle checks display in the left pane.</p>
3	<p>Click the Microsoft SQL Server tab.</p> <p>Microsoft SQL Server checks display in the left pane.</p>

Step	Action
4	Click the + icon next to the Identification/Password Control category. The category expands to display each Identification/Password Control check.
5	Check Easily-guessed password . Easily-guessed password check details (for example, title, description, summary, etc.) display in the right pane.
6	Enable the check by checking Check Enabled .
7	Select Dictionary Name .
8	Click the Browse button. The Open pop-up appears.
9	Do the following: <ul style="list-style-type: none">• Locate your dictionary file (for example, C:\dictionary\spanish.txt).• Click the Open button. The dictionary file path/name displays in the Dictionary Name field.
10	Do the following: <ul style="list-style-type: none">• Click the Save button. The Save New Policy pop-up appears. <ul style="list-style-type: none">• Enter the Policy name in the Policy Name: field (required), for example, Spanish Dictionary Audit.• Enter a Policy description in the Policy Description: field (optional).• Click the OK button.

Using Your New Custom Dictionary Policy

To use your new custom dictionary Policy:

Step	Action
1	<p>In the network tree view of the AppDetectivePro main page, click the + icons to expand the nodes and display all the applications.</p> <p>Prerequisite: You must have a previous Session loaded, or you must create a new Session.</p>
2	<p>Right click the application you want to Audit with your new Policy. A drop-down list appears.</p>
3	<p>Choose Audit With... > Spanish Dictionary Audit.</p> <p>The Run Audit dialog box appears. Your selected Policy (Spanish Dictionary Audit) displays in the Policy to use: drop-down.</p>
4	<p>Do the following:</p> <ul style="list-style-type: none"> • Click the Audit Information column header. <p>The Connection Details pop-up appears.</p> <ul style="list-style-type: none"> • Enter the user name and password to perform the Audit under. • Click the OK button.
5	<p>Click the Run Audit button.</p> <p>The ASI Engine dialog box displays as the Audit runs, allowing you to monitor Audit progress. When the Audit is complete, detected vulnerabilities display in the vulnerability view of the AppDetectivePro main page, as well as in the main view (when you click the Details tab).</p>
6	<p>To view additional details, click the vulnerability in the vulnerability view of the AppDetectivePro main page.</p> <p>The Vulnerability Info pop-up displays detailed vulnerability information.</p>

Appendix O: Oracle Critical Patch Update Detection

This appendix explains the different methods AppDetectivePro uses to detect if the Oracle Critical Patch Update (CPU) has been applied to your Oracle database.

This appendix consists of the following topics:

- Java Method
- OS Method
- Legacy Patch Detection
- Patches_History.txt Method for Oracle CPU Collection on OpenVMS
- REGISTRY\$HISTORY Table Method.

Java Method

Important!	AppDetectivePro does not support the Java Method for January 2006 and newer Oracle CPU checks. Instead, AppDetectivePro supports the REGISTRY\$HISTORY CPU detection method for all Oracle CPU checks January 2006 and newer Oracle CPU checks (when no OS credentials are supplied). For more information on the REGISTRY\$HISTORY CPU detection method, see REGISTRY\$HISTORY Table Method.
-------------------	--

The Java Method is new functionality added to AppDetectivePro 5.1.5 and greater. This new method uses existing Java configured on the target database server to collect the OPatch data. AppDetectivePro requires Java Virtual Machine (JVM) on the target database server, as well as the following privileges, in order to use the method correctly:

- JAVASYSPRIV
- CREATE PROCEDURE.

You can run the commands below to grant these privileges:

- `grant JAVASYSPRIV to <username>`
- `grant CREATE PROCEDURE to <username>.`

Caution! Java XML is required to use the Java Method. Some custom scripts used to install JVM may not include Java XML (initxml.sql and xmlja.sql scripts).

By default, AppDetectivePro uses the OS (Operating System) Method to detect if the Oracle CPU has been applied to your Oracle database; for more information, see OS Method. The Java Method uses Oracle Java Stored Procedures to connect to the operating system, and then reviews the OPatch files to detect which CPUs have been installed.

