



AppDetectivePRO 8.9
Getting Started Guide

Legal Notice

Copyright © 2017 Trustwave Holdings, Inc.

All rights reserved. This document is protected by copyright and any distribution, reproduction, copying, or decompilation is strictly prohibited without the prior written consent of Trustwave. No part of this document may be reproduced in any form or by any means without the prior written authorization of Trustwave. While every precaution has been taken in the preparation of this document, Trustwave assumes no responsibility for errors or omissions. This publication and features described herein are subject to change without notice.

While the authors have used their best efforts in preparing this document, they make no representation or warranties with respect to the accuracy or completeness of the contents of this document and specifically disclaim any implied warranties of merchantability or fitness for a particular purpose. No warranty may be created or extended by sales representatives or written sales materials. The advice and strategies contained herein may not be suitable for your situation. You should consult with a professional where appropriate. Neither the author nor Trustwave shall be liable for any loss of profit or any commercial damages, including but not limited to direct, indirect, special, incidental, consequential, or other damages.

The most current version of this document may be obtained by contacting:

Trustwave Technical Support:

Phone: +1.866.659.9097

Email:

- dbsstacsupport@trustwave.com
- for United States Government Customers: support@trustwavegovt.com

Website: <https://www.trustwave.com/Company/Support/>

Trademarks

Trustwave and the Trustwave logo are trademarks of Trustwave. Such trademarks shall not be used, copied, or disseminated in any manner without the prior written permission of Trustwave.

Formatting Conventions

This manual uses the following formatting conventions to denote specific information.

Table 1: Formatting Conventions

FORMATS AND SYMBOLS	MEANING
Blue Underline	A blue underline indicates a Web site or e-mail address.
Bold	Bold text denotes UI control and names such as commands, menu items, tab and field names, button and checkbox names, window and dialog box names, and areas of windows or dialog boxes.
Code	Text in <code>Courier New</code> in <code>blue</code> indicates computer code or information at a command line.
Italics	Italics denotes the name of a published work, the current document, name of another document, text emphasis, or to introduce a new term.
[Square brackets]	Square brackets indicate a placeholder for values and expressions.

Notes, Tips, and Cautions



Note: This symbol indicates information that applies to the task at hand.



Tip: This symbol denotes a suggestion for a better or more productive way to use the product.



Caution: This symbol highlights a warning against using the software in an unintended manner.



Question: This symbol indicates a question that the reader should consider.

About This Document

This guide describes the basic uses of AppDetectivePRO, and helps you to run AppDetectivePRO for the first time. For further details on the functions of the application, refer to the User Guide.

Table of Contents

Legal Notice	2
Trademarks	2
Formatting Conventions	3
Notes, Tips, and Cautions	3
About This Document	4
Table of Contents	5
1 Overview	7
1.1 What are Scans?	7
1.2 What are Policies?	7
1.3 What are Sessions?.....	7
1.4 Overview of AppDetectivePRO Workflow.....	8
1.5 What's New in AppDetectivePRO 8.9.....	8
2 Before You Begin	9
2.1 Install AppDetectivePRO	9
2.1.1 Upgrade to AppDetectivePRO 8.9 from Versions Older than 8.7	10
2.1.2 Upgrade from AppDetectivePRO versions older than 8.7	10
2.1.3 Upgrade from AppDetectivePRO Versions 7.6 to Version 8.x	10
2.2 Configuring the AppDetectivePRO User	10
2.3 Supported Database Platforms.....	11
2.4 Setting Up Database Access	12
2.5 Licensing.....	12
2.5.1 Installing the License File	12
2.5.2 Online License Generator.....	13
2.6 Keeping Your Software Up-To-Date	14
2.7 Customer Support.....	14
3 Customizing Scans	15
3.1 Working with Policies	16
4 Running Scans	17
4.1 Discovery	17
4.2 Adding or Importing Assets into a Session.....	20
4.3 Editing Assets	21
4.4 Pen Tests.....	22
4.4.1 What Does a Pen Test Do to the Database?	22
4.4.2 Running a Pen Test	23
4.5 Audits	24
4.5.1 Running an Audit	24
4.6 User Rights Review	27

- 4.6.1 Running a User Rights Review..... 27
- 5 Understanding Scan Results 28**
 - 5.1 Viewing Scan History 28
 - 5.2 Viewing Scan Results 28
 - 5.3 Policy Results 29
 - 5.4 User Rights Results 31
- 6 Generating Reports 32**
 - 6.1 Additional Information 33

1 Overview

AppDetectivePRO is a database security assessment solution that allows you to identify vulnerabilities and security configuration issues, perform data access diagnostics on your system, and enables you to take corrective action on any issues you may find.

In the most basic sense, AppDetectivePRO connects to an asset (or assets), collects data about the asset(s), analyzes the collected data, and allows you to generate reports on that data.



Note: In AppDetectivePRO (and in this document), an asset is a “target” database (or data store) on the system; it is a target you intend to scan.

1.1 What are Scans?

AppDetectivePRO runs scans that collect data about the security of your system. You can run the following types of scans:

- **Discover:** Discover locates and identifies the type of assets that exist on your network.
- **Pen Test:** A Pen Test is a zero-knowledge, non-intrusive and unauthenticated scan. It performs an assessment of your system from an outside-in perspective.
- **Audit:** An Audit is an authenticated scan that requires an account with read-only privileges. It performs a deep assessment, checking the configuration of your database for known vulnerabilities and configuration issues.
- **User Rights:** User Rights Review is a deep analysis of user and role entitlements on a database. This scan analyzes database user and role privileges, enabling you to investigate—and analyze the root cause of—possible access control violations.

After identifying all specified types of assets on your network to be scanned, you can run Pen Tests, Audits, or User Rights Reviews on those assets.

1.2 What are Policies?

A policy is a grouping of security and configuration controls and checks that are used for Pen Test and Audit scans. AppDetectivePRO allows for customization of policies, but also comes with numerous built-in policies that allow you to get up and running right away.

1.3 What are Sessions?

The work you do in AppDetectivePRO is organized into Sessions. A Session is a grouping of unique assets you add to AppDetectivePRO (by running discovery scans or manually adding assets), and all of the data related to each of those assets. When you create a Session, you can give it a unique name and description to distinguish it from other Sessions.

1.4 Overview of AppDetectivePRO Workflow

Using AppDetectivePRO, you follow these basic steps:

1. Create a Session.
2. Start a new Session, or re-open an existing Session, where you will store your scan data.
3. Build a list of Assets.
4. Create a list of Assets that you will scan during the session. You build a list of Assets by running a Discovery Scan, which locates Assets on a system. You can also add or import Assets into a Session.
5. Run Scans.
6. When you have established your Session and list of Assets, you can run Pen Tests, Audits, or User Rights Review scans.
7. Review Results.
After running a scan, you can view results from within the AppDetectivePRO interface.
8. Run Reports.

After filtering results to suit your business needs, you can run reports that will display your scan results in various formats.

1.5 What's New in AppDetectivePRO 8.9

- PostgreSQL 9.3, 9.4, 9.5 & 9.6 Audits
- MongoDB 3.0, 3.2, 3.4 User Rights Reviews
- Edit checks and controls enhancements
- UX Improvements
- Performance Improvements

To see what's new in the specific version, view the Readme file installed with the specific version of the product.

