



USER GUIDE

Trustwave AppDetectivePRO

Version 10.8

October 2023

Revision History




Version	Date	Changes
10.8	October 2023	<ul style="list-style-type: none"> Added SAP ASE Server and Redis Server to the Database Platforms table in Supported Database Platforms User Rights Review is now supported for Cassandra
10.7	July 2023	<ul style="list-style-type: none"> Added Cassandra to the Database Platforms table in Supported Database Platforms Support for Azure SQL Database
10.6	May 2023	<ul style="list-style-type: none"> Audit is now supported for Amazon DynamoDB Discovery, Audit and User Rights Review are now supported for Teradata 17 Support for PostgreSQL, MSSQL and MySQL on Microsoft Azure platform Removed support for Web Application Scanning
10.5	January 2023	<ul style="list-style-type: none"> Audit and User Rights Review are now supported for MySQL, MariaDB, Azure SQL Managed Instance, and PostgreSQL on AWS RDS Improved UI architecture Added IBM DB2 z/OS, Couchbase, and Hadoop to the Database Platforms table in Supported Database Platforms
10.4	June 2022	<ul style="list-style-type: none"> Discovery, audit, and user rights scan are now supported for Postgres 14. Added support for user-defined checks for MongoDB. Now runs as a native 64-bit application on .NET 6 Platform. Improved handling of large User Rights Review data.

Formatting Conventions

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

Formats and Symbols	Meaning
<u>Crimson Underline</u>	A crimson underline indicates a link to a website or email 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 9 pt.</code> indicates computer code or information at a command line.
<i>Italics</i>	Italics denotes the name of a published work, the current document, name of another document, text emphasis, to introduce a new term, and path names.
[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.

About this Document

This guide describes the basic features and uses of AppDetectivePRO. You can use this guide as a reference when using the product. Additional information can be found in knowledgebase articles within the Support Portal.

Contents

AppDetectivePRO Basics.....	8
View your version of AppDetectivePRO	8
Typical System Requirements.....	8
Supported Database Platforms	9
Installation	11
Install AppDetectivePRO	11
Install Nmap for ADPro	12
Configure the AppDetectivePRO User	17
Install the License.....	17
Additional Setup for Client Drivers.....	19
Keeping your software up to date.....	19
Product Support Lifecycle	20
Customer Support	20
Understanding the AppDetectivePRO User Interface	21
Working in Sessions.....	21
Assets	22
Discover	22
New Asset	23
Import.....	23
Edit.....	27
Filter	27
Report	27
Delete.....	27
Run Policy.....	28
Audit.....	28
Pen Test	29
Run User Rights	29
Run Now and Run Later Option.....	30
History	30
Policy Results	31
Check Results.....	31
Understanding the Check Results Filter	31
Control Review	32
Using the Control Review Feature.....	33
Understanding the Control Review Filter	35
User Rights Results.....	36
Object View.....	36
Roles View	37
Users View	38
Reports	39
Generate Check Results Reports	39
Generate Control Review Reports.....	41
Report Reviewer Options.....	42
Generate User Rights Review Reports.....	42

- Working in Policies 43
- Use Frameworks, Controls, and Checks..... 44
- Policies 45
 - Customize Policies 46
 - Delete Policies 48
 - Add/Remove Controls..... 48
- Frameworks..... 48
 - Customize Frameworks..... 49
 - Create/Clone/Delete Framework 49
 - Add/Create/Edit/Remove Control 50
 - Add/Create/Edit/Remove Check..... 50
- System Settings 51**
- User Account Privileges Needed for Audit and User Rights Review Scans 55**
- Additional Information..... 58**
- Legal Notice 59

List of Tables

- [System Requirements](#)
- [Database Platforms](#)
- [Platform Client Drivers](#)
- [Product Support Lifecycle](#)
- [Asset Type](#)
- [Platform \(OS\) Value \(not all options listed\)](#)
- [Database Value](#)
- [Examples of Checks and Result Types](#)
- [Permissions for OS Access](#)
- [Permissions for Unix Access](#)
- [Target Database Permissions for Unix](#)

AppDetectivePRO Basics

AppDetectivePRO is an in-depth database security assessment solution. It provides a comprehensive database security diagnostics approach that includes vulnerability assessment, configuration assessment, and identity access assessment. The solution provides easy to use features that allow you to get up and running quickly.

View your version of AppDetectivePRO

To view the version, go to the **System Settings** by clicking on the gear icon located on the upper right of the application. You will see an **About** section that lists the component versions of AppDetectivePRO.

Typical System Requirements



Caution: It is the recommendation of Trustwave that, to protect data at rest, AppDetectivePRO should be installed on a system drive that has the Windows Bitlocker feature enabled on.

The following table lists AppDetectivePRO typical system requirements:

System Requirements

Requirement	Minimum
Operating System	<ul style="list-style-type: none"> Windows 10 (64-bit) and .NET Desktop Runtime 6.0.1 or above
Rights	To install AppDetectivePRO and perform an ASAP Update or upgrade of the software, you must have Administrator privileges on the Windows host.
Processor	Dual core processors 1.60 GHz or higher
RAM	8GB or higher
Hard Drive	<ul style="list-style-type: none"> 1.25 GB of free disk space for installation 5 GB 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	When installing AppDetectivePRO, an SQLite database will be created and will be used specifically for the AppDetectivePRO installation.
Server Certificate(s)	If scanning is performed over SSL/TLS/HTTPS, the server's certificate will need to be installed as a trusted certificate in order for a connection to be established.

Supported Database Platforms

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

Database Platforms

Requirement	Minimum
Oracle (SID)	<ul style="list-style-type: none"> Version: 19c* Scan Type: Audit, Pen Test, User Rights Review Required database drivers are included. <p>*Pen Test is not supported for 19c.</p>
Microsoft SQL Server (instance)	<ul style="list-style-type: none"> Version: 2019, 2017, 2016, 2014 Scan Type: Audit, Pen Test, User Rights Review Required database drivers are included. When adding an asset, Azure SQL Managed Instance is supported by selecting Microsoft SQL Server as Asset Type and Microsoft Azure as Platform.
IBM DB2 LUW (Database)	<ul style="list-style-type: none"> Version: 11.5* Scan Type: Audit, User Rights Review You must install 32-bit runtime client drivers on your host for Audit and User Rights Review scans to function.
SAP (Sybase) ASE (Data Server)	<ul style="list-style-type: none"> Version: 16.0 Scan Type: Audit, Pen Test, User Rights Review You must install 32-bit client drivers (both ODBC and ADO.NET) on your host for Audit and User Rights Review scans to function
PostgreSQL	<ul style="list-style-type: none"> Version: 14, 13, 12, 11.x Scan Type: Audit, User Rights Review Pen Test is not supported Required database drivers are included
MySQL (Server)	<ul style="list-style-type: none"> Version: 8.0, 5.7 Scan Type: Pen Test, Audit, User Rights Review Database drivers required for Audit scans and User Rights Review are included You must install 32-bit ODBC client drivers on your host for pen tests and user-defined checks to function.

Requirement	Minimum
MariaDB (Server)	<ul style="list-style-type: none"> Version: 10.5 Scan Type: Audit, User Rights Review Pen Test is not supported Required database drivers are included
Microsoft Azure SQL Database	<ul style="list-style-type: none"> Scan Type: Audit User defined checks not supported. Discovery and Pen Test is not supported. Required database drivers are included.
Teradata Database	<ul style="list-style-type: none"> Version: 17.20, 17.10, 17.05 Scan Type: Audit, User Rights Review Pen Test is not supported. You must install 32-bit client drivers (both ODBC and .NET) on your host for Audit and User Rights Review scans to function.
MongoDB	<ul style="list-style-type: none"> Version: 5.0, 4.4 Scan Type: Audit, User Rights Review User defined checks not supported. Required database drivers are included.
Amazon Aurora	<ul style="list-style-type: none"> PostgreSQL, MySQL Scan Type: Audit, User Rights Review User defined checks not supported Pen Test is not supported Required database drivers are included
Amazon Web Services	<ul style="list-style-type: none"> PostgreSQL, MySQL, Microsoft SQL Server, Oracle, Maria DB Scan Type: Audit, User Rights Review User defined checks not supported. Pen Test is not supported Required database drivers are included

Requirement	Minimum
Percona Server for MySQL (Server)	<ul style="list-style-type: none"> Version 8.0, 5.7 Scan Type: Audit, User Rights Review User defined checks not supported Pen Test is not supported Required database drivers are included
DynamoDB	<ul style="list-style-type: none"> Scan Type: Audit User defined checks not supported Pen Test and User Rights Review is not supported Required database drivers are included
Cassandra	<ul style="list-style-type: none"> Version 4.0 Scan type: Audit, User Rights Review Pen Test is not supported Required database drivers are included
Redis	<ul style="list-style-type: none"> Version 7.0 Scan type: Discovery, Audit Required database drivers are included

Installation

This section describes the installation and configuration of the AppDetectivePRO. Complete installation of Nmap 3.92 and above is required prior to installing AppDetectivePRO v10.8.



Note: Nmap (Network Mapper) is an open-source, third party software used for mapping networks, auditing, and security scanning. You can download the Nmap executable file from their website <https://nmap.org/>.

Install AppDetectivePRO

Run the executable file as a local Windows Administrator. Double-clicking on the executable file opens the dialog box where you can choose to allow changes to be made to your computer system. You will see a message that you have successfully installed the application when the process has finished successfully.

Notes:

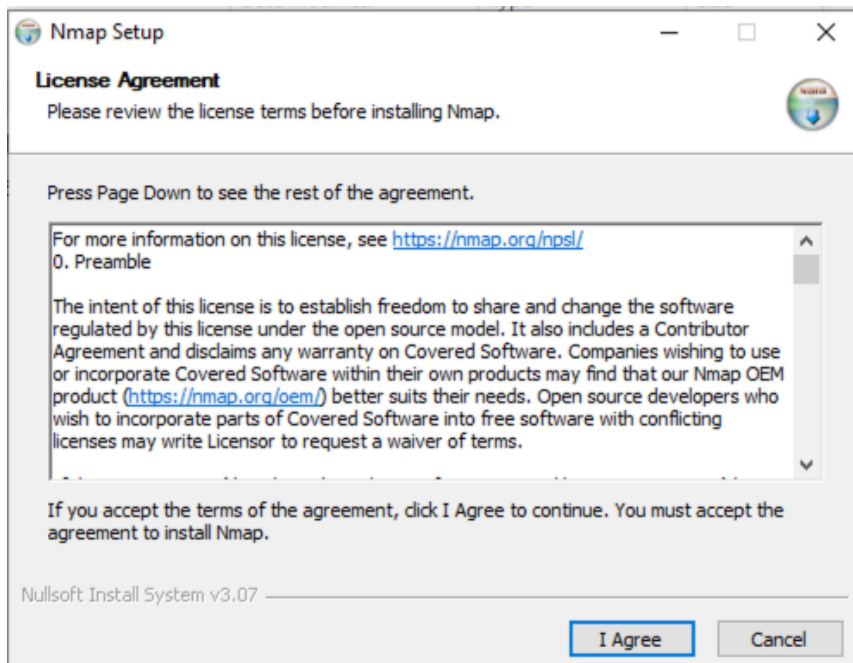


- The backend database is created when AppDetectivePRO is started for the first time. AppDetectivePRO must be started by a local Windows Administrator to create this database.
- Support for Web Application Scanning ended with v10.6. Upgrading to v10.8 will purge web application-related control and check results. This is an irreversible action upon upgrade.

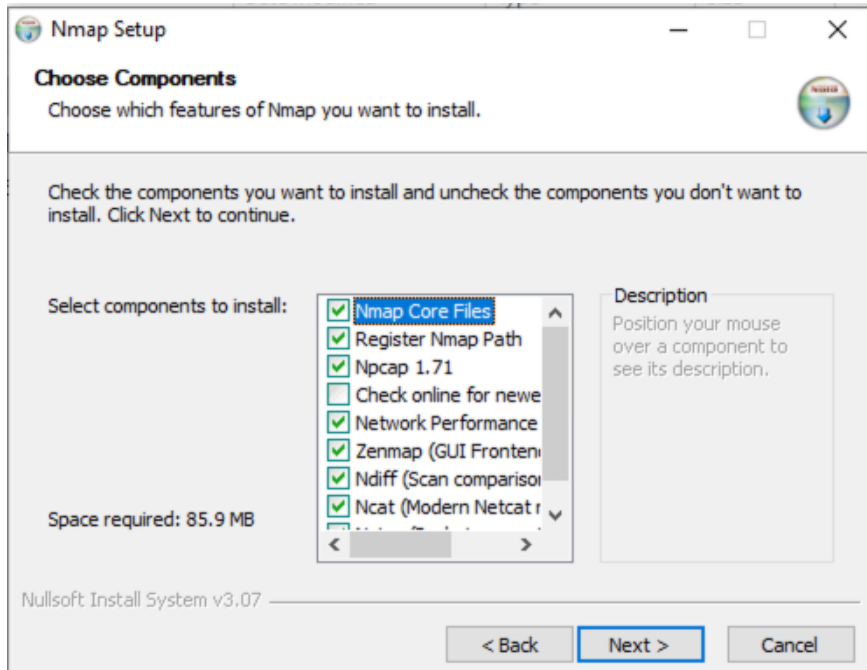
Install Nmap for ADPro

Here are the steps related to the Scan Engine installation during ADPro setup:

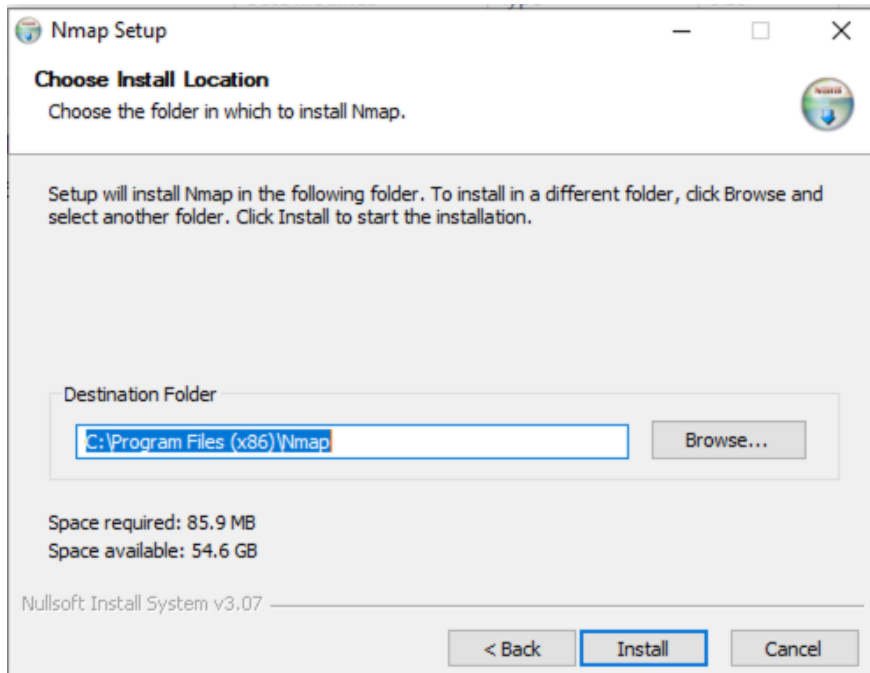
1. In the **Nmap Setup** dialog, click **I Agree**.