To enable the use of the Java Method:

Step	Action
1	Choose Edit > Properties . The Properties dialog box appears.
2	Click the Pen Testing/Auditing branch.
3	Click the Oracle tab.
4	Select Use Java method .
5	Click the OK button.

Using the Java Method creates the following database objects: a Java source and function. AppDetectivePro deletes these objects as soon as AppDetectivePro completes the Audit. If an error occurs during the Audit, it is probably because the operating system user lacks the aforementioned permissions.

In addition, you can only use the Java Method on versions of Oracle 9iR2 and above, where CPUs have been applied to the database using OPatch.

OS Method

By default, AppDetectivePro uses the OS (Operating System) Method to detect if the Oracle CPU has been applied to your Oracle database. This method requires you to supply OS credentials, in addition to a valid database account.

The OS Method uses:

- telnet or SSH to connect to the operating system, then reviews the OPatch files to detect which CPUs have been installed
- Windows Administrative shares, such as `C$` and `D$`, to connect to the operating system for the Windows platforms.

Note:	For more information on Oracle OS credential requirements, see Operating System Considerations (for Audits) in Appendix G: Audit and User Rights Review Privileges.
--------------	---

	Also note, the OS Method only applies to version of Oracle 9iR2 and above, where CPUs have been applied to the database using OPatch.
--	---

If you encounter an error when running an Audit, verify the following:

- You have supplied the proper user name and password.
- The operating system user has the proper `ORACLE_HOME` set.
- The operating system user has permission to access `ORACLE_HOME`.

Legacy Patch Detection

For versions of Oracle 8i and 9iR1, AppDetectivePro performs its own method of examining whether the CPU is applied on the target database. This method, Legacy Patch Detection, also requires for you to supply OS credentials, in addition to having a valid database account.

Legacy Patch Detection uses telnet or SSH to connect to the operating system and then reviews various attributes such as files dates and sizes to tell what patches have been installed.

If you encounter an error when running an Audit, verify the following:

- You have supplied the proper user name and password.
- The operating system user has the proper `ORACLE_HOME` set.
- The operating system user has permission to access `ORACLE_HOME`.

Patches_History.txt Method for Oracle CPU Collection on OpenVMS

Oracle CPU checks on OpenVMS work the same way as they do on other platforms. AppDetectivePro includes a feature that looks up a local copy of the CPU history file. This is called `comps.xml` on most platforms, but on OpenVMS the file is called `patches_history.txt`.

The `patches_history.txt` file is located under the `PATCHES` subdirectory of `ORACLE_HOME` on the target OpenVMS server. The `patches_history.txt` contains information about installed and de-installed patches.

AppDetectivePro uses an existing copy instead of collecting files remotely. After the CPU check finishes, AppDetectivePro renames the local file (with a `.bak` extension) so it won't be used next time.

CPU DATA COLLECTION

When AppDetectivePro executes the CPU check against an OpenVMS server, you can select one of two CPU data collection methods:

- **Java method.** The Oracle database account requires the same privileges as required for the Java method on other platforms. For more information, see Java Method.

- **OS method.** As opposed to other platform, on OpenVMS the OS account **must** have *at least* one of the following:
 - ORACLE_HOME logical defined
 - actual `oratab` file in home directory
 - listener banner containing `PRMFILE` string.

AppDetectivePro uses this information to extract the `ORACLE_HOME` path.

USING A LOCAL FILE FOR AN ORACLE CPU CHECK ON AN OPENVMS SERVER

If you cannot Telnet/SSH to a remote OpenVMS server, you can use a local file for to perform your Oracle CPU check.

To do so, you must place a copy of the `patches_history.txt` file under the AppDetectivePro installation directory -- specifically, under the `\mirror\<IP>\<PORT>\<SID>\PATCHES` directory. For example, if the address of your OpenVMS server is `192.168.1.1`, and there is Oracle database on port `1521` with the SID `sales`, then the path is: `\mirror\192.168.1.1\1521\sales\PATCHES` (under the AppDetectivePro installation directory).

If the `\mirror\192.168.1.1\1521\sales\PATCHES\patches_history.txt` exists, then AppDetectivePro parses this file, and uses *it* (instead of performing a Telnet/SSH to the remote OpenVMS server). When AppDetectivePro completes the Audit, it changes the file name by appending `.bak`, to avoid confusion in the future.