2 Before You Begin

The following table lists AppDetectivePRO typical system requirements:

REQUIREMENT	MINIMUM
Operating System	<ul style="list-style-type: none"> Windows 7 SP1 (64-bit) Windows 8 (64-bit) Windows 8.1 (64-bit), Windows 10 (64-bit) Windows 2008 Server SP2 (64-bit) Windows 2008 Server R2 SP1 Windows Server 2012 Windows Server 2012 R2 Note: Even if you are an Administrator user on the host, you must run the installer using the Run as administrator option. Refer to the “Install AppDetectivePRO” section in the <i>Trustwave AppDetectivePRO User Guide</i> for more details.
Rights	<ul style="list-style-type: none"> To install AppDetectivePRO and perform an ASAP Update or upgrade of the software, you must have Administrator privileges on the Windows host.
Processor	<ul style="list-style-type: none"> Dual core processors 1.60 GHz or higher
RAM	<ul style="list-style-type: none"> 3GB or higher
Hard Drive	<ul style="list-style-type: none"> 400 MB of free disk space for installation 5GB and higher for scan data storage
Networking	<ul style="list-style-type: none"> ASAP Update requires access to the internet Scan of asset(s) require network connection access to the asset(s)
Backend Database	<ul style="list-style-type: none"> When installing AppDetectivePRO, a SQLite database will be created and will be used specifically for the AppDetectivePRO installation for storing AppDetectivePRO Session data..
Required	<ul style="list-style-type: none"> Microsoft .NET Framework 4.6
Component	<ul style="list-style-type: none"> If not installed already, then the AppDetectivePRO installer will install it.

2.1 Install AppDetectivePRO

Run the executable file as a local Windows Administrator. Use the **Run as administrator** option even if you log in as a Windows Administrator. The AppDetectivePRO installer provides the option to launch the product and open the Readme file when the installation finishes. You will see a message that you have successfully installed the application when the process has finished successfully.



Note: The backend database is created when AppDetectivePRO is started for the first time. AppDetectivePRO must be started by a local Windows Administrator in order to create the database

2.1.1 Upgrade to AppDetectivePRO 8.9 from Versions Older than 8.7

Only AppDetectivePRO 8.7 and newer can be upgraded directly to AppDetectivePRO 8.9. If upgrading from a version of AppDetectivePRO that is older than 8.7, you *must* upgrade to 8.7 first. (See section 2.1.2 below for details.)



Note: You can upgrade directly to AppDetectivePRO 8.7 from version 8.5.1 or newer.

2.1.2 Upgrade from AppDetectivePRO versions older than 8.7

Only AppDetectivePRO 8.7 and 8.8 can be upgraded directly to AppDetectivePRO 8.9. If upgrading from an installation of AppDetectivePRO that is older than version 8.7, you *must* first upgrade any version prior to 8.7 to AppDetectivePRO 8.7. Previous versions of AppDetectivePRO are available for download on the Trustwave support portal (<https://login.trustwave.com/>).



Note: Legacy versions of AppDetectivePRO that can be upgraded directly to 8.7 include version 8.4 and newer.

2.1.3 Upgrade from AppDetectivePRO Versions 7.6 to Version 8.x

If your current installed version is AppDetectivePRO 7.6 and you want to upgrade your software to version 8.x, you can do so by downloading the latest executable file from the Support Portal at <https://login.trustwave.com>.

AppDetectivePRO 8.x will not replace your installation of 7.6. This means you will not lose any of your data from version 7.6 and you can start new sessions using version 8.x.



Caution: Starting with AppDetectivePRO 8.8, Trustwave no longer supports importing sessions from the legacy version 7.6. Trustwave strongly recommends you do not install version 8.x on the same host with your installation of 7.x

2.2 Configuring the AppDetectivePRO User

At installation time, you are required to be a local Windows Administrator. This is the only user that initially gets access to the AppDetectivePRO software. To add any other Windows login, the Windows Administrator who installed the software can go to the System Settings and choose User Configuration to add any other users.



Note: It is best practice to create a local Windows user and configure it in AppDetectivePRO.

2.3 Supported Database Platforms

This section details all the supported assets AppDetectivePRO support for scanning.

DATABASE PLATFORM	SUPPORTED VERSION & FUNCTIONALITY
Oracle (SID)	Version: 12c*, 11gR2, 11gR1, 10gR2, 10gR1, 9iR2 Scan Type: Audit, Pen Test, User Rights Review *Pen Test is currently not supported for 12c.
Microsoft SQL Server (instance)	Version: 2016, 2014, 2012, 2008 R2, 2008, 2005, 2000 Scan Type: Audit, Pen Test, User Rights Review
SAP (Sybase) ASE (Data Server)	Version: 16.0, 15.7, 15.5, 15.0, 12.5 Scan Type: Audit, Pen Test, User Rights Review* *You must install the appropriate client drivers (both ODBC and ADO.NET) on your host for Audit and User Rights Review scans to function.
IBM DB2 LUW (Database)	Version: 10.5*, 10.1*, 9.7, 9.5, 9.1 *Pen Test is currently not support for version 10.5 and 10.1. Scan Type: Audit, Pen Test, User Rights Review** *You must install the appropriate runtime client drivers on your host for Audit and User Rights Review scans to function.
IBM DB2 z/OS (Subsystem)	Version: 10.1, 9.1, 8.1 Scan Type: Audit* *You must install the appropriate client/connect drivers on your host for Audit scans to function.
PostgreSQL	Version 9.3, 9.4, 9.5, 9.6 Scan Type: Audit* *You must install the appropriate client/connect drivers on your host for Audit scans to function.
MySQL (Server)	Version: 5.7, 5.6, 5.5, 5.1, 5.0 Scan Type: Pen Test, Audit* *You must install the appropriate client drivers (both ODBC and .NET) on your host for Audit scans to function.
Hadoop (Node)	Scan Type: Audit
Microsoft Azure SQL Database	Scan Type: Audit
Teradata Database*	Version: 15.10, 15, 14.10, 14 Scan Type: Audit, User Rights Review** * Pen Test is not supported. ** You must install the appropriate client drivers (both ODBC and .NET) on your host for Audit and User Rights Review scans to function.

DATABASE PLATFORM	SUPPORTED VERSION & FUNCTIONALITY
MongoDB	Version: 3.0, 3.2, 3.4 Scan Type: Audit, User Rights Review

2.4 Setting Up Database Access

To perform an Audit or User Rights Review scan, you must have user access (read-only privileges) to the asset (the target database). The following will help you properly set up the required access:

1. Confirm that you have an existing account, or create an account on the database in scope for scanning. Database User Creation Scripts are available in the following locations depending on which version of AppDetectivePRO you are using:
 - a. For versions prior to 8.5, and any 8.5 versions that have been upgraded from a previously installed version of 8.0 to 8.2:
`C:\Program Files\AppSecInc\AppDetectivePRODataComponent\Resources\ShatterKnowledgebase\UserCreationScripts`
 - b. For new installations of version 8.3 and above:
`C:\Program Files\Trustwave\AppDetectivePRODataComponent\Resources\ShatterKnowledgebase\UserCreationScripts`
2. Confirm that you have an existing OS account that grants access to the installation directory of the database (or create that OS account). More information is available in the User Guide.
3. Make sure the specific IP/Port of the databases are accessible from the scanning host where AppDetectivePRO is installed (i.e. change any firewall rules if needed).
4. Add necessary assets to AppDetectivePRO using the Discovery process, or by adding or importing assets from an existing CSV file. More information is available in the *Trustwave AppDetectivePRO User Guide*.