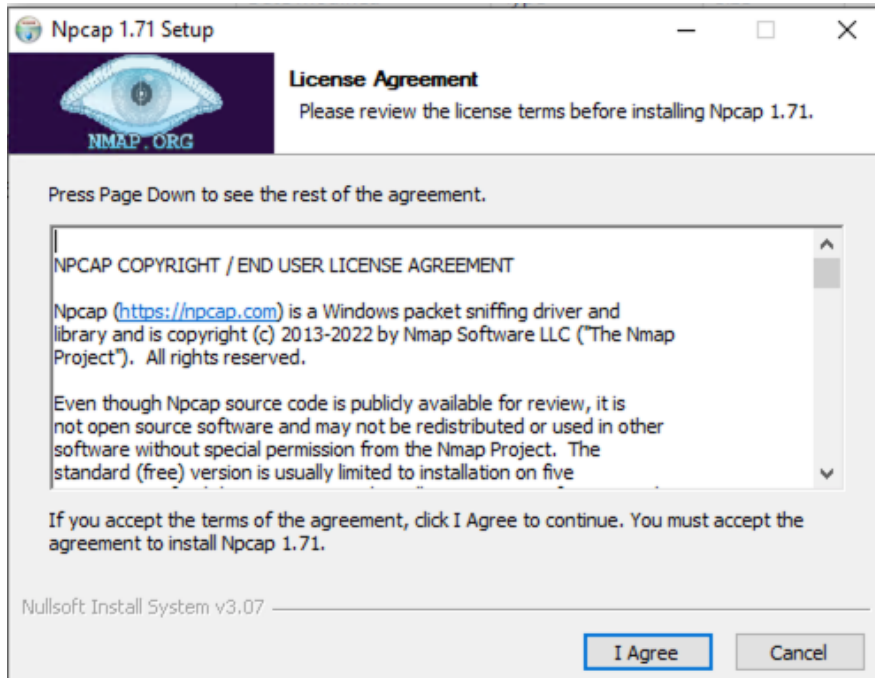
2. Click **Next**.



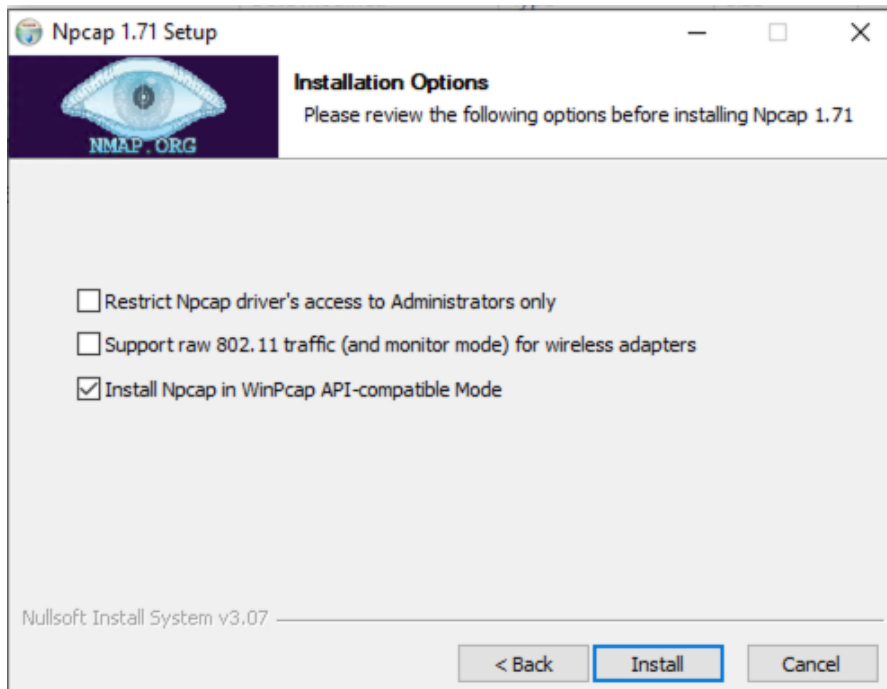
3. Choose the location of the destination, and then click **Install**. The required components are downloaded and the installation of Npcap starts.



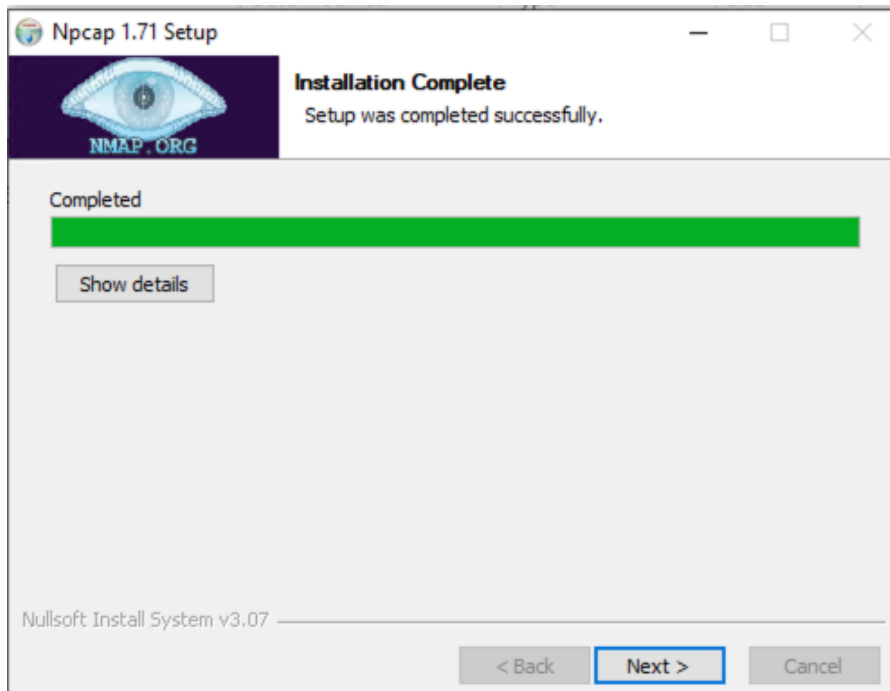
4. Click **I Agree**.



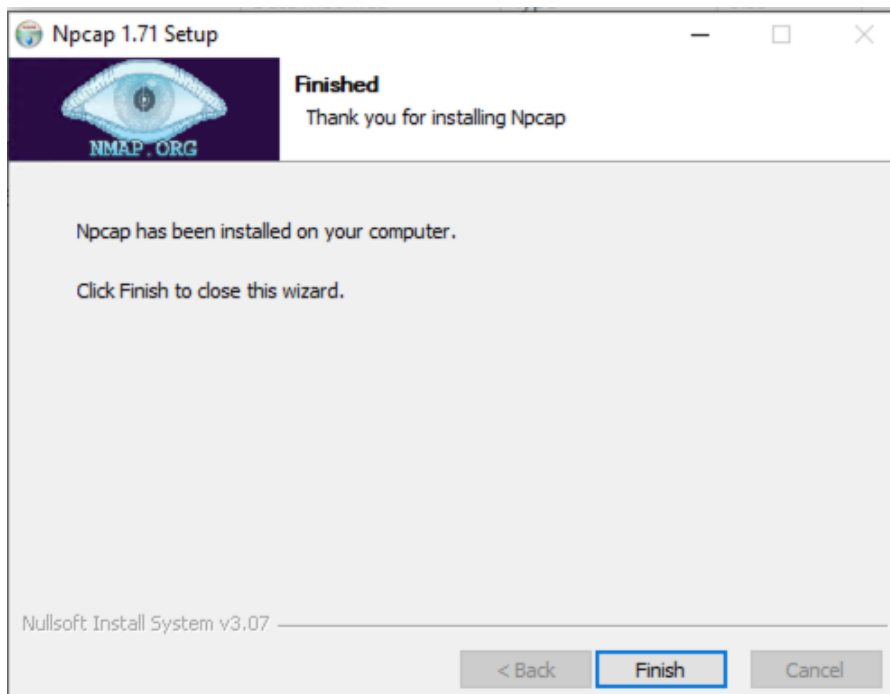
5. Choose the installation option, and then click **Install**.



6. Click **Next**.

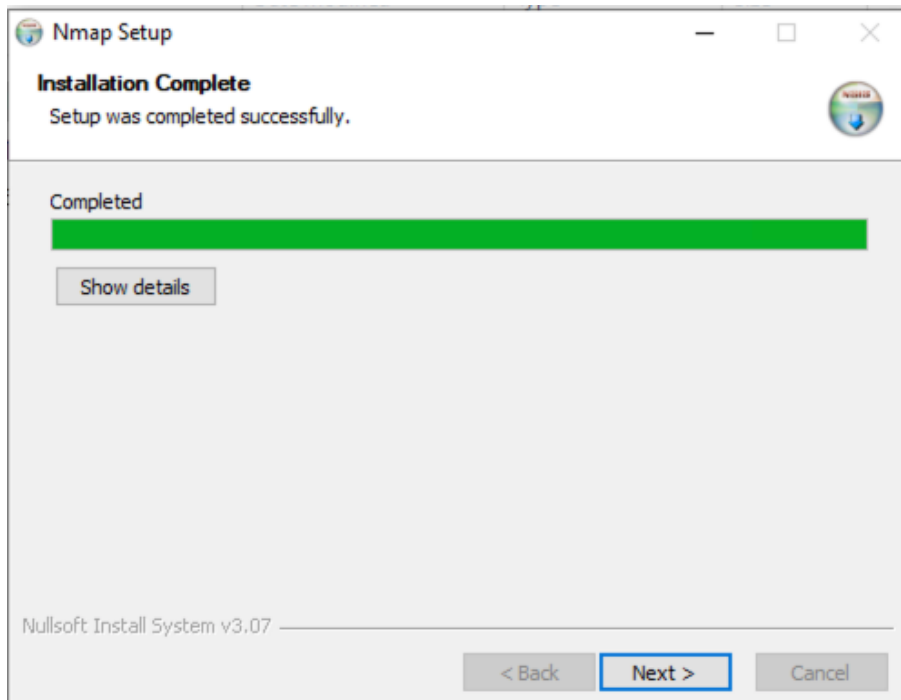


7. Click **Finish**.

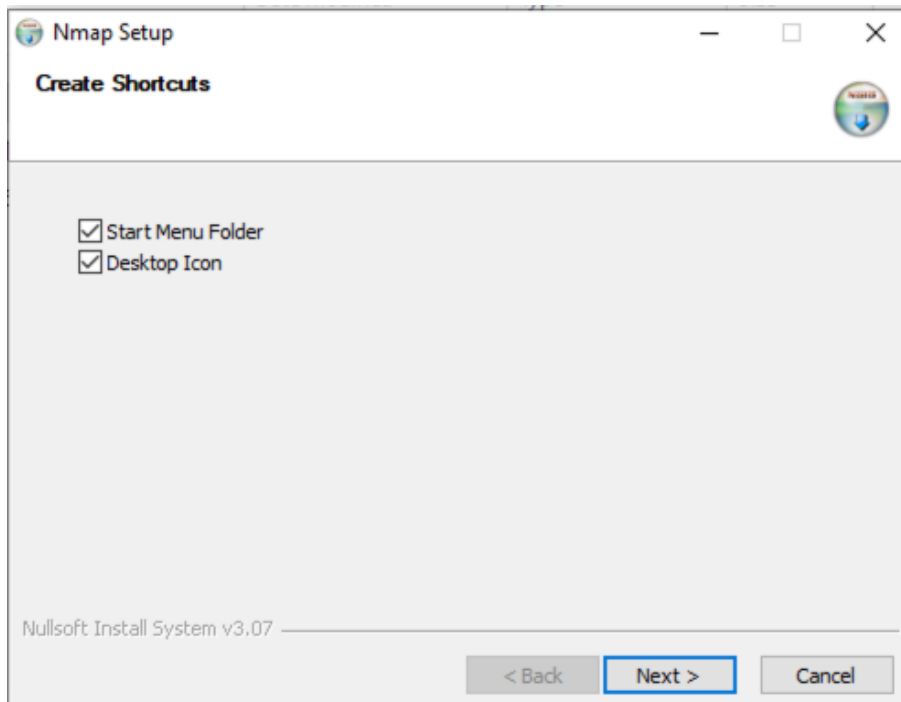


The Npcap installation completes, and the Nmap setup resumes.

8. Click **Next**.



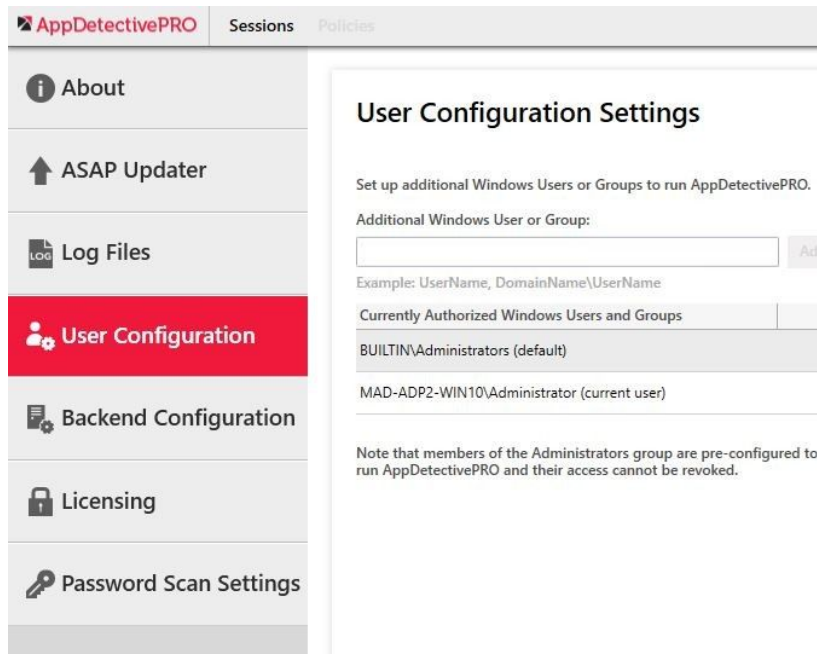
9. Choose the appropriate options, and then click **Next**.



10. Click **Finish**. After the Installation of Nmap completes, ADPro will start the installation of Scan Engine that does not require any user interaction.

Configure the AppDetectivePRO User

At installation time, you must be logged on as a Windows Administrator. The account used for installation is the only user that initially has access to the AppDetectivePRO software. To add any other Windows login, the Windows Administrator who installed the software can navigate to the **System Settings** and choose **User Configuration**.



Note: It is best practice to create a local Windows user and configure it in AppDetectivePRO. You can use this user to always get access to AppDetectivePRO.

Install the License

After you purchase licenses for AppDetectivePRO, you receive your licenses. Some licenses require a machine ID and other types do not.

If a machine ID is required for your license, you are required to provide it to the Trustwave Account Executive or Delivery Ops Department to receive a new license file. To obtain the machine ID, go to the **Licensing** section in the **System Settings**. Copy and paste the number from the **Machine ID** field and send it to the Trustwave contact.

AppDetectivePRO Sessions Policies

Licensing

Customer Name: EngineeringDevLicense2023
Machine ID: 103442761
Product Expiration Date: 2023-12-31
ASAP Expiration Date: 2023-12-31

Add a License... Show Expired Licenses

Feature Name	Purchased	Used	Available
AD20221129130627 (Production, 2023-12-31)			
IBM DB2 z/OS Subsystem Locations (Audit)	999	0	999
Units Under Test (UUTs) - Policy Scans (Audit/Pen Test) and User Rights Review	999	5	994

IP Address / Hostname	Port	Database	Platform	Version
tgt-postgres14-cent7...	5432	Database: postgres	Linux	PostgreSQL 14
tgtmssql2017w12.ny...	49398	Instance: MSSQL2017	Microsoft Windows	Microsoft SQL Server 2017
utwin33.tslab.prv	1433	Instance: MSSQLSERVER	Microsoft Windows	Microsoft SQL Server 2016
scs-sql2k16.nycapt35...	3306		Microsoft Windows	MySQL 8.0 Database
tgt-elastics01-rh8.ny...	9200		Linux	Elasticsearch

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

Once you have received a license file from Trustwave, navigate to the **Licensing** section in the **System Settings**, choose **Add a License** and browse to the .lic file you received. Once the license is added you will see the following information:

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

Notes:



- In this version, you do not need to be an Administrator to add a license.
- In this version, do not move the license files to the licensing folder within the AppDetectivePRO 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 greatest expiry date.