REGISTRY\$HISTORY Table Method

For CPUs dated January 2006 and later, AppDetectivePro supports the `REGISTRY$HISTORY` CPU detection method. This method checks information in the `SYS.REGISTRY$HISTORY` table to determine whether a CPU was applied.

This method only requires '`SELECT on SYS.REGISTRY$HISTORY`' rights. This method does not require OS or JAVA credentials, but is considered less accurate in certain cases.

Appendix P: Migrating Your Back-End Database

This appendix explains how to migrate your Microsoft SQL Server or Microsoft Access back-end database from one machine to another. It consists of the following topics:

- Migrating a Microsoft Access Back-End Database
- Migrating a Microsoft SQL Server Back-End Database.

Migrating a Microsoft Access Back-End Database

To migrate a Microsoft Access back-end database from one machine to another:

Step	Action
1	Back up and copy the AppDetective.mdb file on your <i>old</i> AppDetectivePro machine.
2	Install AppDetectivePro on a <i>new</i> machine, and update it to the <i>exact same version</i> of as your old AppDetectivePro.
3	Place the old AppDetective.mdb file that you backed-up/copied from your <i>old</i> AppDetectivePro machine (in Step 1), and replace the existing AppDetective.mdb file that is on your <i>new</i> machine. The file is located by default in the following folder: <code><installation directory>\Program Files\AppSecInc\AppDetective</code> .

Migrating a Microsoft SQL Server Back-End Database

To migrate a Microsoft SQL Server back-end database from one machine to another:

Step	Action
1	Back up the AppDetectivePro database on the Microsoft SQL Server instance where it's installed (i.e., your <i>old</i> AppDetectivePro machine).
2	Install AppDetectivePro on a <i>new</i> machine, and update it to the <i>exact same version</i> of as your old AppDetectivePro.

Step	Action
3	<p>If your <i>new</i> installation of AppDetectivePro:</p> <ul style="list-style-type: none"> • uses the same credentials and settings as the <i>old</i> installation, you can restore the backup on your new AppDetectivePro database. • is on a new Microsoft SQL Server instance, then you must: <ul style="list-style-type: none"> -Copy/place the AppDetectivePro database on the <i>new</i> instance. -Run <code>apprepair.exe</code> located by default in the following folder: <code><installation directory>\Program Files\AppSecInc\AppDetective</code> -Click the Repair ODBC button. -Specify your new Microsoft SQL Server instance and the proper authentication credentials. -Click the OK button.

Appendix Q: Understanding System Auditing

AppDetectivePro also includes [System Auditing](#), an audit tracing component that tracks user actions (events). These events are logged to a log file and in the Windows Event Log. You can modify the [System Auditing](#) settings under the [Tracing](#) branch in the Properties dialog box. Specifically, you can:

- log events into a log file
- log events into the Windows Event Log
- turn off System Auditing.

For more information, see *Properties*.

This appendix explains in more detail how System Auditing works in AppDetectivePro. It consists of the following topics:

- What Events are Logged?
- What Information is Stored When an Event is Logged?
- How Do I View the Logs?

What Events are Logged?

The following events are logged:

- **Session Creation**
- **Discovery Performed (included scheduled)**
- **Application Addition/Removal**
- **Pen Test Performed (included scheduled)**
- **Audit Performed (included scheduled)**
- **Risk Level Modification**
- **Policy Creation**
- **Exception Creation/Edit/Deletion**
- **Policy Edited**
- **Export/Import/Purge Session**
- **Export/Import/Purge Policy**
- **ASAP Update Performed (included scheduled)**
- **Fix Script Creation**
- **Report Creation**
- **User-Defined Check Creation/Edit/Deletion**
- **Properties Edited**
- **Scheduled Job Addition/Deletion**
- **Sessions Merged**
- **Sessions Renamed**
- **Vulnerability Suppression**
- **System Auditing Turned On**
- **System Auditing Turned Off.**

What Information is Stored When an Event is Logged?

Each event is logged with the following information:

- **Date and Time**
- **Event Type**
- **Success or Failure**
- **User Name.**

How Do I View the Logs?

The log file used to store System Auditing events is `SystemAuditing.log`, and is placed in the `logs` folder of AppDetectivePro. This file is never deleted by AppDetectivePro.