2.5 Licensing

The AppDetectivePRO license file specifies whether your version of AppDetectivePRO software is a trial, evaluation or production version, as well as other important license details. Trial licenses enable limited functionality in AppDetectivePRO during the trial period, and expire 30 days after you have downloaded the application. If you have an evaluation license, the license file specifies when your evaluation period ends. Requests for evaluation licenses should be sent to your Trustwave Account Manager, or by contacting us at infosales@trustwave.com. Evaluation and production license files are bound to a customer's specified host machine, and will list your machine ID number and the number of assets that can be scanned during the term of the license. To get the machine ID, go to the Licensing section in the System Settings. Copy and paste the number from the Machine ID field and provide it back to them.

After you purchase licenses of AppDetectivePRO, you will receive a temporary license via e-mail, along with instructions on how to request your permanent license.

2.5.1 Installing the License File

Once you have received a license file from Trustwave, open up AppDetectivePRO and go to the Licensing section in the System Settings. Choose 'Add a License' and browse to the .lic file you received. Once added, you will see the following information:

- Customer Name
- License Type
- Product Expiration Date
- ASAP Expiration Date
- Purchased amount of UUTs¹ for Policy Scans (Pen Test/Audit) and User Rights Scans
- Purchased amount of UUTs for IBM DB2 z/OS

Licensing

Customer Name: CloudShareADPEEnvironment
Machine ID: 139295221
Product Expiration Date: 2017-12-31
ASAP Expiration Date: 2017-12-31

[Add a License...](#) Show Expired Licenses

Feature Name	Purchased	Used	Available
AD20160119165133 (Production, 2017-12-31)			
IBM DB2 z/OS Subsystem Locations (Audit)	0	0	0
Units Under Test (UUTs) - Policy Scans (Audit/Pe...	100	5	95

To purchase additional number counts for features, please contact your Trustwave Sales Representative.
Phone Number: +1 (888) 878-7817
Email: infosales@trustwave.com
<https://www.trustwave.com/contact/>

Trustwave Government Solutions contact information
Support Email: support@trustwavegovt.com
Phone Number: +1 (877) 233-5190
Sales Email: sales@trustwavegovt.com

Notes:



- As of version 8.2, you no longer need to be an Administrator to add a license.
- As of version 8.2, do not move the license files to the licensing folder within the AppSecInc directory.
- You must use the **Add a License** function in the product.
- If you have added more than one license, the Product Expiration Date and ASAP Expiration Date will display the information from the license file that has the furthest date out.

2.5.2 Online License Generator

For some licensing agreements, an Online License Generator (OLG) is available. If you have this type of agreement, the username and password are assigned to you when you purchase AppDetectivePRO.

The Online License Generator allows you to generate any number of licenses for one or more AppDetectivePRO users. Licenses generated by the OLG are drawn down from your pool of purchased AppDetectivePRO OLG licenses.

¹ “UUT”, or Unit Under Test – refers to the number of database instances that can be assessed with this license.

If you need more information on the OLG or did not receive a username and password, contact infosales@trustwave.com.

2.6 Keeping Your Software Up-To-Date

Staying current with the latest software and knowledgebase updates is always encouraged. A best practice for keeping your system current is to run the ASAP Updater, available in the Settings section of AppDetectivePRO. Updates are also available for download from the Support Portal, at: <https://login.trustwave.com>.

2.7 Customer Support

Customer Support is available from 6 A.M. to 6 P.M. (GMT -5) Monday through Friday, except for company holidays. Actively licensed customers can open support tickets via our Support Portal: <https://login.trustwave.com>

Beyond opening and checking the status of tickets, the Customer Support Portal is a resource for product downloads, including SHATTER Knowledgebase releases, product documentation, and provides solutions for common user errors and other troubleshooting information.

For contact information by region, go to the following link, select AppDetectivePRO from the drop-down for Product or Service, and select the appropriate country:

<https://www.trustwave.com/Company/Support/>

Premium (24x7) support is available at an added cost. Please contact infosales@trustwave.com if you require this service.

3 Customizing Scans

Policies contain the complete list of controls you want to review for your assessment. These controls may contain checks that will be analyzed during the scan process (Pen Test or Audit).

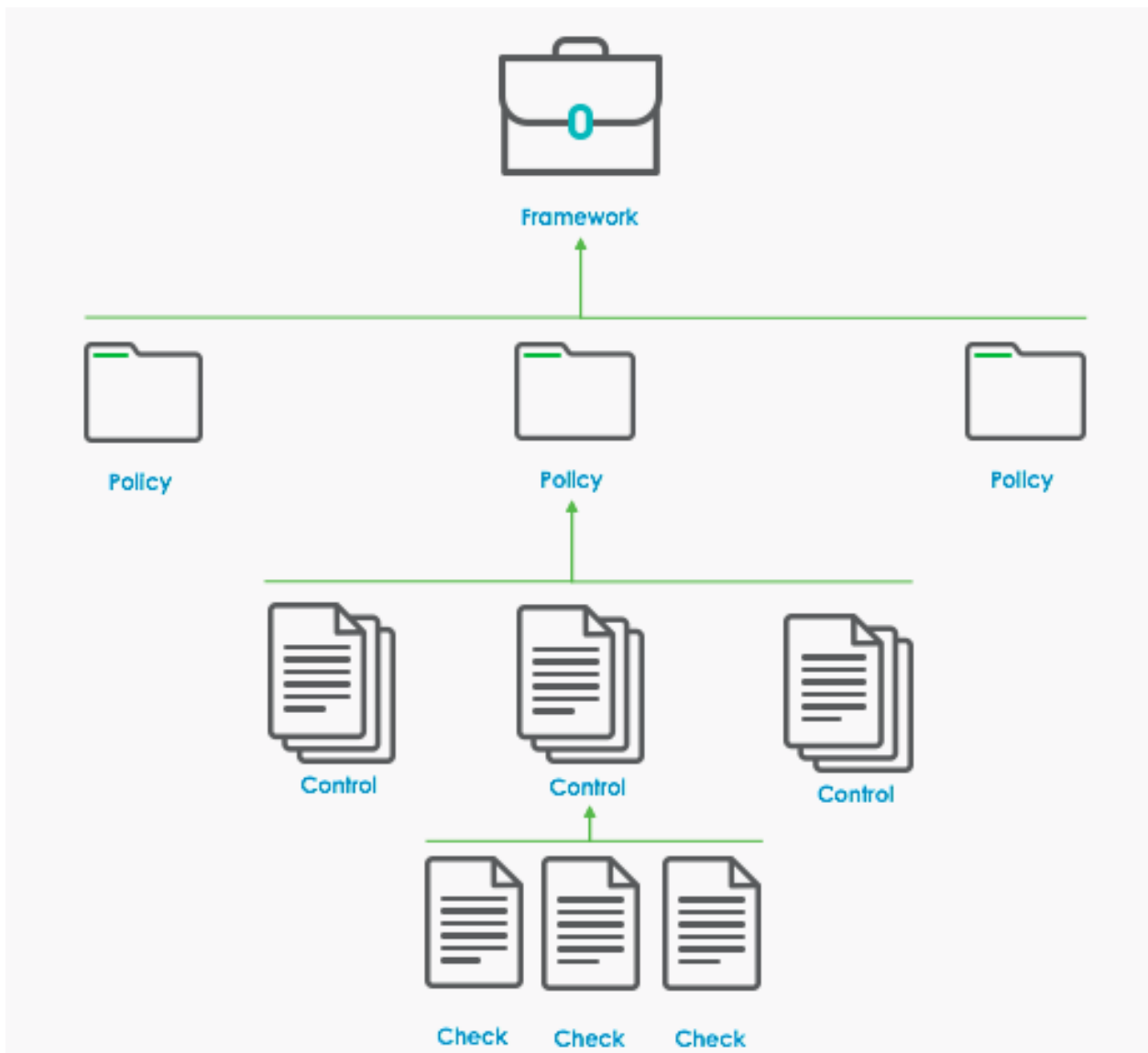
Policy scans (Pen Test or Audit) can be customized and user configurable parameters and exceptions can be modified or added to match your environment settings.