Additional Setup for Client Drivers

Additional client driver installations must be performed to run Audit policy scans and Rights Review scans. The following table includes details.



Caution: Even if you have installed AppDetectivePRO on a 64-bit OS, you must install the 32-bit client drivers. If client drivers are installed after the installation of AppDetectivePRO, you must restart the Trustwave Scan Engine Service. If this is not done, then testing credentials or running scans will not work.

Platform Client Drivers

Platform	Client Drivers Required
IBM DB2 LUW (Database)	<ul style="list-style-type: none"> Versions supported: 11.5 You must install the appropriate runtime client drivers on your host for Audit and User Rights Review scans to function. Trustwave recommends that you use the latest version and Fix Pack of the client driver. To obtain access to downloads from IBM proceed to the following link (access may require free registration or require a valid support agreement with IBM): http://www-01.ibm.com/support/docview.wss?uid=swg27007053 <p>Note: Work with your DBA group to obtain the drivers needed.</p>
Teradata Database	<ul style="list-style-type: none"> Versions supported: 17.x (both ODBC and .NET) (32-bit only) You must install the appropriate runtime client drivers on your host for Audit and User Rights Review scans to function. To obtain access to downloads from Teradata proceed to the following links (access may require free registration or require a valid support agreement with Teradata): http://downloads.teradata.com/download/connectivity/net-data-provider-for-teradata <p>Note: Work with your DBA group to obtain the drivers needed</p>

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 **System Settings** section of AppDetectivePRO. Updates are also available for download from the Support Portal, at: <https://portal.trustwave.com>.

Product Support Lifecycle

Trustwave's Database Security Product Support Lifecycle is 18 months.

Product versions older than 18 months are generally unsupported. For your convenience, a recent product support matrix is included below.

Version upgrades are available to all customers that have a current and valid software subscription. Upgrading is only allowed from supported versions. Also, session import functionality is only allowed if exported from a supported version.

Clients running unsupported software are strongly encouraged to plan for an upgrade or fresh installation of their licensed software. Newer releases of software offer better performance, new features and capabilities, and often resolve issues experienced in older releases of software.

Product Support Lifecycle

Version	Software Release Date	End of Support Date
AppDetectivePRO 10.8	10/31/2023	04/31/2025
AppDetectivePRO 10.7	07/31/2023	01/31/2025
AppDetectivePRO 10.6	05/31/2023	11/30/2024
AppDetectivePRO 10.5	01/16/2023	06/16/2024
AppDetectivePRO 10.4	06/30/2022	12/30/2023

Customer Support

You are welcome to contact Trustwave Technical Support for any questions or concerns arising from operation of the product. For the various ways to contact us, please visit <https://www.trustwave.com/Company/Support/>.

Understanding the AppDetectivePRO User Interface

The user interface allows you to see different sections at a time. It has three main areas where you can perform different tasks: **Sessions**, **Policies**, and **System Settings**.

- **Sessions:** manage assets and perform all your different scans, review results, and run scan reports
- **Policies:** view how the built-in policies are configured and create any custom policies
- **System Settings:** configure users of the product, run **ASAP Updates**, and change other settings

When working in **Sessions** and **Policies**, you see data laid out in a grid control format. At any time, you can choose to sort and group by different attributes of the data you are viewing by dragging and dropping the attributes from the top row.

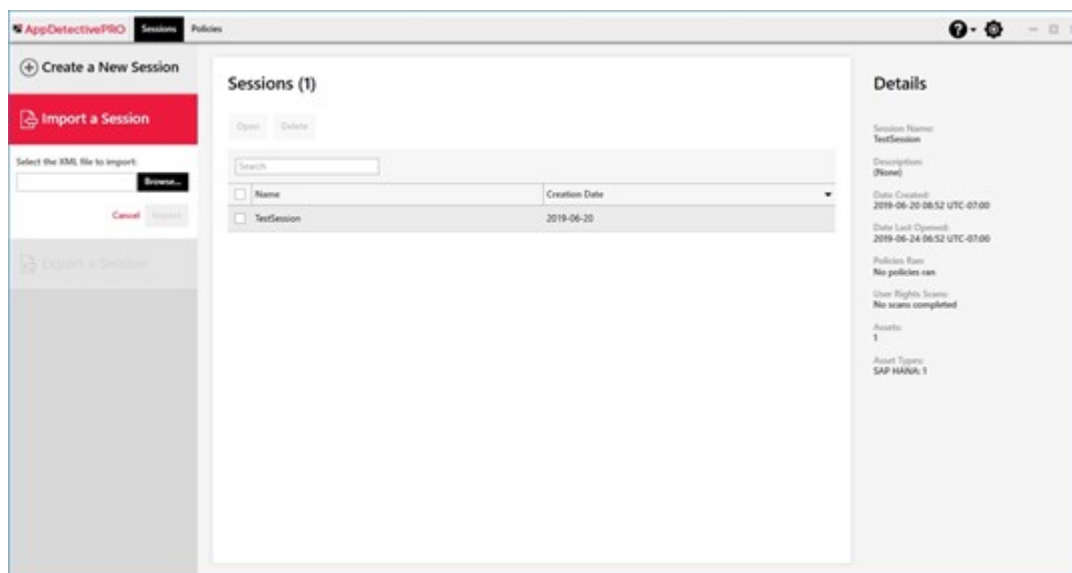
Working in Sessions

When you create a new session or open an existing session, you can view the data in a single session at a time. Multiple sessions cannot be opened at a time.

Sessions can be exported from AppDetectivePRO and imported back into it. Exported sessions can be used to back up the data to be imported at a later date or be used to import to another installation of AppDetectivePRO.



Note: The session import functionality is only allowed if exported from a supported version (see [Product Support Lifecycle](#)).



Sessions are made up of different sections: **Assets**, **History**, **Policy Results**, and **User Rights Results**.

You can lock a session with a password. You will be prompted for the password when you open, delete or export the session.



Note: The password is not part of the session data. Sessions that are exported are not locked.

Assets

Assets are any target database you input into a session. Assets can be discovered, added manually, or imported using a CSV file. Once assets are added to your session you can perform different types of scans against them.

Asset Name	IP Address / Hostname	Port	Database	Platform	Version	Scan Status
10.25.241.8 on 50001 (db2inst1SAMPLE)	10.25.241.8	50001	db2inst1SAMPLE	IBM AIX	DB2 9.7	
10.25.241.7 on 50000 (db2inst1SAMPLE)	10.25.241.7	50000	db2inst1SAMPLE	IBM AIX	DB2 9.7	
10.25.241.9 on 50000 (db2inst1SAMPLE)	10.25.241.9	50000	db2inst1SAMPLE	Linux	DB2 11.1	
10.25.241.0 on 49318 (SQL2012)	10.25.241.0	49318	SQL2012	Microsoft Windows	Microsoft SQL Server 2012	
10.25.241.5 on 1433 (MSSQLSERVER)	10.25.241.5	1433	MSSQLSERVER	Microsoft Windows	Microsoft SQL Server 2005	
10.25.241.10 on 3341 (SQL2K8R2)	10.25.241.10	3341	SQL2K8R2	Microsoft Windows	Microsoft SQL Server 2008 R2	Policy (r)

Banner Information

Last Policy Scan

TestPolicy
 Start Time: 2019-06-26 07:21 UTC-07:00
 End Time: 2019-06-26 07:22 UTC-07:00

10.25.241.7 on 5000 (aix1_1502) | 10.25.241.7 | 5000 | aix_1502 | Unknown Platform | Sybase 15.0 Database


Discover

To run a discovery, select the **Discover** button in the UI. This opens a wizard that prompts you to insert certain information, such as an IP address, ports, and detection options that will be used to run the discovery against. The discovery performs a combination of an IP/Port sweep and an intelligent database detection to accurately identify the assets to add to the Session.



Note: Versions of Oracle 10g or greater may not be discovered. If TCP/IP or Browser Services are not enabled on Microsoft SQL Server, then discovery may not identify the instances. If the DB2 Admin Server is not running, then the discovery of IBM DB2 LUW databases may not be discovered. Microsoft Azure SQL Database are not supported for discovery. To add these to the Asset list, use the **New Asset** option.

New Asset

To manually add an asset, select the **New Asset** button in the UI. This allows you to enter information about the target database you want to add as an asset. You can test the database connection to the target by supplying credentials. If the test connection is successful you see a green “plug” icon  under the **Audit** column in the grid. This test checks that you can connect to the asset. It does not verify the credentials needed to run an **Audit** policy.



Note: When creating a new Oracle asset, you have the option of setting up the connection with the SID or Service Name. When creating a new Microsoft SQL Server asset, you have the option of setting up the connection with Port/Instance or Named Pipe. Once a policy or user rights scan is completed against the asset, the license is tied to that asset. Changing between connection types (SID vs Service Name or Port/Instance vs Named Pipe) will be treated as a new asset.

Import

To import a list of assets, select the **Import** button in the UI. This allows you to select a CSV file with information to add assets to the session. You can select the **View sample file** link to see an example. Here are more details on formatting the CSV file:

The file should include the following information:

```
"Name", "Host", "Port", "PipeName", "Type", "Platform", "Version", "InstanceName", "
DatabaseName", "OracleSIDName", "OracleServiceName"
```



Notes:

- PipeName is only to be used for Microsoft SQL Server. If used, Port and InstanceName are not to be specified.
- OracleServiceName is only to be used for Oracle. If used, OracleSIDName is not to be specified.

Here are examples for different asset types:

- Microsoft SQL Server:
 - Example using Microsoft Azure


```
"ASMI-SQLServer",
"foobarasml.public.01dcf250e159.database.windows.net", "3342", "",
"Microsoft SQL Server", "Microsoft Windows", "Microsoft SQL Server
2014", "", "", "", "", ""
```
 - Example using Port and InstanceName

```
"Share Point", "10.25.244.24", "1433", "", "Microsoft SQL Server",
"Microsoft Windows", "Microsoft SQL Server 2012", "MSSQLSERVER", "", "",
"", ""
```

- Example using PipeName

```
"Company Wiki", "10.25.245.135", "", "MSSQL$MSSQL2K5INST2\sql\query",
"Microsoft SQL Server", "Microsoft Windows", "Microsoft SQL Server
2005", "MSSQL2K5INST2", "", "", "", ""
```

- Oracle

- Example using OracleSIDName

```
"E-Business 1", "10.25.244.42", "1521", "", "Oracle", "Microsoft
Windows", "Oracle11gR2 Database", "", "", "orcl11g2", "", ""
```

- Example using OracleServiceName

```
"ERP App", "10.25.245.113", "1521", "", "Oracle", "Linux", "Oracle12c
Database", "", "", "", "pdb1.qany.prv", ""
```

- IBM DB2 LUW

```
"DB2 Test", "10.25.244.13", "50000", "", "IBM DB2 LUW", "Microsoft Windows",
"DB2 9.7", "DB2", "SAMPLE", "", "", ""
```

- MySQL

```
"10.25.244.81 on 3306 ()", "10.25.244.81", "3306", "", "MySQL", "Linux",
"MySQL 5.6 Database", "", "", "", "", ""
```

- SAP ASE Server

```
"Sybase-16-Asset", "tgt-syb-ssl.nycapt35k.com", "5000", "", "SAP ASE", "Microsoft
Windows", "SAP ASE 16", "", "", "", "", ""
```

- Redis Server

```
"tgt-redis-7-2-tls-ulx22.nycapt35k.com on 6379 ()", "tgt-redis-7-2-tls-
ulx22.nycapt35k.com", "6379", "", "Redis", "Linux", "Redis", "", "", "", ""
```

- Microsoft Azure SQL Database

```
"myAzure", "168.62.32.75", "1433", "", "Microsoft Azure SQL Database",
"Microsoft Azure", "Microsoft Azure SQL Database 11", "", "master", "", "",
""
```

- Teradata Database

```
"myTeradata", "192.168.2.25", "1025", "", "Teradata", "Linux", "Teradata
16.20", "", "", "", "", ""
```


- MongoDB

```
"mongodb-host on 27017 ()", "mongodb-host", "27017", "", "MongoDB", "Linux",
"MongoDB 3.2", "", "", "", "", ""
```

- Cassandra

```
"Cassandra-4", "mad-cassandra-
olx8.nycapt35k.com", "9042", "", "Cassandra", "Linux", "Cassandra
4", "", "", "", "", ""
```

- PostgreSQL

```
"postgresql-host on 5432 ()", "postgresql-host", "5432", "", "PostgreSQL",
"Unknown Platform", "PostgreSQL", "", "postgres", "", "", ""
```

- MariaDB

```
"mariadb on 3306()", "10.25.240.69", "3306", "", "MariaDB", "Linux",
"MariaDB 10.5", "", "", "", "", ""
```

- Percona Server for MySQL

```
"10.25.244.69 on 3306 ()", "10.25.244.69", "3306", "", "Percona Server for
MySQL", "Linux", "Percona Server for MySQL 5.7", "", "", "", "", ""
```

- Databases on Amazon Web Services (i.e. MySQL, PostgreSQL, Oracle)

```
"Amazon Web Services", "mydbinstance.cycgnfvxfrep.us-
west-2.rds.amazonaws.com",
"3306", "", "MySQL", "Amazon Web Services", "MySQL 5.7 Database", "", "",
"", "", ""
```

The following tables list some of the possible options for **Asset Type**, **Platform (OS)**, and **Version**.



Note: You can always change the value of any of the imported assets using the **Edit** option after the import is complete.

Asset Type

Asset	Value to use in the file
Microsoft SQL Server	Microsoft SQL Server
Oracle	Oracle
IBM DB2 LUW	IBM DB2 LUW
MySQL	MySQL
Microsoft Azure SQL Database	Microsoft Azure SQL Database
Teradata	Teradata
MongoDB	MongoDB

Asset	Value to use in the file
MariaDB	MariaDB
Percona Server for MySQL	Percona Server for MySQL
SAP ASE	SAP ASE
Redis	Redis

Platform (OS) Value (not all options listed)

Operating System	Value to use in the file
Windows	Microsoft Windows
Linux	Linux

Database Value

Database Version	Value to use in the file
Oracle 19c	Oracle 19c Database
Microsoft SQL Server 2014	Microsoft SQL Server 2014
Microsoft SQL Server 2016	Microsoft SQL Server 2016
Microsoft SQL Server 2017	Microsoft SQL Server 2017
Microsoft SQL Server 2019	Microsoft SQL Server 2019
IBM DB2 LUW 11.5	DB2 11.5
PostgreSQL 11.0	PostgreSQL 11.0
PostgreSQL 11.1	PostgreSQL 11.1
PostgreSQL 11.2	PostgreSQL 11.2
PostgreSQL 11.3	PostgreSQL 11.3
PostgreSQL 11.4	PostgreSQL 11.4
PostgreSQL 11.5	PostgreSQL 11.5
PostgreSQL 11.8+	PostgreSQL 11.8+
PostgreSQL 12	PostgreSQL 12
PostgreSQL 13	PostgreSQL 13
PostgreSQL 14	PostgreSQL 14
MySQL 5.7	MySQL 5.7 Database
MySQL 8.0	MySQL 8.0 Database
Microsoft Azure SQL Database	Microsoft Azure SQL Database 11
Teradata 17.05	Teradata 17.05
Teradata 17.10	Teradata 17.10
Teradata 17.20	Teradata 17.20
MongoDB 4.4	MongoDB 4.4
MongoDB 5.0	MongoDB 5.0

Database Version	Value to use in the file
MariaDB (any version)	MariaDB
Percona Server for MySQL 5.7	Percona Server for MySQL 5.7
Percona Server for MySQL 8	Percona Server for MySQL 8
SAP ASE	SAP ASE
Redis	Redis
Redis 7	Redis 7

Edit

At any time, you can edit an asset in the session. Mark the check box next to the asset and the **Edit** button is enabled. You can edit the platform type, version, or asset name of any discovered asset. You can edit the platform type, version, asset name, hostname, port, or instance name of any asset manually added or imported. You can also test the database credentials of any asset.