You can view System Auditing events stored in the Windows Event Log with the Event Viewer provided by Microsoft Windows. Events are stored under the Application category, with the source AppDetectivePro.

Appendix R: Updating Your Back-End Database from Microsoft SQL Server 2000 to Microsoft SQL Server 2005 or Microsoft SQL Server 2008

To update your back-end AppDetectivePro database from Microsoft SQL 2000 to Microsoft SQL 2005 or Microsoft SQL 2008:

Step	Action
1	Download the AppDetectivePro setup file (for example, appdetective_setup.exe) to a local folder. This appendix only explains how to update your back-end AppDetectivePro database, not how to install AppDetectivePro. For more information on AppDetectivePro installation, see <i>Installing/Configuring AppDetectivePro (and the Database and SHATTER Knowledgebase Components)</i> .
2	Go to the local folder where AppDetectivePro setup file is saved, and run the following command: <pre>appdetective_setup.exe /extractcab</pre> This command extracts the installers for all AppDetectivePro components installed in the <code>/Support</code> folder (under the local folder where you saved the AppDetectivePro setup file).
3	Locate the following installer files: <ul style="list-style-type: none"> • Database Component installer (DatabaseInstaller.msi) • SHATTER Knowledgebase Component installer (DataComponent.msi). You will need these files in Step 6.

Step	Action
4	Back up your Microsoft SQL 2000 AppDetectivePro back-end database.
5	Uninstall your Microsoft SQL 2000 back-end database; for more information, see Steps 2-3 in <i>Uninstalling AppDetectivePro (and the Database and SHATTER Knowledgebase Components)</i> , and <i>Deleting the AppDetectivePro Back-End Database</i> .
6	<p>Create a new AppDetectivePro back-end database.</p> <p>Go to the /Support folder (described in Step 2).</p> <ul style="list-style-type: none">• Double click the Database Component installer file (DatabaseInstaller.msi) to install the back-end database schema.• Double click the SHATTER Knowledgebase Component installer file (DataComponent.msi) to install the back-end database data. <p>During the new back-end database installation, make sure you point to your new Microsoft SQL 2005 or 2008 instance.</p>
7	Move your backup copy of the AppDetectivePro back-end database (from Step 4) to the server hosting your new Microsoft SQL 2005 or 2008 instance.
8	Restore your backup copy of the AppDetectivePro database (from Step 4) to your Microsoft SQL 2005 or 2008 Microsoft SQL server.

Appendix S: Dynamic Shell Prompt Handling

This appendix consists of the following topics:

- Dynamic Shell Prompt Handling in AppDetectivePro

Dynamic Shell Prompt Handling in AppDetectivePro

Some shells allow you to set a *dynamic* prompt string that the shell interprets before it prints each prompt. Special character sequences in the prompt allow you to include variables like the current directory, date and time, username, hostname, and more. Your shell's manual page should list these at the PS1 or prompt variable. (If you use the Korn shell or the original C shell, you don't have these special sequences.)

However, certain dynamic prompt strings -- such as "history number of commands" -- can cause the prompt to increase in number with each command (201, 202, etc). AppDetectivePro only processes *constant* shell prompts (for example, \$ and #), not dynamic, and can time-out waiting for the wrong prompt.

Below is an example of the problematic dynamic component in a shell prompt, where the Session prompt increases numerically with each command (201, 202):

```
wledeagle_Ora10g_eagle (201) >  
wledeagle_Ora10g_eagle (202) >
```

There are two known workarounds:

- **Force AppDetectivePro to use a specific Session prompt, that disregards the incremental number.** Use the **Session Prompt:** field in the **Connection Details** dialog box to specify the Session prompt that AppDetectivePro should use to connect via Telnet/SSH (rather than relying on AppDetectivePro to locate the Session prompt automatically in the login banner after connecting).

In the example above, you would enter `wledeagle_Ora10g_eagle` in the **Session Prompt:** field in the **Connection Details** dialog box. For more information, see *Understanding the Connection Details Dialog Box*.

- Change shell profile settings for the OS audit user to have a static shell prompt (default on the Solaris OS).