- Using Frameworks, Controls, and Checks

Frameworks, controls, and checks help you set up the policies you want to use.

- Framework is a container of total controls possible to be added to policies.
- The built-in default Framework in AppDetectivePRO is the SHATTER framework, which represents all the controls available out of the box.
- Additionally, there are built-in DISA STIG frameworks with specific policies for Oracle and Microsoft SQL Server.
- Policies can be created within a single framework.
- You select controls to add to policies within that single framework.
- With the built-in SHATTER framework, AppDetectivePRO has several built-in policies, including SOX, PCI, Baseline, Evaluation, and more.
- Controls are the items in a policy that are used to review during an assessment.
- You can associate check(s) to a control.
- With the built-in SHATTER framework, AppDetectivePRO has thousands of built-in checks that can be associated to any custom control.
- Checks are specific tests — an executable test that AppDetectivePRO runs against the database — that provides results.

Figure 1: How Frameworks, Policies, Controls and Checks are Related



3.1 Working with Policies

A policy is set up as either an Audit or a Pen Test type. Policies import controls from within frameworks; that is, a policy can contain a sub-set of controls that you import from existing frameworks. A control can contain one or many checks. Essentially, a policy selects a group of controls relevant to a particular security issue, and each of these controls contains relevant checks.

AppDetectivePRO includes built-in audit policies and built-in pen test policies.



Note: Built-in policies cannot be modified. However, you can clone any built-in policy and save it as a new name and customize any of it, by adding or removing controls, changing any parameter values, or adding exceptions.

4 Running Scans

The steps for running scans differ depending upon the type of scan you run, and the type of assets (databases or data stores) being scanned.

4.1 Discovery

When AppDetectivePRO performs a Discovery, it locates assets on your network and identifies the assets' IP addresses (as well as ports used to provide network services).

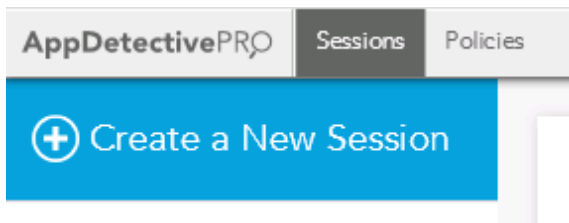
Discovery scans do not identify vulnerabilities. Discovering vulnerabilities (findings) is the function of Pen Tests and Audits.



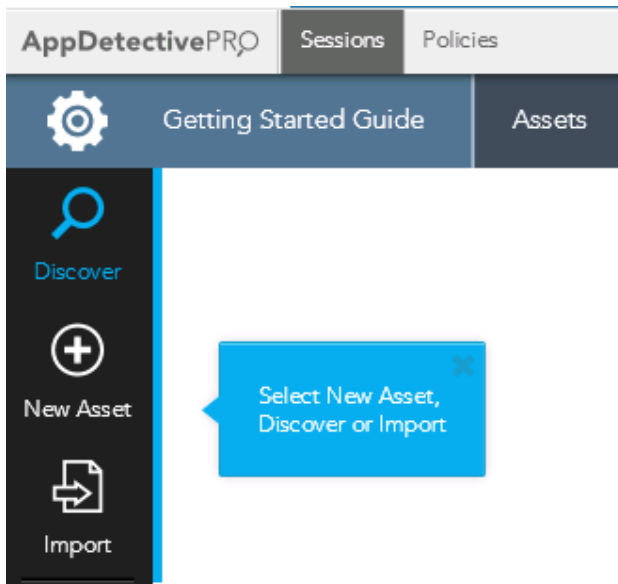
Note: Some databases may not be discoverable, depending on their configurations (i.e. Oracle 10g and later versions) or security configurations. For undiscovered assets, you can use the New Asset option or Import Asset option to create the assets in the Asset list.

To run a Discover scan:

1. Open a session (or create a new session).



2. Under the **Asset List** tab, on the left side of the screen, click the **Discover** icon:



3. Select a network for the discovery from the **Network Card** drop down list.

AppDetectivePRO Sessions Policies

Getting Started Guide Assets Policy R

Discovery

Please select hostnames and/or an IP range for the discovery.

Network Card:
 Intel(R) PRO/1000 MT Network Connection ▼

Add Host
 Hostname / IP Address:
 Add

Hostname	IP Address	
localhost	127.0.0.1	🗑️

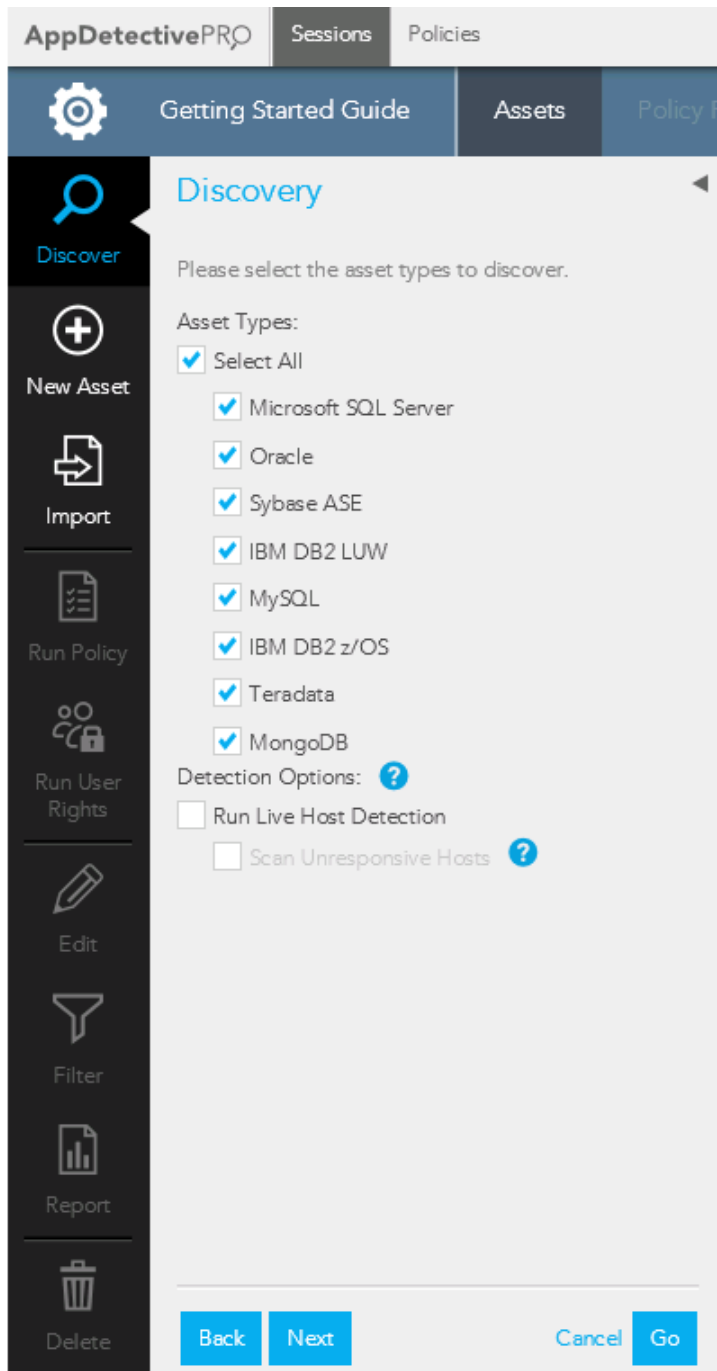
Specify Address Range
 Start IP: End IP:

Use Default Port
 Start Port: End Port:

Back **Next** Cancel Go

4. Provide a host name. To specify multiple hosts, type a name in the **Host Name/IP** field and click **Add** for each host you want to include.