Note: OS detection is not always available with discovery based on the configuration of the target database. You can always edit the platform (OS) using the edit option. Some checks rely on understanding the platform (OS) to run properly. If you imported a list of assets and you see something listed as “Unknown”, you can use the **Edit** option to enter the correct value.

Filter

The filter allows you to sort out the assets in the **Asset** list. You can choose to filter by asset type or by keywords you can enter in the search box.

Report

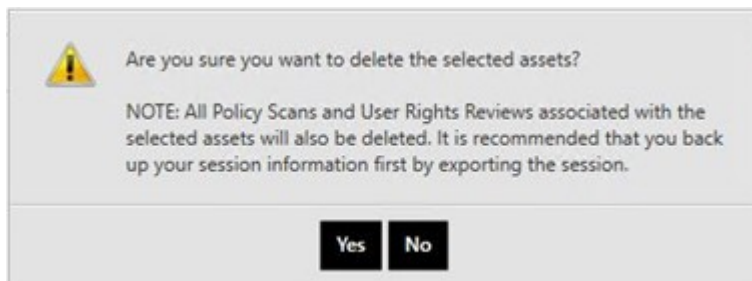
At any time, you can generate an **Asset Inventory Report**. Select the asset(s) from the grid to include in the report. You have the option of including banner information if it was collected during discovery in the report. The report is available in AppDetectivePRO report viewer format which can be exported to PDF or as a CSV file. The CSV file can also be used to import assets into another session.

Delete

At any time, you can delete an asset in the session. Mark the check box next to the asset(s) and the **Delete** button is enabled.



Note: If you have any scan results data associated with the asset, this data will also be deleted. You will be prompted with a warning message to confirm that you want to proceed with the deletion.



Run Policy

After assets are added to the session, you can run policy scans against them. Mark the check box next to the asset(s) you want to run the policy scan against and click the **Run Policy** button. There are three types of policies that can be run: Audit, Pen Test, and Application Scan.

Audit

After clicking **Run Policy**, you see a list of Audit policies. Select a policy and then enter the database credentials for the asset(s). Use the scroll bar and then also enter the OS credentials if your policy requires OS access. Some controls and checks require OS access to perform its configuration analysis. If you have a policy that requires this, make sure you also test the OS credentials prior to running the scan.

Notes:



- In this version of AppDetectivePRO, you no longer select a specific DISA STIG or CIS framework (the selection is no longer available). When you select either the CIS NEW or the DISA-STIG NEW policy, the appropriate framework will be used on the asset(s) selected. Do not use the **CIS Benchmark – Audit (Built-in)** or **DISA-STIG Database Security – Audit (Built-in)** policies if you have been scanning using specific frameworks in previous versions.
- In this version of AppDetectivePRO, you have the option to collect database users' information when selecting an Audit policy. Mark the checkbox prior to clicking **Next** for this option. This option requires database credentials with privileges to collect **User Rights Review** information. Results from this collection of database users' information can be viewed in the **User Rights Results** section within the **Users** view. See [User Account Privileges Needed for Audit and User Rights Review Scans](#) for more information.

Next, there are options you must choose from to move forward:

- **Test Connection:** This will test that AppDetectivePRO can connect both to the target DB and OS using the credentials supplied.
- **Test DB only:** This will test the connection using the DB credentials supplied.
- **Test OS only:** This will test the connection using the OS credentials supplied.

Verify permissions are enough to run this scan: Selecting this option will verify the credentials supplied when using any of the test options above.

Successful test connection for the database credentials is mandatory to start the audit policy scan for all assets, except DynamoDB. A successful test connection of AWS credentials is mandatory for DynamoDB.



Note: For guidance on the privileges required to run Audit policy scans, see [User Account Privileges Needed for Audit and User Rights Review Scans](#).

Pen Test

You can also choose to run Pen Test policies.

Within the **Run Policy** section, you see a **Pen Test** option next to **Audit**. Pen Test policies do not require database credentials to run. You can run a Pen Test against any discovered assets or assets that have been verified (meaning that you have already successfully tested the database credentials for the assets). If you manually entered or imported the assets and do not know the database credentials, you can verify the asset by running a discovery against it. As with the Audit policy, you will see a **Test** button. Click this button to run a discovery on the single selected asset, to attempt to verify it. Once an asset is verified, you can run the Pen Test policy scan.

Notes:



- You can run up to fifteen concurrent policy scans. The performance of the scans will depend on the amount of RAM allocated at the time of the scan.
- Encrypted connections are not supported for Pen Tests.
- You can cancel all concurrent policy scans by using the cancel option at the overall progress bar. You can cancel a scan for an asset by hovering over the **Scan Status** of the asset in the **Assets** grid and selecting the **Cancel** option.

Run User Rights

You can run User Rights scans against assets. To do so, mark the checkbox next to the asset(s) you want to run the scan against, and click the **Run User Rights** button.

After clicking **Run User Rights**, you will be prompted to enter the database credentials for each of asset(s) you marked to scan. As with the **Run Policy** scan, you will test the connection to the database and verify the credentials have sufficient privileges to perform the scan.



Note: For guidance on the privileges required to run Rights Review scans, see [User Account Privileges Needed for Audit and User Rights Review Scans](#) for more information.

Run Now and Run Later Option

There are two options when you want to run a policy or a user rights review scan:

- **Run Now:** This option will immediately run your policy or user rights review scan.
- **Run Later:** This option will allow you to run your policy or user rights review scan(s) within a 24-hour period. You can select a time within the next 24-hour period when the scan should run, in half hour increments. You can have a total of 15 scans set using the Run Later option at any given time.



Caution: If you use the **Run Later** option, you must leave AppDetectivePRO open in the session where the scans are configured to run later. Closing the application will remove any credentials entered and any time specified for the **Run Later** option.

History

To see what actions you have performed in your session, click the **History** section. History captures some information about the actions you performed in your session.

- If you added an asset, it displays in the **History** list.
- If you ran a discovery, you see an entry showing the details of the asset the discovery scan ran against. You can expand the entry to see all the components discovered beyond the asset (for example, Oracle Listener or Microsoft SQL Server Redirector).
- If you ran a policy scan, you see an entry as well. Expanding the details for a policy scan will display any failed or skipped result status and any associated error message.

Drag a column header here to group by that column		
Action Information	Asset	Execution Time
Policy: TestPolicy against database: 10.25.241.10 on 3341 (SQL2KBR2)	10.25.241.10 on 33...	2019-06-26 07:21 UTC-07:00 to 20...
Deleted asset: sha-hana-rhel7.nycapt35k.com	sha-hana-rhel7.nyc...	2019-06-26 07:13 UTC-07:00
Deleted policy results: TestPolicy2 (framework: testframework) 2019-06-21 07:17 UTC-07:00 to 2019-06-21 07...	sha-hana-rhel7.nyc...	2019-06-26 07:13 UTC-07:00
Discovery ran		
Addresses: 10.25.241.0 - 10.25.241.10 Asset Types: Microsoft SQL Server, Oracle, Sybase ASE, IBM DB2 LUW, MySQL, IBM DB2 z/OS, Teradata, Mong...		2019-06-26 06:56 UTC-07:00 to 20...
Ports: default Live Host Detection: skip		
Discovery cancelled		
Addresses: 10.25.240.0 - 10.25.240.255 Asset Types: Microsoft SQL Server, Oracle, Sybase ASE, IBM DB2 LUW, MySQL, IBM DB2 z/OS, Teradata, Mong...		2019-06-26 06:18 UTC-07:00 to 20...
Ports: default Live Host Detection: skip		
Policy: TestPolicy2 against database: sha-hana-rhel7.nycapt35k.com - policy failed to run Exception message: Audit not supported for Hana	sha-hana-rhel7.nyc...	2019-06-21 07:17 UTC-07:00 to 20...
Added asset sha-hana-rhel7.nycapt35k.com	sha-hana-rhel7.nyc...	2019-06-21 07:12 UTC-07:00 to 20...
Discovery ran (no results found)		
Address: 10.76.180.137 Asset Types: Teradata Port: 1025 Live Host Detection: skip		2019-06-20 08:57 UTC-07:00 to 20...

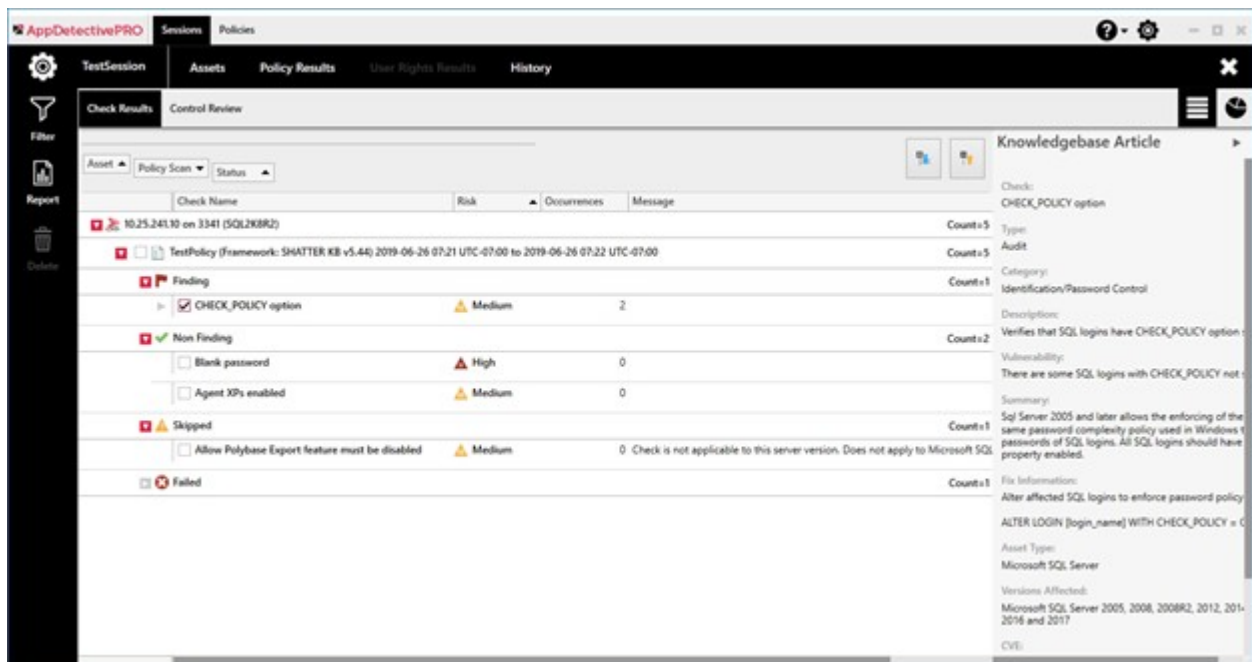
Policy Results

To see the results for your Policy scans, go to the **Policy Results** section.

Check Results

This section becomes enabled only after a successful policy scan is performed against an asset. When you click **Policy Results** the default view of **Check Results** (Informational view) is displayed, 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. If you want to see a graphical representation of the results, choose the **Graphical** view option on the upper right.

If there are any policy scans that you want deleted from the session, mark the check box of the policy scan in the grid and click the **Delete** button on the side toolbar. This action is only available when the **Filter** and **Report** options are collapsed.



Understanding the Check Results Filter

The filter allows you to sort out the data you want to view for any asset with policy results. You can select from the following attributes and click **Filter** to see your desired results. If you click **Clear**, the selection in the filter is removed and shows all possible policy results for all assets.

- **Search:** filter by text anywhere in the entire grid of results. Enter text to search for.

- **Assets and Policies:** filter by asset or specific policy scan. If you select the asset, it will display all the policy results for the selected asset. If you select a specific policy scan, it will display the results only for the one selected.
- **Risk Level:** filter by Risk level of the check: High, Medium, Low, and Informational.
- **Result Type:** filter by the state of the check after the policy scan was executed.
 - **Failed:** the check failed and was not fully executed. The most common error that results in a failed state is that the account used for the audit scan had insufficient privileges to the object needed for review.
 - **Skipped:** the check was skipped because it does not apply to the particular version of the asset, so no review needs to be performed.
 - **Finding:** the check returned a system result that captures a violation.
 - **Non Finding:** the check returned a system result that captures an absence of a violation.
 - **Fact:** the check returned a system result that is informational without positive or negative orientation.

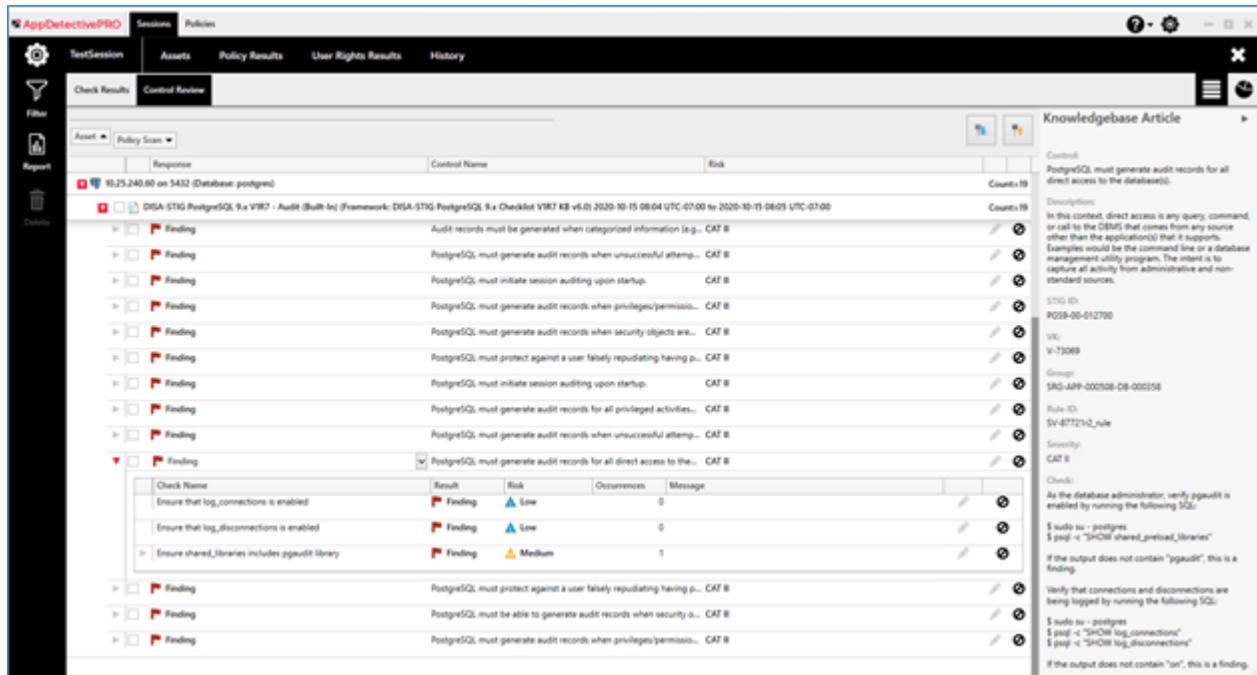
Examples of Checks and Result Types

Check	Result Type	Details
Permissions of files (Sybase)	Failed	Check "Permissions on files" execution failed since we are unable to get the required data: Access is denied. [The check failed because insufficient or no OS credentials were provided]
Auditing of successful logins (Sybase)	Skipped	Auditing subsystem does not seem to be installed.
Software owner umask setting (Oracle)	Skipped	Check is not applicable to this server version.
Default password for Oracle	Finding	When a Finding is returned, the details for this check list the accounts that are in violation (for example. DBSNMP, SCOTT, OUTLN).
Blank password for sa (Microsoft SQL Server)	Non Finding	No details are produced as the check "passed". The check produced no violation found (meaning that the sa account does not have a blank password).
Guest user exists in database (Sybase)	Fact	The details for this check list the system databases that have guest user, if any (such as master, tempdb).