Appendix T: AppDetectivePro Application Log Files and Installation/Upgrade Log Files

This appendix consists of the following topics:

- AppDetectivePro Application Log Files
- AppDetectivePro Installation/Update Log Files.

AppDetectivePro Application Log Files

As explained in the *View Menu* sub-topic, you can click [View > Log Files](#) to display the [AppDetectivePro - Log Viewer](#) window and collect/open application log files.

Note:	For information on the Installation/Upgrade Log Files , see AppDetectivePro Installation/Update Log Files .
--------------	--

When you select the [Application Log Files](#) tab on the [AppDetectivePro - Log Viewer](#) window, you can specify a destination folder and collect available application log files. You can also double-click any individual application log file to view its contents in Notepad.

The **Browse** button on the [AppDetectivePro - Log Viewer](#) window allows you to specify a non-default directory for application log file collection. **This is the recommended method of application log file collection.**

The user running AppDetectivePro **must** have required privileges to be able to copy the collected log files to the specified location.

Hint:	To maximize the number of generated log files and data to send to Application Security, Inc. Support for troubleshooting, you should run a Discovery, Pen Test, Audit, or User Rights Review before collecting log files.
--------------	---

Application log files are stored **by default** in: `<%USERPROFILE%>\<%Local Application Data%>\AppSecInc\AppDetective\logs\ApplicationLogs_<timestamp>` (for example, `C:\Documents and Settings\<UserName>\Local Settings\Application Data\AppSecInc\AppDetective\logs\ApplicationLogs_20090921_220607`).

You can run the command `echo %USERPROFILE%` to determine the name and location of your `USERPROFILE` directory. `%Local Application Data%` varies on different Windows versions. For example, on Windows XP/2000/2003:

`C:\Documents and Settings\\Local Settings\Application Data\AppSecInc\AppDetective\logs\`. On Windows Vista/2008: `c:\Users\\AppData\Local\AppSecInc\AppDetective\logs\`

The specific, available AppDetectivePro application log files are:

- `AppDetective.exe.<PID>.log` (for example, `AppDetective.exe.4200.log`)
- `ASIEngine.exe.<PID>.log` (for example, `ASIEngine.exe.2604.log`)
- `ASIThread.exe.<PID>.log` (for example, `ASIThread.exe.1970.log`)
- `error.log` (AppDetectivePro generates this log file when it encounters a VBGuard error)
- `ScheduledJob.log` (AppDetectivePro generates this log file when you schedule or run a Job in AppDetectivePro)

AppDetectivePro Installation/Update Log Files

As explained in the *View Menu* sub-topic, you can click [View > Log Files](#) to display the [AppDetectivePro - Log Viewer](#) window and collect/open installation/upgrade log files. For information on the **Application Log Files**, see AppDetectivePro Application Log Files.

When you select the [Installation/Upgrade Log Files](#) tab on the [AppDetectivePro - Log Viewer](#) window, you can specify a destination folder and collect available installation/upgrade log files. You can also double-click any individual installation/upgrade log file to view its contents in Notepad.

The [Browse](#) button on the [AppDetectivePro - Log Viewer](#) window allows you to specify a non-default directory for installation/upgrade log file collection. **This is the recommended method of installation/upgrade log file collection.**

Important!	The user running AppDetectivePro must have required privileges to be able to copy the collected log files to the specified location.
-------------------	---

Installation/upgrade log files are stored by default in the following folders:

- `<%UserProfile%>\Local Settings\Temp` (for example, `C:\Documents and Settings\\Local Settings\Temp`)
- `<%USERPROFILE%>\<%Local Application Data%>\AppSecInc\AppDetective\logs`

You can run the command `echo %USERPROFILE%` to determine the name and location of your `USERPROFILE` directory. `%Local Application Data%` varies on different Windows versions. For example, on Windows XP/2000/2003:

`C:\Documents and Settings\\Local Settings\Application Data\AppSecInc\AppDetective\logs\`. On Windows Vista/2008: `c:\Users\\AppData\Local\AppSecInc\AppDetective\logs\`

You only have log files in this folder if you upgrade from AppDetectivePro v.5.4.4 or earlier.

`<Database installation>\Logs` (for example, `C:\Program Files\AppSecInc\Database\Logs`)

You can run the command `echo %TEMP%` to determine the name and location of your `TEMP` directory.