5. Provide starting and ending IP addresses, and starting and ending ports for the discovery. (If you want to use default ports, check **Use Default Port.**)



6. Click the **Next** icon at the bottom of the panel. A list of assets appears.
7. Select the **Assets** you want to discover and click the **Next** icon.

- a. If you selected Oracle or IBM DB2 LUW as an Asset Type, you will then see options to enter a listener password and default instance. Provide this information and click Next to see a summary of your discovery parameters. From here, click Go to run the scan.
8. When Discovery is complete, a list of identified assets appears. There are two things you can do:
 - a. Edit the asset.
 - b. Run policy (Audit or Pen Test) or **User Rights Review** scans against it.

4.2 Adding or Importing Assets into a Session

You can import or add assets into a session. Assets can be added offline for scanning at a later time; assets that may go undetected by a discovery scan (because of a firewall or other security measures) can be manually imported.

To add an asset to a session:

1. Under the **Assets** tab, on the left side of the screen, click the **New Asset** icon. The **Create New Asset** fields appear.

The screenshot shows the 'Create an Asset' dialog box in the AppDetectivePRO interface. The dialog is titled 'Create an Asset' and is overlaid on the 'Assets' tab of a session named 'Full Demo Data - All Asset Types'. The left sidebar contains navigation icons for Discover, New Asset (highlighted), Import, Run Policy, Run User Rights, Edit, Filter, Report, and Delete. The main form area includes the following fields and options:

- Hostname:** A text input field with examples: 192.168.1.1, MyHostName, etc.
- Communication Protocol:** Two radio button options:
 - Port:** A text input field with an example: 1433.
 - Instance (optional):** A text input field with examples: MSSQLSERVER, SQLEXPRESS.
 - Pipe Name:** A text input field with an example: MSSQL\$SQLEXPRESS\sqlquery.
- Database Credentials (optional):** Two radio button options:
 - SQL Server Authentication** (selected).
 - Windows Authentication**.
- User Name:** A text input field.
- Password:** A text input field.
- Test Connection:** A button.
- Cancel** and **Add** buttons at the bottom right.

2. Provide the required information.

3. Click **Add**.

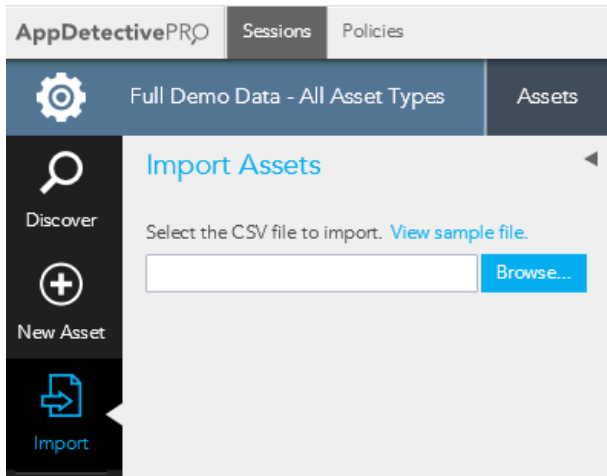
The asset you specified is added to your asset list.



Note: Creating new assets does not require testing the Database Credentials. You can create a new asset without verifying the connection. After adding it you can always test the Database Credentials prior to running an Audit policy or by Editing the Asset.

To import an Asset:

1. Under the **Assets** tab, click the **Import** icon:



Asset attributes are stored in CSV file format. The CSV file lists the asset name, host name, port asset type, platform type, instance name, and version type.

2. Select the appropriate CSV file and click **Import**.

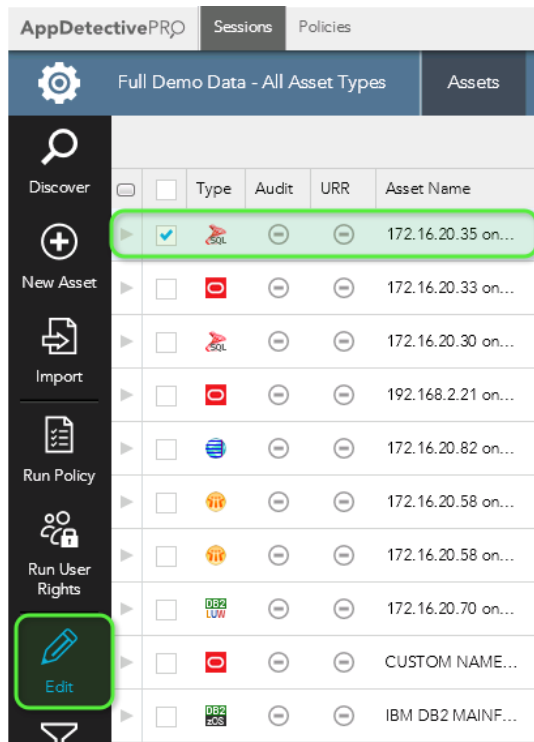
4.3 Editing Assets

You can change metadata about an Asset by editing it. For example, Discovery Scans run on Sybase assets typically do not record the Asset's platform, so data for those Assets may need to be edited in order for scans to run on them properly. You can also edit the Asset name so you can uniquely identify it rather than the default IP address and Port used when added by a Discovery scan.

To edit an asset:

1. Under the **Asset** tab, select the check box next to the Asset you want to edit.

2. Click the **Edit** icon.



3. Edit the asset information you want to change and click **Update**.

4.4 Pen Tests

A Pen Test assesses the security of your assets by running security checks (based on a policy you choose). Pen tests:

- are non-credentialed and non-intrusive
- commonly uncover vulnerabilities and misconfiguration errors that may result in unauthorized access or data exposure.

This section explains how to perform a Pen Test using AppDetectivePRO.

4.4.1 What Does a Pen Test Do to the Database?

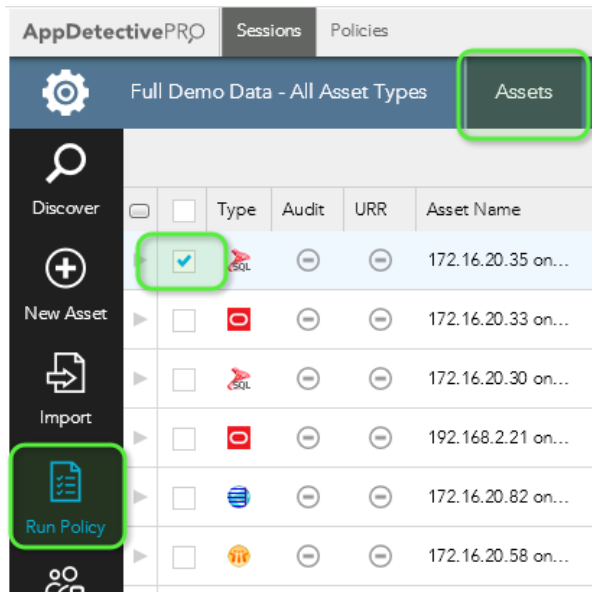
A Pen Test externally probes your database. Inherent to this activity is anonymous querying of network services for a variety of information. AppDetectivePRO does not provide a username or password, so nothing is used to actually connect to—or authenticate to—your system.