Control Review

The other available view in **Policy Results** is the **Control Review**. Use the **Control Review** to review the controls from the Policy scan that was conducted. You can add notes and suppress at all levels of the control (control, check result, or check result occurrence).

If there are any policy scans that you want to delete from the session, mark the check box of the policy scan in the grid and click the **Delete** button from the side toolbar. This action is only available when the **Filter** and **Report** options are collapsed.



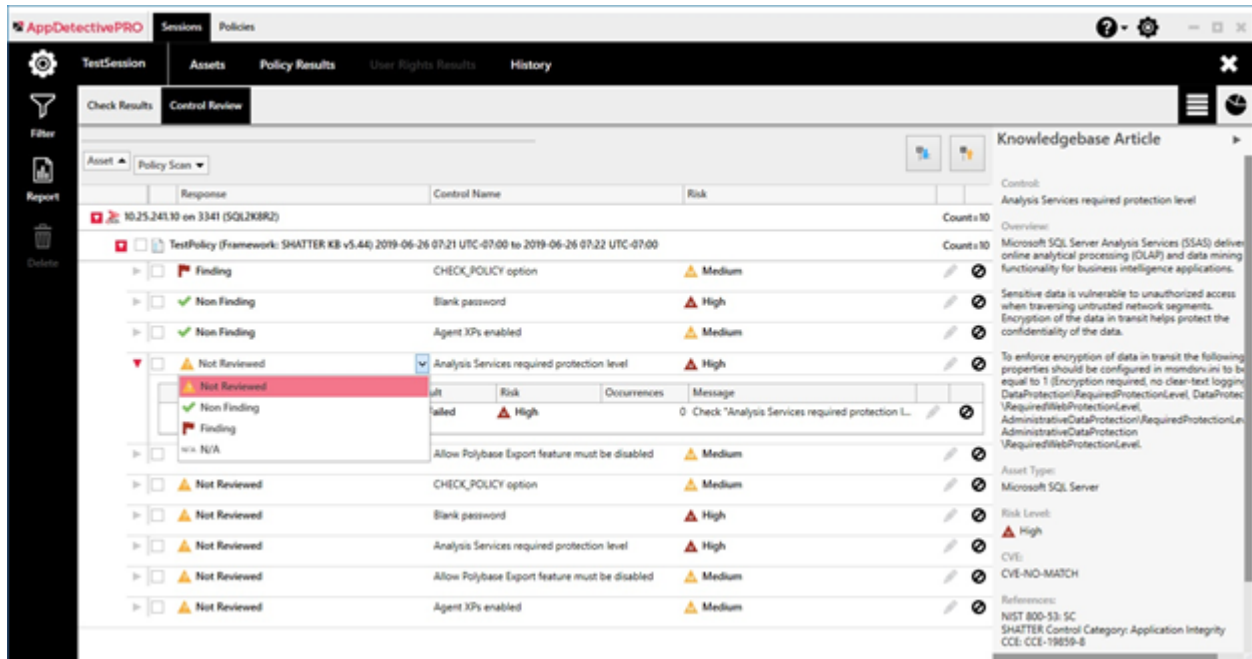
Using the Control Review Feature

By default, the **Control Review** section is grouped by **Asset**, then by **Policy Ran**. You can choose to drag any of the column headers to change the grouping.

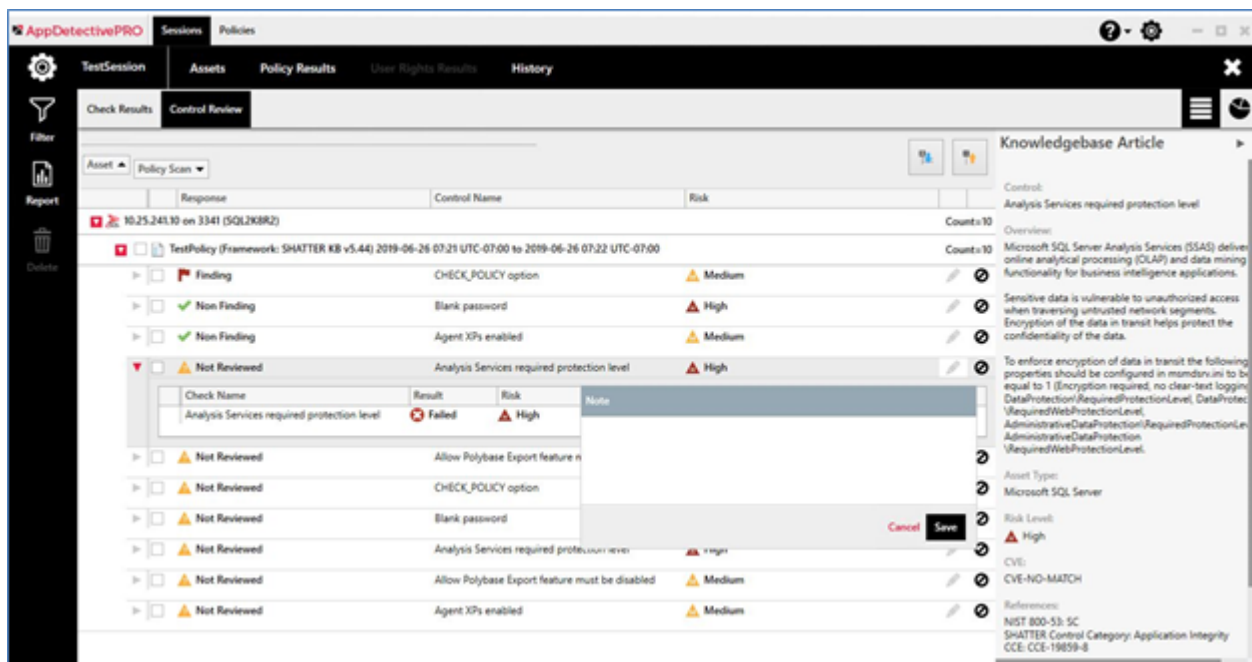
The **Control Review** presents the controls based on your framework and allows you to change the **Response Type** for any of the controls. If there is any check associated to the control, logic is applied to the initial **Response Type** you view.

- If a check resulted in a **Finding**, then the **Response type** will be made a **Finding**.
- If a check resulted in a **Non Finding**, then the **Response type** will be made **Non Finding**.
- If a check result is **Skipped** or **Failed**, then the **Response type** will be made **Not Reviewed** (leaving it up to you to change the type as you see fit).
- If a control has more than one check associated with it and at least one of the checks resulted with a **Finding**, then the **Response type** will be made a **Finding**.

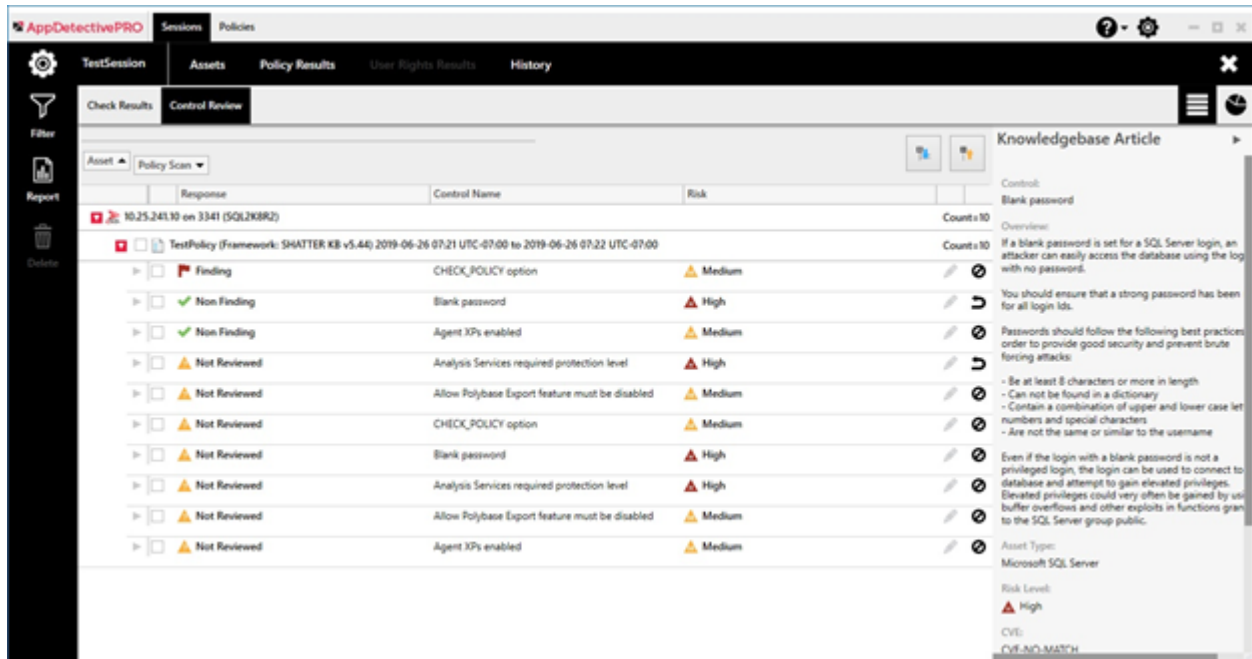
To change a **Response type**, select the control and choose the drop down arrow under the **Response** column. The drop down will allow you to change the response.



Beyond changing the **Response type**, you will notice two other options you can use within the **Control Review** section. You can add any notes that you want by clicking on the pencil icon. You can add notes at any level of the **Control** hierarchy (**Control**, **Check**, and **Check Occurrence**).

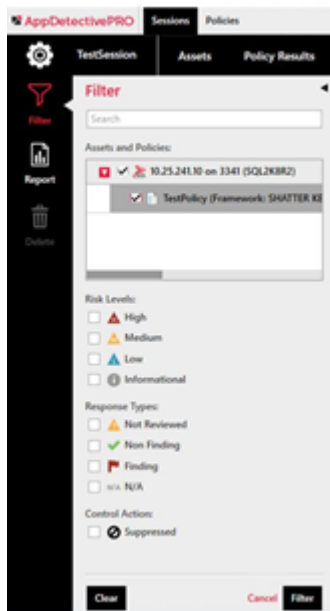


The other option is to suppress information. You can also do this at any level of the **Control** hierarchy (**Control**, **Check**, and **Check Occurrence**) by clicking on the circle icon next to the pencil icon. **Suppression** does not delete any data in your results; it only suppresses it from any report generated.



Understanding the Control Review Filter

Use this filter to sort out the data you want to view for any asset with policy results. You can select from the following attributes and click **Filter** to see your desired results. If you click **Clear**, the selection in the filter is removed and shows all possible Poly policy results for all assets.



- **Search:** filter by text anywhere in the entire grid of results. Enter text to search for.

- **Assets and Policies:** filter by asset or specific policy scan. If you select the asset, it will display all the policy results for the selected asset. If you select a specific policy scan, it will display the results only for the one selected.
- **Risk Level:** filter by risk level of the check: **High, Medium, Low, and Informational**



Note: The Risk Level filter does not apply to any DISA STIG framework.

- **Response Type:** This is the final response you have control over for the judgment of a control.
 - **Not Reviewed:** review the control and create your final response.
 - **Non Finding:** you have reviewed the control and do not think it has an issue.
 - **Finding:** you have reviewed the control and have an issue that is a violation of the control.
 - **N/A:** the control is not applicable and you choose not to provide a definite response.
- **Control Action:** If the check box is marked for **Suppressed**, the filter will include controls that have been suppressed in addition to the ones unsuppressed.

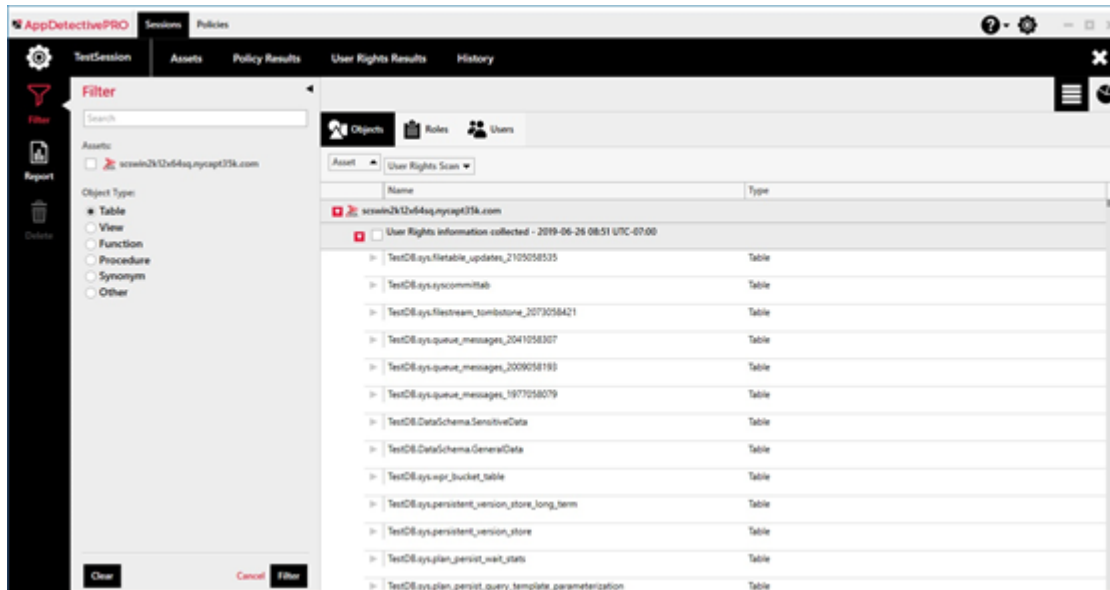
User Rights Results

After a Rights Review scan is performed, the **User Rights Results** section is enabled. When you navigate 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, and Users**) depending on the data to examine. The default view is by **Objects**. Use the **Filter** on the left to drill down to the data you want. Use the arrow to expand and review the details for each of the rows.

If there are any User Rights Scans that you want deleted from the session, mark the check box of the policy scan in the grid and click the **Delete** button from the side toolbar. This action is only available when the **Filter** and **Report** options are collapsed.

Object View

The **Objects** view allows you to view all the objects collected from **User Rights Review** scans. By default the results are grouped by the snapshot collected from each scan.