The specific, available AppDetectivePro installation/update log files in the `<%UserProfile%\Local Settings\Temp` folder are:

- `AsapUpdater.log`
- `AppDetectivePro_{GUID}.log` (for example, `AppDetectivePro_{60A08A66-1D4C-46A1-B43F-D9B55D408E2D}.log`)
- `AppDetectiveProInstall.log`
- `BackendInstaller_install.log`
- `DBC_install.log`
- `Data_install.log`.

Note:	You only have the <code>AsapUpdater.log</code> file if you upgrade from AppDetective v.7.1 or later by running the ASAP Updater. You only have the <code>BackendInstaller_install.log</code> file if you upgrade from AppDetective v.5.4.4 or earlier.
--------------	--

The specific AppDetectivePro installation/update log files in the `<%USERPROFILE%\<%Local Application Data%\AppSecInc\AppDetective\logs` folder are:

- `UpgradeInfo.log`
- `BackendInstaller.exe.<PID>.log` (for example, `BackendInstaller.exe.3700.log`)

You only have log files in this folder if you upgrade from AppDetective v.5.4.4 or earlier.

The specific AppDetectivePro installation/update log file in the <Database installation>\Logs folder are: all *.log files.

Appendix U: Open Ports (on Computers Running Microsoft SQL Server) Required to Run Discoveries, Pen Tests, and Audits

In order to run a Discovery, Pen Test, or Audit against a Microsoft SQL Server database, certain ports on the machine running Microsoft SQL Server must be open. This appendix consists of the following topics:

- [Open Ports \(on Computers Running Microsoft SQL Server\) Required to Run a Discovery](#)
- [Open Ports \(on Computers Running Microsoft SQL Server\) Required to Run a Pen Test](#)
- [Open Ports \(on Computers Running Microsoft SQL Server\) Required to Run an Audit](#)

Open Ports (on Computers Running Microsoft SQL Server) Required to Run a Discovery

To Discover Microsoft SQL Server on the default port:

- **TCP:** [1433](#) Microsoft SQL Server default port.
- OR:
- **UDP:** [1434](#) Microsoft SQL Monitor.

Note:	Microsoft SQL Server 2005/2008 requires the Microsoft SQL Server Browser service to run on the target server.
--------------	---

To Discover Microsoft SQL Server on a non-default port:

- **TCP:** Any port number for the default instance or named instances.
- OR:
- **UDP:** [1434](#) Microsoft SQL Monitor.

Open Ports (on Computers Running Microsoft SQL Server) Required to Run a Pen Test

TCP: 1433 Microsoft SQL Server default port or any port number for the default instance or named instances.

Open Ports (on Computers Running Microsoft SQL Server) Required to Run an Audit

To connect to Microsoft SQL Server via named pipes:

- **TCP:** 135 Service Control Manager, 445 Microsoft Directory Service, DCOM dynamic ports (1024-65535).

Note:	DCOM dynamically allocates TCP and UDP ports in the range 1024-65535.
--------------	---

To connect to SQL Server via TCP/IP:

- **TCP:** 135 Service Control Manager, 445 Microsoft Directory Service, 1433 SQL Server default port or any port number for the default instance or named instances, DCOM dynamic ports (1024-65535).

Appendix V: Uploading Comma-Delimited Text Files, CSV Files, or NMAP Files Containing IP Addresses (or IP Addresses and Ports) to Discover

As explained in Step 4 of Creating a Session, as well as Step 4 of Running a Discovery, AppDetectivePro allows you upload a standard, comma-delimited text file or CSV file containing the IP addresses that you want to Discover. The supported format for IPs only is the following:

<ip address>

<ip address>

<ip address>

For example:

192.168.1.1

192.168.1.1

192.168.1.1

As explained in Step 5 of Creating a Session, as well as Step 5 of Running a Discovery, AppDetectivePro allows you upload a standard, comma-delimited text file or NMAP file containing the IP addresses and ports that you want to Discover. The supported format for IPs and ports is the following:

<ip address>,<port>

<ip address>,<port>

<ip address>,<port>

For example:

192.168.1.1,1024

192.168.1.1,1052

192.168.1.1,1072