During the course of a Pen Test, AppDetectivePRO can run tests which may result in acquiring a valid username and password that attackers could potentially use to authenticate to the asset. These tests are password related and do require AppDetectivePRO to try and log in to the database, but also come with settings to protect from locking out accounts. You can configure these settings within the policy. Pen Tests do not make any updates or changes to your database.

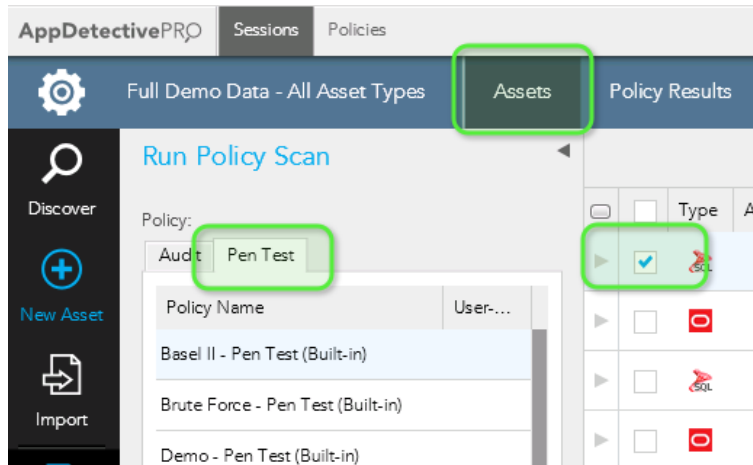
4.4.2 Running a Pen Test

To run a Pen Test:

1. Select the check box for the asset(s) you want to Pen Test.
2. Under the **Assets** tab, on the left side of the screen, click the **Run Policy** icon:



3. Click the **Pen Test** tab and select the policy you want to run.



4. Click **Run Now** and the Pen Test will run.

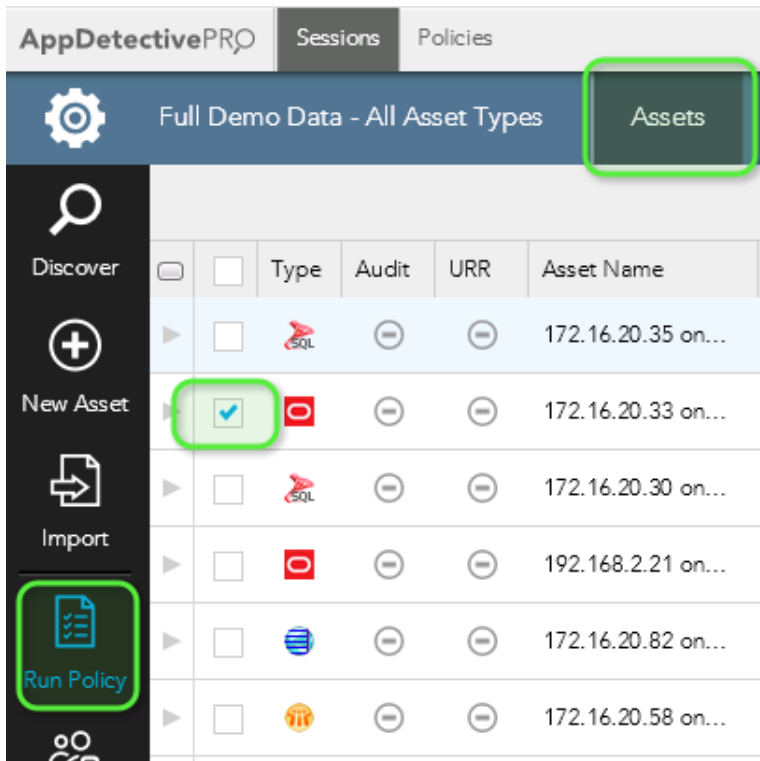
4.5 Audits

An Audit tests the security of your Asset and provides a deeper analysis of your database security configuration. Audits are credentialed scans that require a read-only account on the asset(s). Refer to 'Setting Up Database Access' section for more details.

4.5.1 Running an Audit

To run an audit:

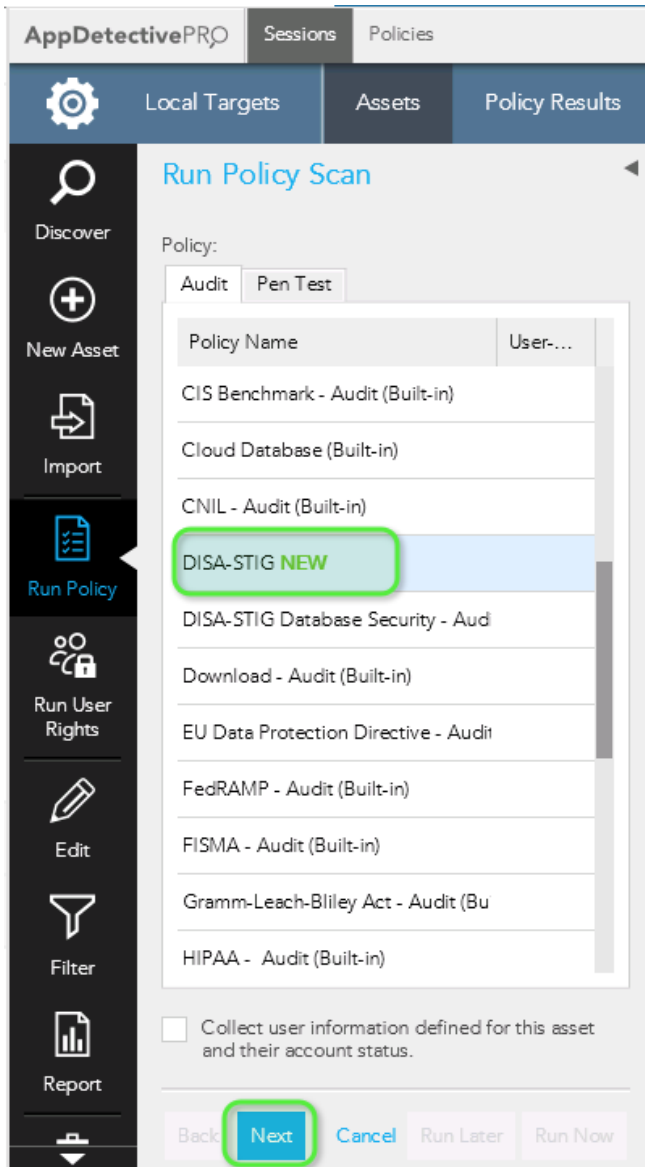
1. Select the check box for the asset(s) you want to audit.
2. Under the **Assets** tab on the left side of the page, click the **Run Policy** icon and choose the Asset to execute the Audit against:



The screenshot shows the AppDetectivePRO interface. At the top, there are tabs for 'Sessions' and 'Policies'. Below them is a dark blue header with a gear icon, the text 'Full Demo Data - All Asset Types', and a green-bordered 'Assets' button. On the left side, there is a vertical sidebar with icons for 'Discover', 'New Asset', 'Import', and 'Run Policy'. The 'Run Policy' icon is highlighted with a green border. The main area displays a table of assets with columns for 'Type', 'Audit', 'URR', and 'Asset Name'. The second row in the table has a green-bordered checkbox checked.