You can filter on the following:

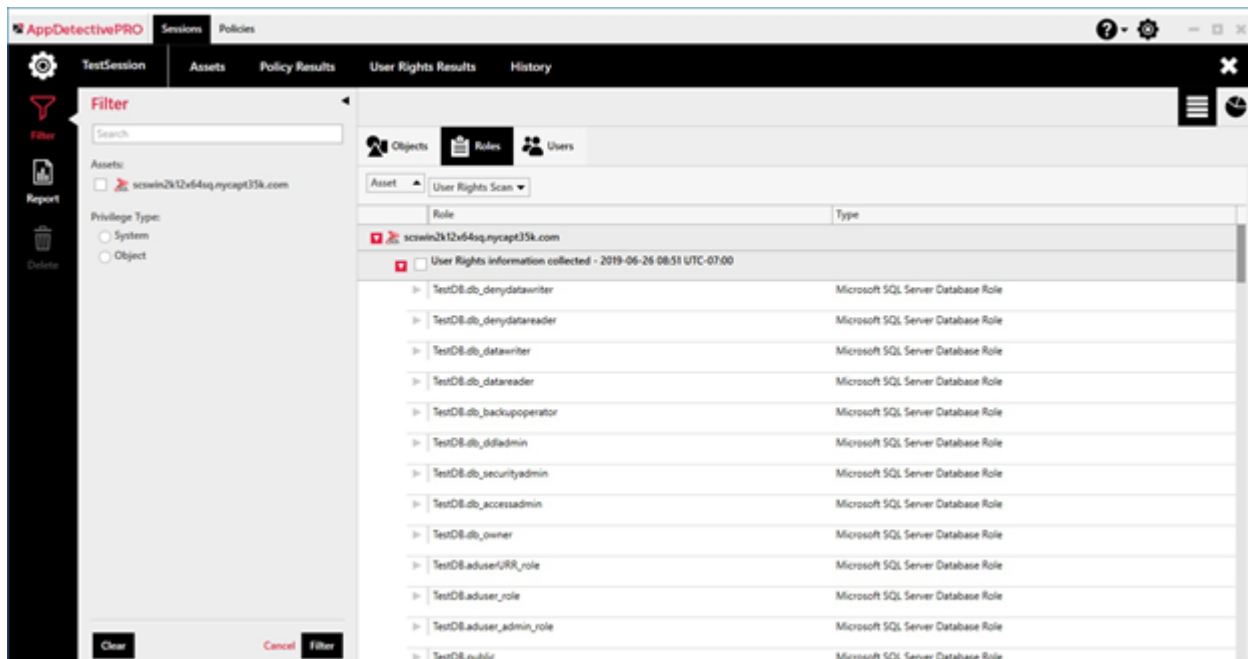
- **Search:** filter by text anywhere in the entire grid of results. Enter text to search for.
- **Assets:** filter by the asset and then provide you the results for all snapshots taken for that asset.
- **Object Type:** select the object type you want to filter the results on: **Table, View, Function, Procedure, Synonym, Other**

To view the details of an object, click the arrow next to the object. You will then see the **Object Access** of the selected object. The object access shows which users and roles have access to the object with the following columns:

- **Granted To:** The user/role that has access to the object.
- **Grantee Type:** The type of the user/role who inherits this privilege.
- **State:** The privilege state; for example, **GRANT**.
- **Privilege:** The type of privilege; for example, **SELECT, UPDATE, or EXECUTE**.

Roles View

The **Roles** view allows you to view all the roles collected from **User Rights Review** scans. By default, the results are grouped by the snapshot collected from each scan.



Using the filter, you can filter on the following:

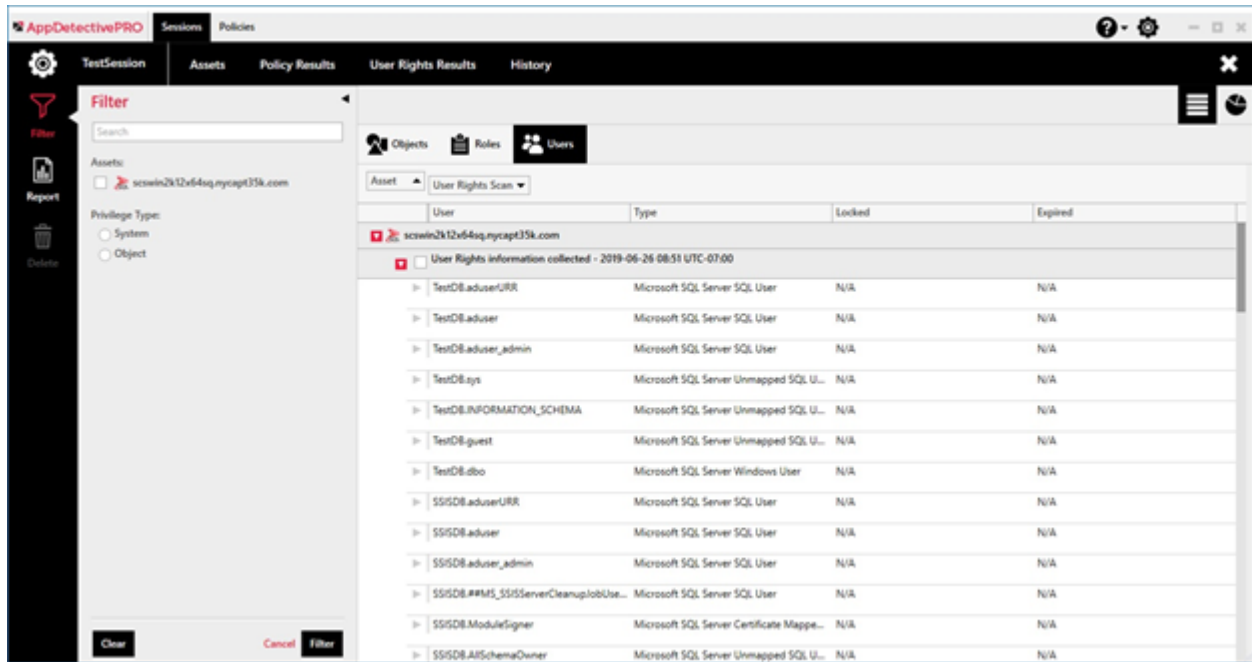
- **Search:** filter by text anywhere in the entire grid of results. Enter text to search for.
- **Assets:** filter by the asset and then provide you the results for all snapshots taken for that asset.
- **Privilege Type:** select the privilege type you want filter the results on: **System** or **Object**

To view the details of a role, click the arrow next to the role. You will then see the three sections:

- **Users:** displays all the users that are a member of the role. You will also see a column that specifies if the user was granted the role directly or indirectly.
- **Effective Privileges:** displays all the privileges effectively granted to the role. It also displays columns for **Privilege Type**, **Grant Path** (how the privilege was granted), and **Grantee Type**.
- **Roles:** displays all the roles that are granted to the role.

Users View

The **Users** view allows you to view all the users collected from **User Rights Review** scans. By default, the results are grouped by the snapshot collected from each scan.



Using the filter, you can filter on the following:

- **Search:** filter by text anywhere in the entire grid of results. Enter text to search for.
- **Assets:** filter by the asset and then provide you the results for all snapshots taken for that asset.
- **Privilege Type:** select the privilege type you want filter the results on: **System** or **Object**.

To view the details of a user, click the arrow next to the user. You will then see the two sections:

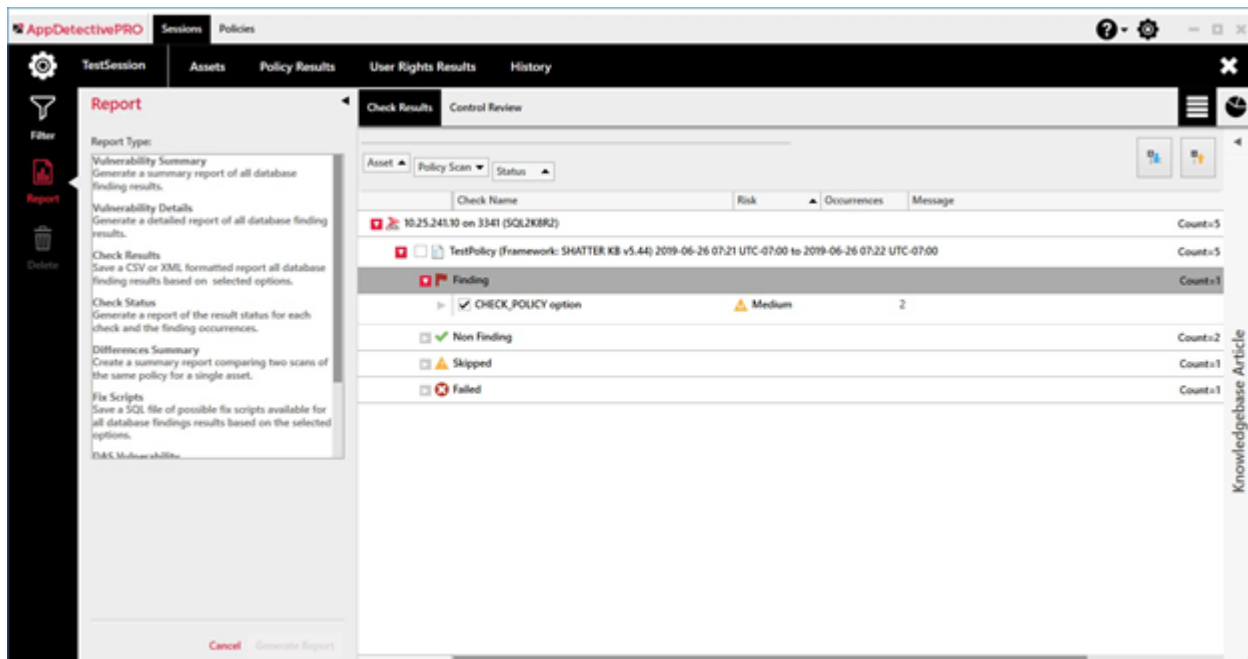
- **Roles:** displays all the roles that are granted to the user and where they are granted from.
- **Effective Privileges:** displays all the privileges effectively granted to the user. It also displays columns for **Privilege Type**, **Grant Path** (how the privilege was granted), and **Grantee Type**.

Reports

Generating reports works together with the filtered view of your scan results. You can generate reports based on whatever filter is currently applied to the data set. You can generate reports from the **Check Results** section, the **Control Review** section, and the **User Rights Review** section.

Generate Check Results Reports

After reviewing your check results data and filtering to the data set, select the checks you want to include in your report.



You can mark the check box at the **Policy Scan** level to include all the checks in the hierarchy or mark the checkboxes of the specific checks you want to include. After you have selected the data set, click the **Report** icon on the left tool bar.

The following reports are available:

- **Vulnerability Summary:** A summary report of all database finding results based on selected options in the filter. This will only report result type findings, even if your filter also contains other result types.
- **Vulnerability Details:** A detailed report of all database finding results based on the selected options in the filter. This will include all occurrence details of finding results. Like the summary report, this will only report on result type findings, even if your filter contains other result types.



Note: From version 8.6 you can choose to exclude exceptions information.

- **Check Results:** This report allows you to select from fields from the Knowledgebase Article to include in an XML or CSV formatted report. There is also an option to include the occurrence details.
- **Check Status:** A summary report of all checks and their result types based on the selected options in the filter. This will only include the result types you have filtered.
- **Differences Summary:** A summary report of the differences between two scans of the same policy against the same asset.

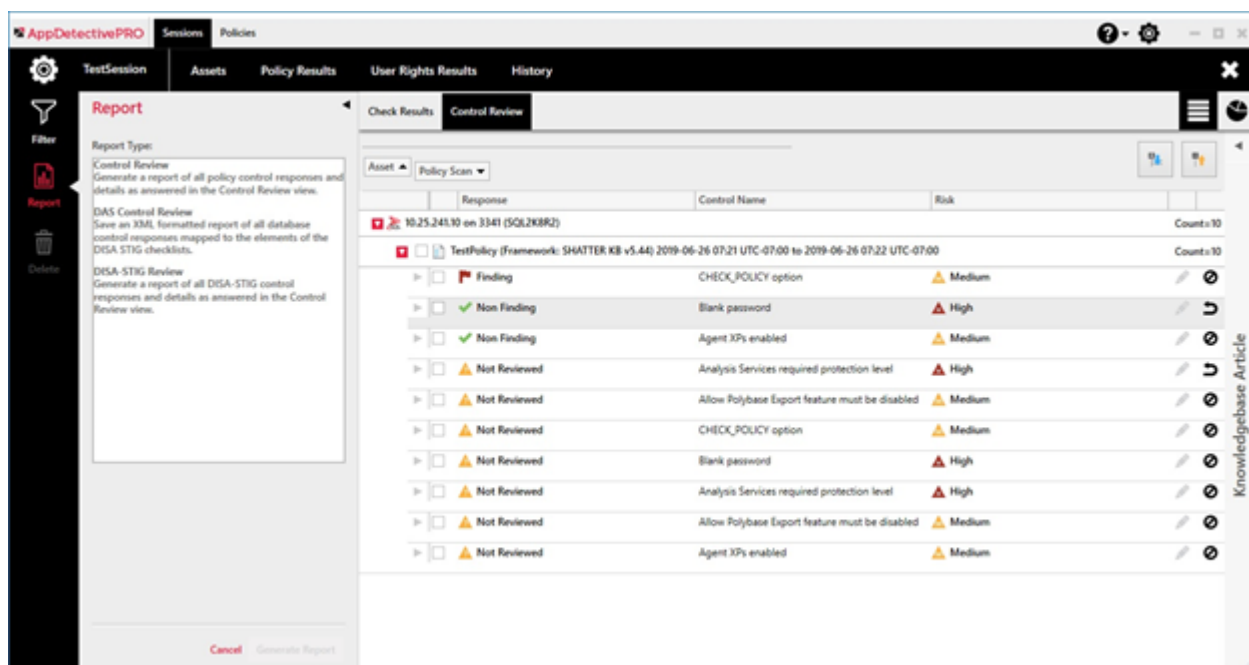


Note: To generate this report mark the checkboxes of two policy scans (same policy used) from the same asset. When selecting this report, the grid in the UI will collapse and show you what assets have valid policy scans for this report to generate.

- **Fix Scripts:** A detailed report of possible SQL statements to fix findings uncovered for an Audit policy. Fix Scripts do not apply to findings from a Pen Test policy ran. Not all findings have a related fix script.
- **DAS Vulnerability:** An XML formatted report of all database findings mapped to elements of the DISA STIG Checklist. This specific report is used to import details to the TMA TAD system.
- **DIACAP Vulnerability:** An XML formatted report of all database findings mapped to elements of the DISA STIG Checklist.

Generate Control Review Reports

After reviewing your **Control Review** data and filtering to the data set, select the controls you want generated in the report. You can mark the checkbox at the **Policy Scan** level to include all the controls in the hierarchy or mark the checkboxes of the specific controls you want to. After you have selected your desired results, click the **Report** icon on the left tool bar.

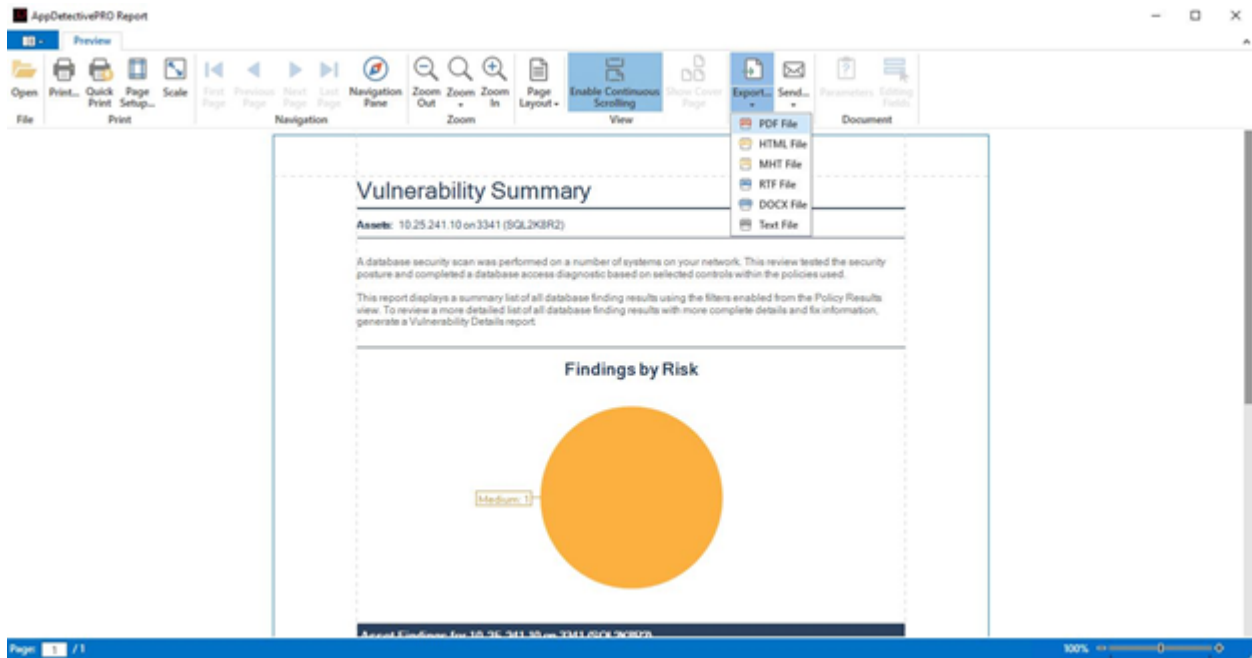


There are three reports available for generation:

- **Control Review:** A detailed report of all policy control responses and associated check result details.
- **DAS Control Review:** XML formatted report of all database control responses mapped to elements of the DISA STIG Checklist. This specific report is used to import details to the TMA TAD system.
- **DISA-STIG Review:** A detailed report of all policy control responses and associated check result details in complete DISA STIG context. You must run the DISA-STIG NEW policy or have results from DISA-STIG framework policies to generate this report.