Type	Audit	URR	Asset Name
<input type="checkbox"/>			172.16.20.35 on...
<input checked="" type="checkbox"/>			172.16.20.33 on...
<input type="checkbox"/>			172.16.20.30 on...
<input type="checkbox"/>			192.168.2.21 on...
<input type="checkbox"/>			172.16.20.82 on...
<input type="checkbox"/>			172.16.20.58 on...

3. Select the policy you want to run and then click the **Next** arrow at the bottom of the panel to view summary data about the assets you are about to scan.



- Provide credentials and then click **Test Connection** to verify the asset you want to audit. Database authentication is required; operating system authentication is optional.



Note: Assets must be verified in order for you to run audits on them.

AppDetectivePRO Sessions Policies

Local Targets Assets Policy Results

Discover

New Asset

Import

Run Policy

Run User Rights

Edit

Filter

Report

Run Policy Scan (DISA-STIG)

Select assets (ctrl+click) to add and test credentials.

Asset Name	DB	OS
localhost on 5432 ()	✔	✘

There is a limit of 15 assets per scan.

Credentials for localhost on 5432 ():

Port: 22

User Name: postgres

Password: ●●●●●●

Advanced credential settings

Verify permissions are enough to run this scan.

Test Connection

Back Next Cancel Run Later Run Now

- Click **Run Now** and the **Audit** will run.

4.6 User Rights Review

User Rights Review provides a detailed view of a database's data ownership, access controls, and privileges to sensitive information.

4.6.1 Running a User Rights Review

To run a user rights review:

1. Under the **Assets** tab, select the check box for the asset(s) you want to audit.
2. Under the **Assets** tab, on the left side of the page, click the **Run Rights Review** icon.

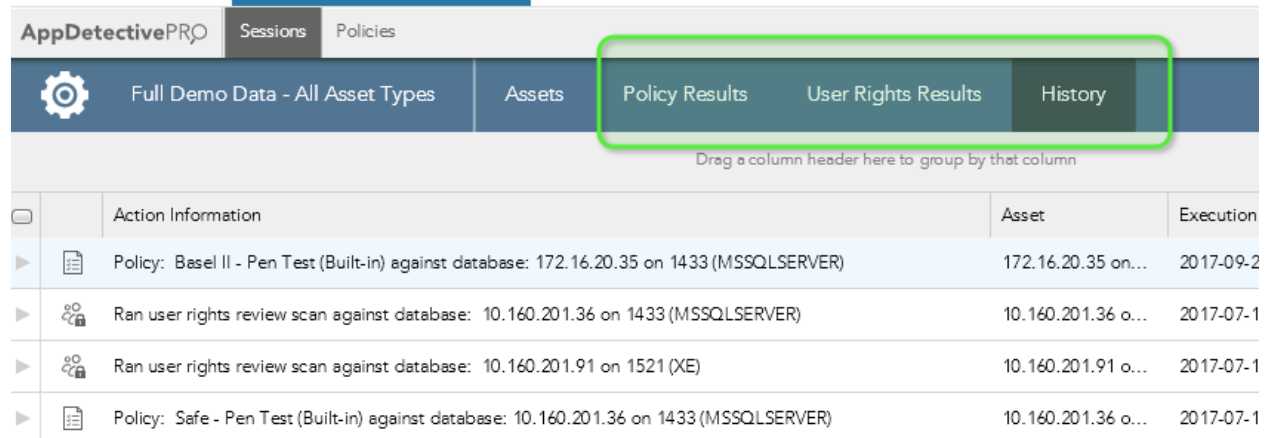
The screenshot shows the AppDetectivePRO interface. At the top, there are tabs for 'Sessions' and 'Policies'. Below that, there are three main sections: 'Full Demo Data - All Asset Types', 'Assets' (highlighted with a green box), and 'Policy Results'. On the left sidebar, there are several icons: 'Discover', 'New Asset', 'Import', 'Run Policy', 'Run User Rights' (highlighted with a green box), 'Edit', and a filter icon. The main content area is titled 'User Rights Review' and contains the following elements:

- A search bar with a magnifying glass icon.
- A text prompt: 'Select assets (ctrl+click) to add and test credentials.'
- A table with columns 'Asset Name' and 'Verified'. The first row is highlighted in blue and contains the text '172.16.20.35 on 1433 (MSSQLSERVER)'. A green box highlights the checkbox in the 'Verified' column for this row.
- A note: 'There is a limit of 15 assets per scan.'
- 'Database Credentials' section with two radio buttons: 'SQL Server Authentication' (selected) and 'Windows Authentication'.
- 'User Name:' and 'Password:' input fields.
- A blue 'Verify Credentials' button.
- A table on the right side of the interface with columns for 'Type' and a 'Run' button (represented by a red square with a white circle). The first row is highlighted in blue and contains a checkmark in the 'Verified' column and a red 'SQL' icon in the 'Type' column.

3. Provide credentials to verify the asset you want to scan. Database authentication is required.
Note: Assets must be verified in order for you to run audits on them.
4. Click **Run Now** and the scan will run.

5 Understanding Scan Results

Various views of scan results are available on the **History**, **Policy Results**, and **User Rights Results** sections that appear under the **Sessions** tab.



	Action Information	Asset	Execution
▶	Policy: Basel II - Pen Test (Built-in) against database: 172.16.20.35 on 1433 (MSSQLSERVER)	172.16.20.35 on...	2017-09-2
▶	Ran user rights review scan against database: 10.160.201.36 on 1433 (MSSQLSERVER)	10.160.201.36 o...	2017-07-1
▶	Ran user rights review scan against database: 10.160.201.91 on 1521 (XE)	10.160.201.91 o...	2017-07-1
▶	Policy: Safe - Pen Test (Built-in) against database: 10.160.201.36 on 1433 (MSSQLSERVER)	10.160.201.36 o...	2017-07-1

5.1 Viewing Scan History

You can view information about all of the actions performed during a session by clicking **History**. The table that appears shows the types of actions that occurred, the assets that were scanned, and the execution time of each scan.

You can view any errors that occurred during Policy scans for skipped or failed check status results in this section.

5.2 Viewing Scan Results

Scan results are split into two main sections: **Policy Results** and **User Rights Results**. After you have run a Policy scan, the **Policy Results** section becomes enabled. You can go here to review results in two different views: **Check Results** and **Control Review**. After you have run a **Rights Review** scan, the **User Rights Results** section becomes enabled.

5.3 Policy Results

When you click on **Policy Results**, you will be brought to the default view of **Check Results** (Informational view), filtered to show all the findings from the scan. You can choose different options using the Filter on the left to tailor your results. You have options to filter on showing results from a specific asset, a specific policy scan from an asset, by risk level of the check, and by the check result. You can also view the KB Article/CVE associated with the selected finding. If you want to see a graphical representation of the results, choose the **Graphical** view option on the upper right.