Report Reviewer Options

The **Vulnerability Summary**, **Vulnerability Details**, **Check Status**, and **Control Review** reports all generate in a report viewer. The viewer provides viewing options such as search, zoom in and out, and print. It also allows you the ability to save the report in several formats including PDF, HTML, MHT, RTF, XLS, Text, and XPS.



Generate User Rights Review Reports

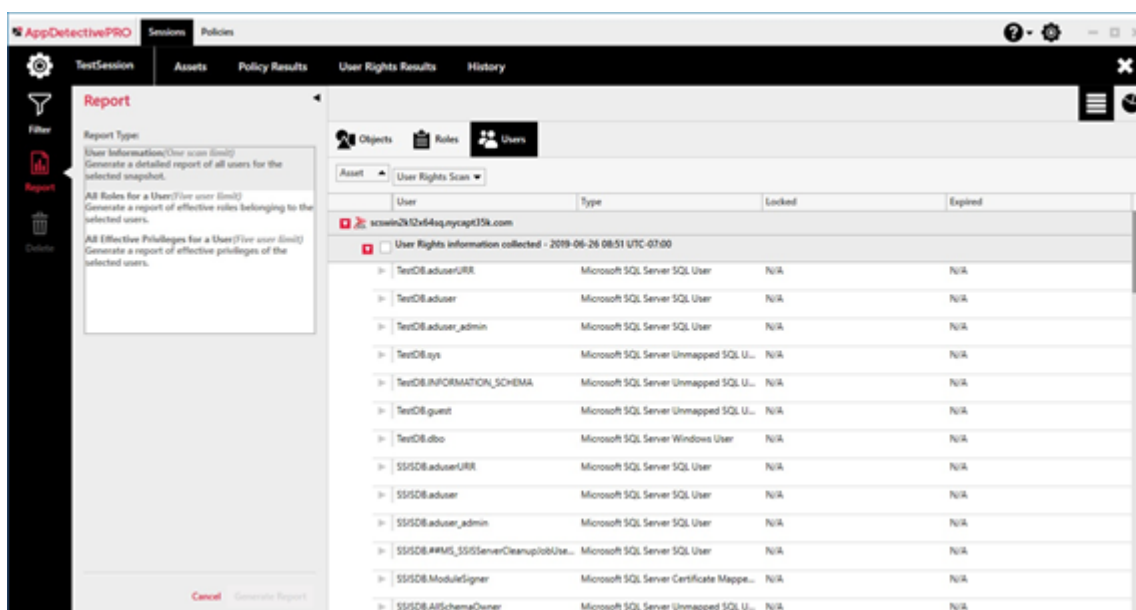
Different reports are available depending on the view you are in (Objects, Roles, and Users). All reports generated for User Rights Review results are created as a CSV file. Like the other results sections, click the **Report** icon to see the available reports.



Note: You must mark off the desired checkboxes in the results grid to generate any of the reports. You are limited to selecting five objects, roles, or users for any of the reports.

- **Objects View:** There are two available reports:
 - **Objects:** generates a list of all objects checked off in the results grid.
 - **Object Access:** generates a list of all the objects checked off in the results grid and all the details of how access was granted.
- **Roles View:** There are four available reports:
 - **Roles:** This report will generate a list of all roles checked off in the results grid.

- **All Effective Members for a Role(s):** This report will generate a list of all roles checked off in the results grid and the details of each user granted to the role.
- **All Roles for a Role(s):** This report will generate a list of all roles checked off in the results grid and the details of all roles granted to the role.
- **All Effective Privileges for a Role(s):** This report will generate a list of all roles checked in from the results grid and the details of each privilege granted to the role.
- **Users View:** There are three available reports:
 - **User Information:** This report replaces the old Users (CSV format) report from previous versions prior to version 8.4. This report will generate the list of all users from a selected User Rights Scan with detailed information about each user's status.
 - **All Roles for a User(s):** This report will generate a list of all users checked off in the results grid and the details of each role granted to the user.
 - **All Effective Privileges for a User(s):** This report will generate a list of all users checked off in the results grid and the details of each privilege granted to the user.



Working in Policies

Policies represent the complete list of items you want to review for your assessment. Policies are a list of all controls to be reviewed for the assessment. These controls may contain checks that will be analyzed during the scan process (Pen Test, Audit, Application Scan).

Policy scans (Pen Test, Audit, Application Scan) can be customized to either throttle up or down what you want to test for. Additionally, parameters and exceptions can be changed or added to match your environment settings.

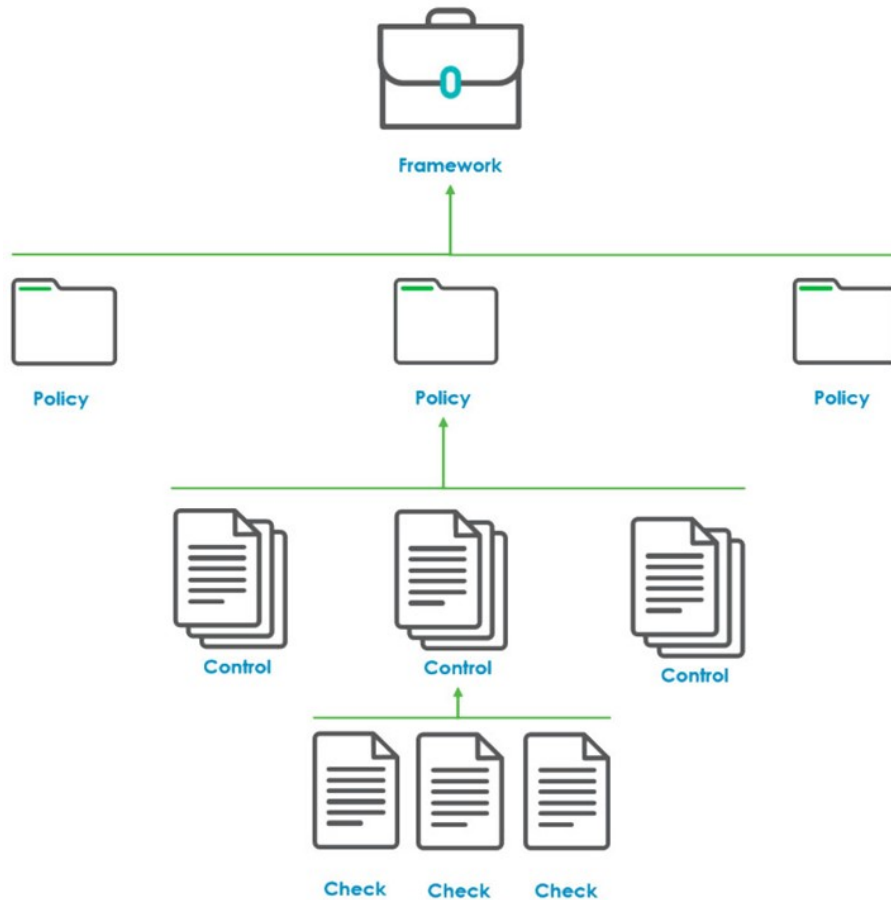
Custom policies can be exported from AppDetectivePRO and imported (back into the same installation, or into any other installation of AppDetectivePRO).

To work with Policies, select the **Policies** section from the top of the UI next to **Sessions**.

Use Frameworks, Controls, and Checks

Frameworks, controls, and checks help you to set up the ultimate 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 and CIS Benchmark frameworks with specific policies for different database types.
- 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 over 1,000 built-in checks that can be associated to any custom control.
- Checks are specific, executable tests that AppDetectivePRO runs against the database that provides results.



Policies

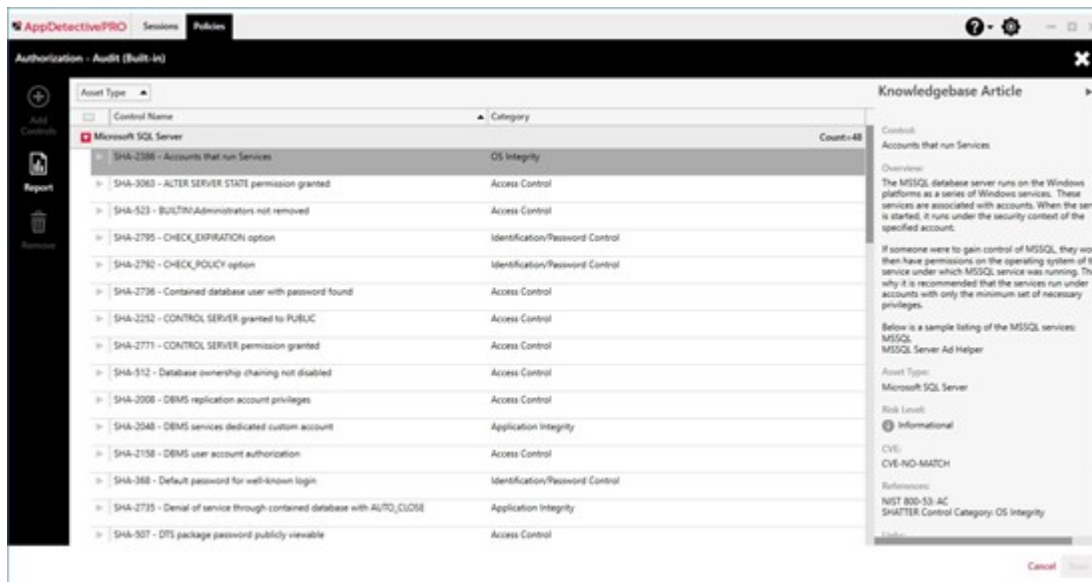
A policy is set up as either an Audit type, Pen Test type or Application Scan type. Policies include controls from within frameworks; that is, a policy can contain a sub-set of controls that you include from existing frameworks. A control can contain one or many checks. Essentially, a policy selects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

AppDetectivePRO includes built-in policies for all policy types.



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.

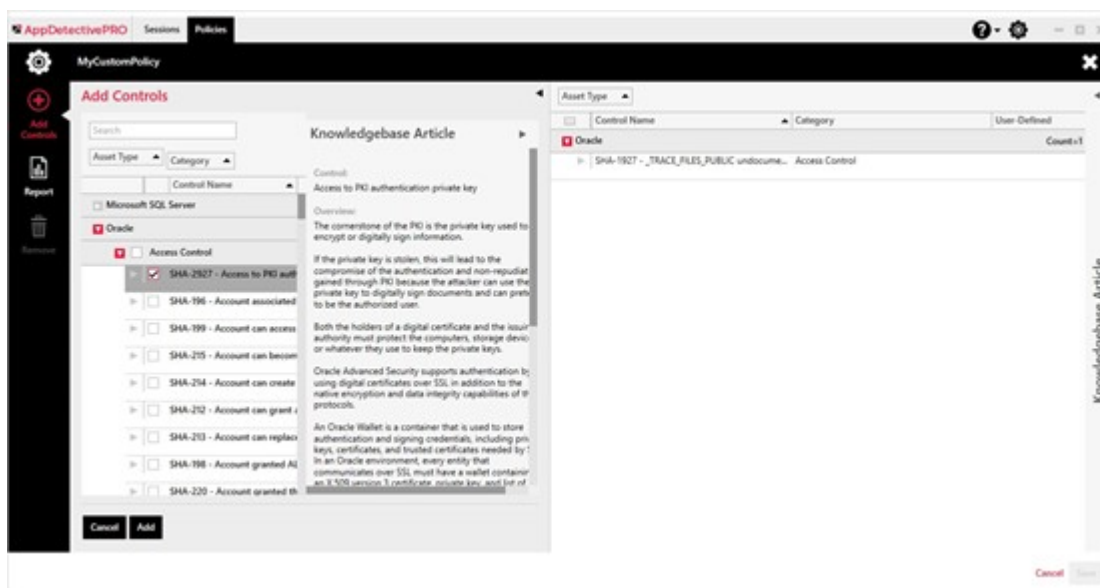
Within the **Policies** section, you open up any built-in policy and view what is included in it. You can also clone any built-in policy and customize it to your liking, as well as create any new custom policies. If you have any custom policies from another installation of AppDetectivePRO, you can import them as well.



Customize Policies

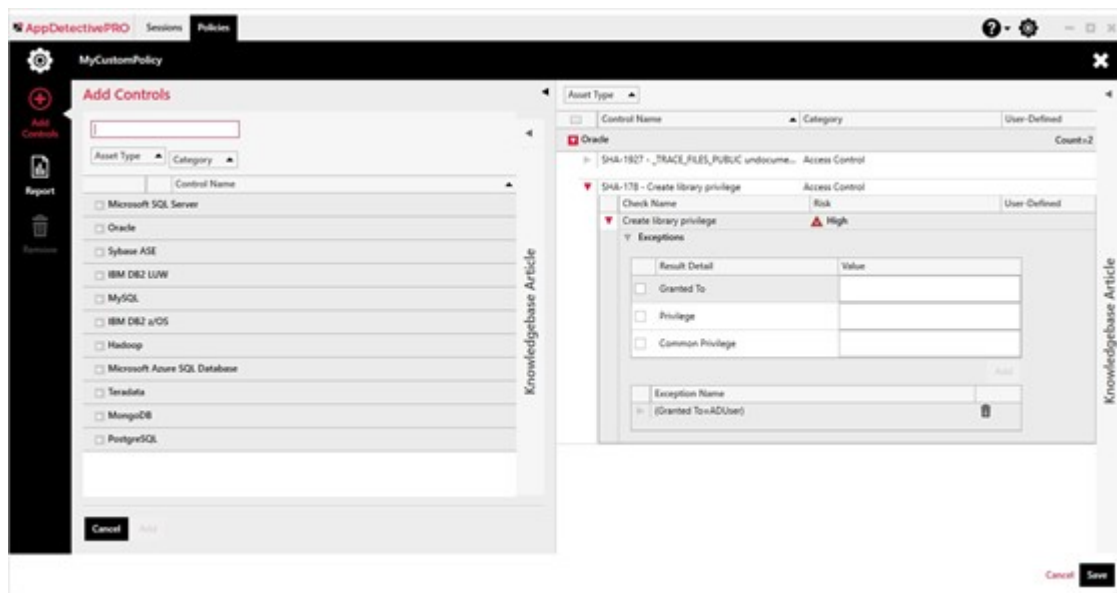
You can create a new policy or clone a policy and customize it to your own needs. To add controls, click the **Add Controls** icon in the left toolbar. This opens a grid of all possible controls not already included in your policy. You can add individual controls or an entire control category from an **Asset type** by marking the checkbox in the grid and clicking the **Add** button. If you need to read more about the control, you can expand the **Knowledgebase Article** within the grid.