The screenshot shows the AppDetectivePRO interface with the 'Policy Results' view selected. The main content area displays a table of findings for the asset '10.160.201.102 on 1025 ()'. The findings are categorized into 'Finding' and 'Non Finding'. A 'Knowledgebase Article' panel is open on the right, showing details for the finding 'Latest patch not applied'. The article includes a description, vulnerability information, a summary, and references.

Check Name	Risk	Count
10.160.201.102 on 1025 ()		Count=14
CIS Benchmark - Audit (Custom with Teradata) (Framework: SHATTEI)		Count=3
<ul style="list-style-type: none"> Latest patch not applied (High) List any login with permissions on tables (Low) List any application objects granted to PUBLIC (Info) 		Count=8
<ul style="list-style-type: none"> List authorities granted privileges 'with grant' option (Med) List any login or role with grant or revoke privileges (Med) List any login/role with any DDL (create/alter/drop) pr (Med) List any login or role with modify or replace privileges (Med) List any database level privileges granted to PUBLIC (Med) List DBA role members (Low) List status and configuration of audit system (Info) List any privilege directly granted to users (Info) 		

Knowledgebase Article

Check: Latest patch not applied

Type: Audit

Category: Application Integrity

Description: Verify that the latest patches are applied to the database.

Vulnerability: Found that latest patches are not applied to the database.

Summary: Teradata Database should be updated with latest patches to fix security issues.

Fix Information: N/A

Asset Type: Teradata

Versions Affected: Teradata Database 14 and 15

CVE: CVE-NO-MATCH

References: SHATTER Control Category: Application Integrity
NIST 800-53: SI



Note: If you are familiar with previous versions of AppDetectivePRO, the **Check Results** (Informational view) allows you to see all the findings (or vulnerabilities with violation found) and filter them by Asset or specific policy scan for that Asset.

The other available view in Policy Results is the **Control Review**. The **Control Review** allows you to review the controls from the Policy scan that was conducted. You can use this view to do further examination. You can add notes and suppress at all levels of the control (control, check result, or check result occurrence). You can also view the KB Article/CVE associated with the selected finding.

The screenshot displays the 'Control Review' interface. On the left, a 'Filter' sidebar shows a search box and a list of assets and policies, including '10.160.201.102 on 1025 ()', '10.160.201.36 on 1433 (MSSQLSER)', '10.160.201.91 on 1521 (XE)', and '172.16.20.30 on 1433 (MSSQLSERV)'. Below this, 'Risk Levels' (High, Medium, Low, Informational) and 'Response Types' (Not Reviewed, Non Finding, Finding, N/A) are listed. The main area shows a table of findings for the asset '10.160.201.102 on 1025 ()' under the policy 'CIS Benchmark - Audit (Custom with Teradata) (Framework: SHATTEI)'. The table has columns for 'Response', 'Control Name', and 'Risk'. The first finding is 'Latest patch not applied' with a 'High' risk level. A right-hand pane displays the 'Knowledgebase Article' for this finding, with an overview: 'Download latest Teradata Database patches from https://tays.teradata.com.' and a link to the same URL.



Note: If you are familiar with previous versions of AppDetectivePRO (prior to 8.5), the Control Review (Informational view) replaces the Interview interface.

5.4 User Rights Results

After a Rights Review scan is performed, the **User Rights Results** section becomes enabled. When you go to this section you can review all the details of any Rights Review scan performed in the Session. You can choose from different views (**Objects**, **Roles**, **Users**) depending on the data you are looking to further examine. The default view is by **Objects**. Use the **Filter** on the left to drill down to the data you want.

Use the icon to expand and review the details for each of the rows.

The screenshot shows the AppDetectivePRO interface with the 'User Rights Results' section active. The navigation bar includes 'Full Demo Data - All Asset Types', 'Assets', 'Policy Results', 'User Rights Results', and 'History'. The filter sidebar on the left has 'Objects' selected. The main content area displays a table of user rights information for a scan on 10.160.201.102. One row is expanded to show details for 'DBC.TVFIELDS_TD13', including a table of granted privileges.

Granted To	Grantee Type	State	Privilege
[DBC: Dump Privilege WITH GRANT O...	Implicit Privilege	GRANT_WITH_GRANT_OPTION	Dump
[DBC: Restore Privilege WITH GRANT...	Implicit Privilege	GRANT_WITH_GRANT_OPTION	Restore
[DBC: Select Privilege WITH GRANT O...	Implicit Privilege	GRANT_WITH_GRANT_OPTION	Select

6 Generating Reports

Generating reports work together with the filtered view of your scan results. Whatever you currently have filtered on in the data set you can select from to generate reports. You can generate reports from the **Assets** section, the **Policy Results** section, and the **User Rights Results** section.



Note: If you are familiar with previous versions of AppDetectivePRO, the default filter view in the **Check Results** view is the same as the vulnerabilities displayed after your Audit or Pen Test scan is completed. You can then just choose to generate a **Vulnerability Summary** or **Details** report.

After you review and filter the results of your assessment and have selected the rows from the grid, you can include those results in a report for presentation purposes. Click the **Reports** icon in the top left side of the screen to generate reports.

The screenshot shows the AppDetectivePRO interface. The top navigation bar includes tabs for Sessions and Policies. Below this, there are tabs for Assets, Policy Results, User Rights Results, and History. The Assets, Policy Results, and User Rights Results tabs are highlighted with a green box. On the left sidebar, the Reports icon (a document with a bar chart) is highlighted with a green box. The main content area shows a table of scan results for the asset 10.160.201.102 on 1025 (). The table has columns for Check Name, Risk, Occurrences, and Message. A finding is selected, and its details are shown below the table. The finding is 'latest patch not applied' with a High risk level and 1 occurrence. Other findings include 'list any login with permissions on tables' (Low risk, 2 occurrences) and 'list any application objects granted to PUBLIC' (Informational risk, 248 occurrences). The Reports icon in the sidebar and the finding selection checkbox are also highlighted with green boxes.

Check Name	Risk	Occurrences	Message
10.160.201.102 on 1025 ()			
CIS Benchmark - Audit (Custom with Teradata) (Framework: SHATTER KB v5.0) 2016-04-18 14:50 UTC-07:00 to 2016-04-18 14:50 UTC-07:00			
Finding			
latest patch not applied	High	1	
list any login with permissions on tables	Low	2	
list any application objects granted to PUBLIC	Informational	248	
Non Finding			

Various Report types are available with a description of each available report and is provided on the AppDetectivePRO interface. Different reports and formats are available based on the Policy or User Rights results you want to report on.

6.1 Additional Information

More information about using AppDetectivePRO is available in the *Trustwave AppDetectivePRO User Guide*.

To access the User Guide, you can login to the Customer Support Portal: <https://login.trustwave.com>

If you do not have access to the portal, feel free to contact infosales@trustwave.com to gain access.

For contact information, by region, go to the following link, select **AppDetectivePRO** from the drop-down for **Product** or **Service**, and select the appropriate country:

<https://www.trustwave.com/Company/Support/>

About Trustwave®

Trustwave is a leading provider of compliance, Web, application, network and data security solutions delivered through the cloud, managed security services, software and appliances. For organizations faced with today's challenging data security and compliance environment, Trustwave provides a unique approach with comprehensive solutions that include its TrustKeeper® portal and other proprietary security solutions. Trustwave has helped hundreds of thousands of organizations—ranging from Fortune 500 businesses and large financial institutions to small and medium-sized retailers—manage compliance and secure their network infrastructures, data communications and critical information assets. Trustwave is headquartered in Chicago with offices worldwide. For more information, visit <https://www.trustwave.com/home/>.