Once controls are added, they are listed in the main **Controls** grid and not visible in the **Add Controls** grid. If you want to remove a control from your policy, simply select the control (or CTRL + select to multi-select controls) in the grid and select the **Remove** icon on the left toolbar.

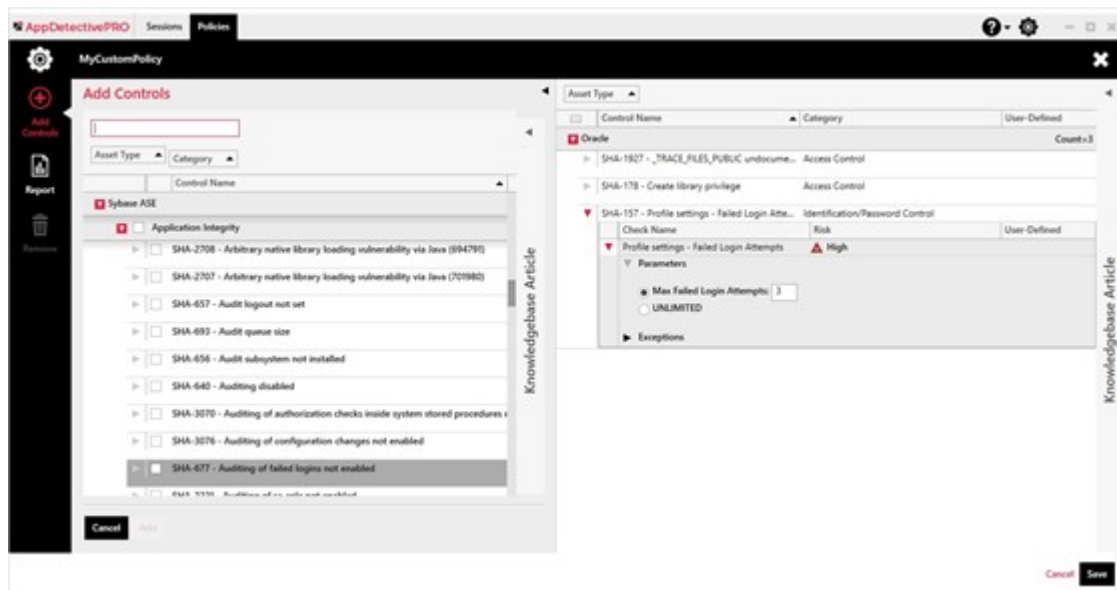


In addition to choosing the controls you want in your policy, there are other elements that can add further customization. Within the **Controls** grid you can expand the control to check level to see **Parameters** and **Exceptions**.

- **Exceptions** allow you to add known environmental variables to the policy that will in effect not show finding occurrences for them. In essence, if a check examines if a user has a certain privilege, you can create an exception for a certain user that should be examined for that privilege grant.

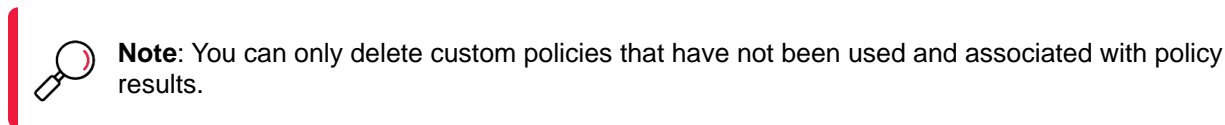


- Parameters allow you to change the behavior of a check to inspect for a certain value. In essence, if a check examines a certain number value setting, you can change the default value as you see fit for your requirements.



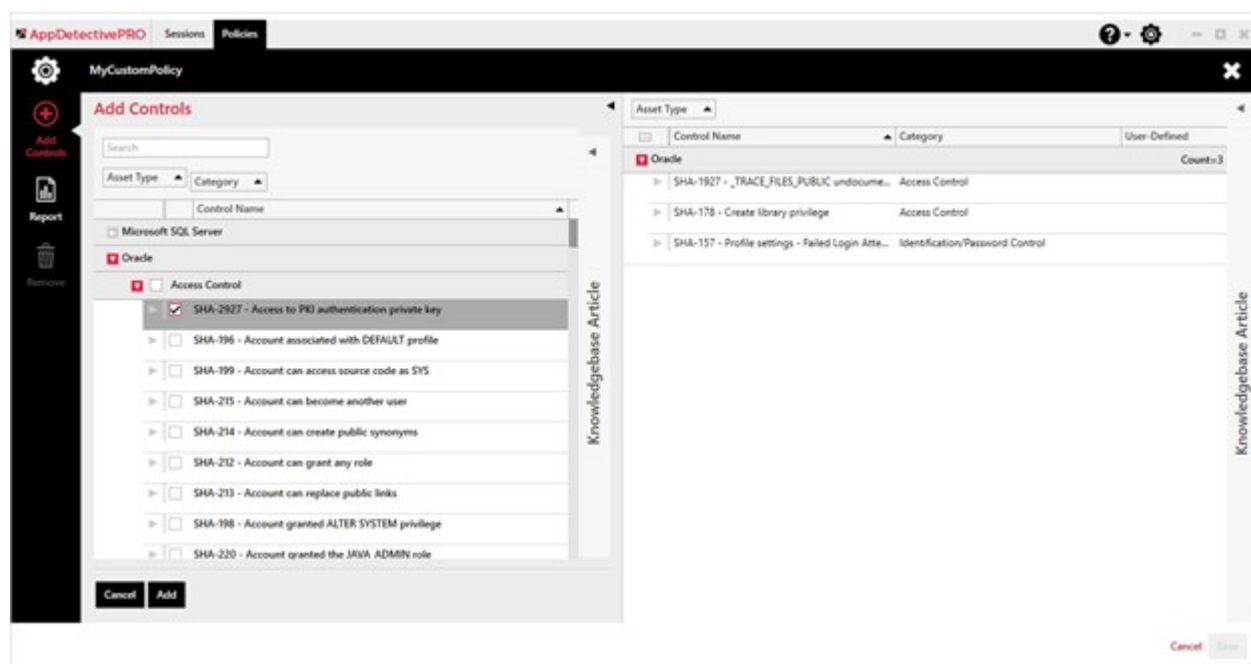
Delete Policies

Any custom policy that you created can also be deleted. To do so, select the policy from the grid and click the **Delete** button.



Add/Remove Controls

Any custom policy that you create allows you to choose precisely which controls are included in that policy. To associate a control with a custom policy, select the desired control(s) from the grid and click the **Add** button.



Frameworks

A framework is a container of total controls possible to be added to policies. AppDetectivePRO has some built-in frameworks available: SHATTER, CIS, and DISA STIG.

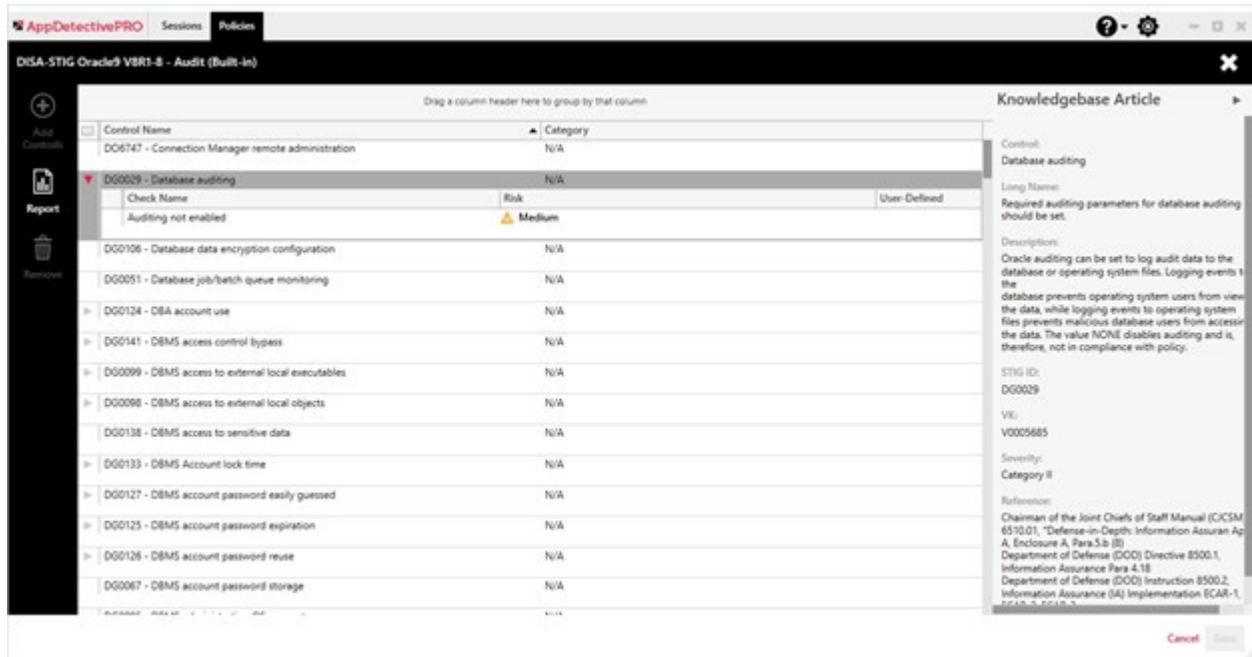
Other frameworks may be added in newer versions of the software.

The SHATTER framework is the default framework which comes with controls and checks that can be used within policies. This framework is maintained by Trustwave's research and development group, SpiderLabs. The SHATTER framework and policies associated with it are updated monthly via ASAP

Updates. It is the only framework that can be cloned. The CIS and DISA STIG frameworks cannot be cloned because they represent content from outside organizations.

The CIS and DISA STIG frameworks are frameworks associated to their respective industry specific guidance standards. CIS is associated with the Center for Internet Security, and DISA STIG is associated with the Defense Information Systems Agency.

Within Frameworks, you can create your own custom frameworks or view the current built-in ones. You can further customize a user-created framework as described in the following sections.



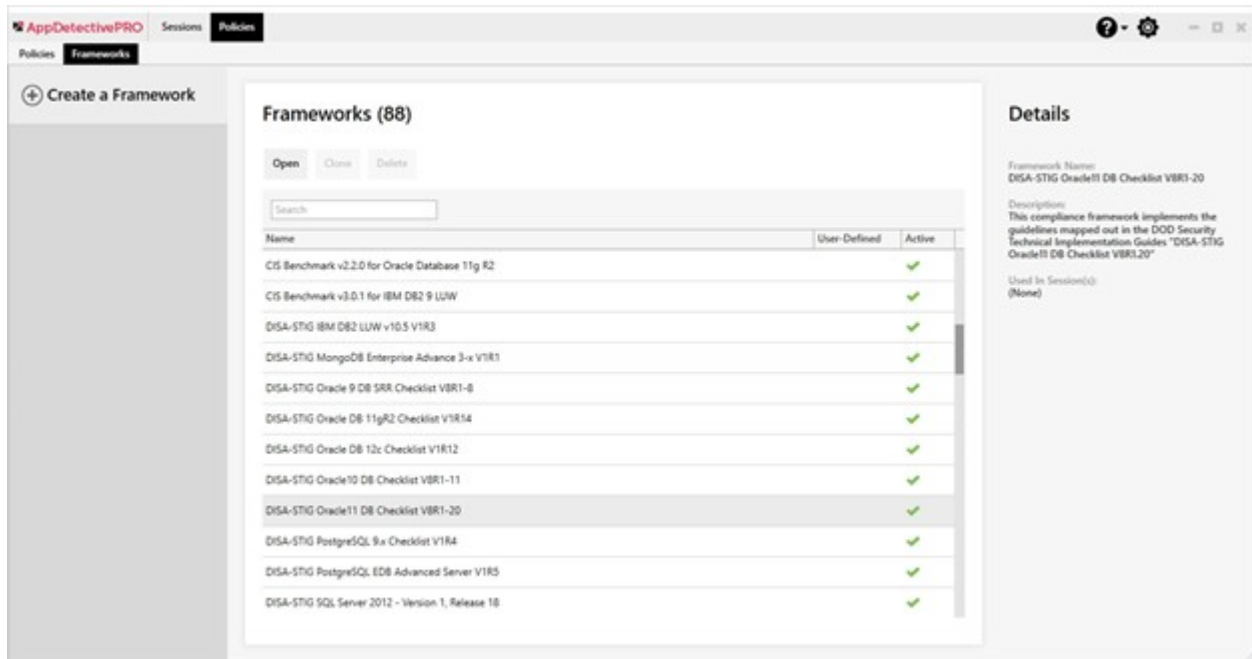
Customize Frameworks

Users can create, clone, and delete frameworks in the **Frameworks** tab.

Create/Clone/Delete Framework

Users can create their own frameworks or clone the existing non-built in frameworks and the built in SHATTER framework. To create a framework, click the **Create a Framework** icon in the left toolbar.

If a user would like to delete a non-built-in framework or clone a framework, simply select the control and choose the desired **Delete** or **Clone** button from the main window.



Add/Create/Edit/Remove Control

With non-built in frameworks, you can manipulate and modify the controls which belong to the framework that they are customizing. When the control edit panel is in use, you cannot change the control that is currently selected.

Controls can be added, created, edited or removed from framework. To add an existing control, click the **Add Controls** icon on the left tool bar and select the controls to be added to the framework. To create a control, click the **Add Controls** icon in the left tool bar then select **Create a Control**. To edit a control, click the **Edit Control** icon on the left tool bar and to remove a control, click on the **Remove** icon on the left tool bar.

Add/Create/Edit/Remove Check

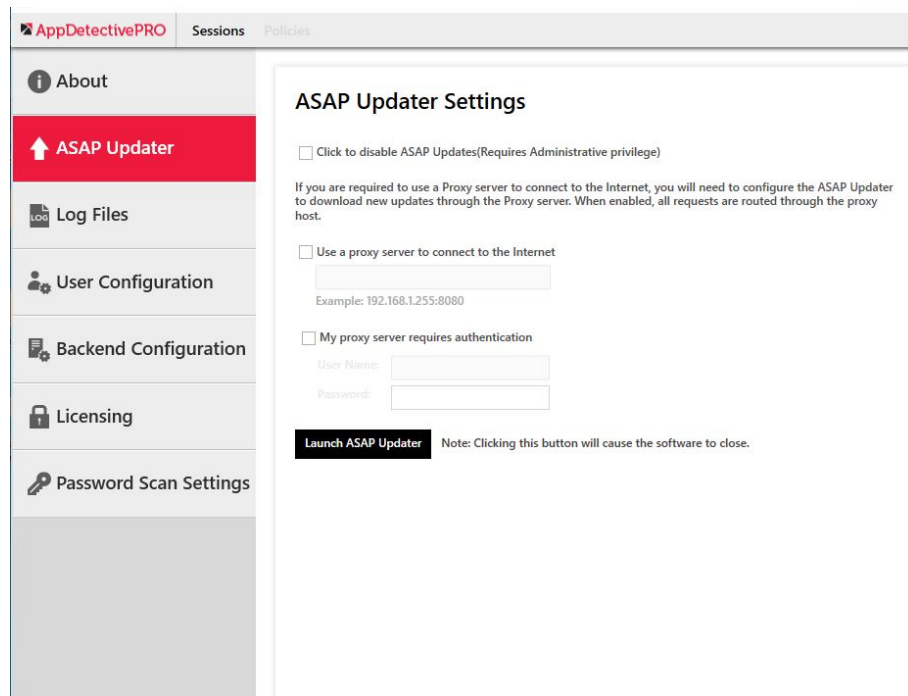
Similarly, with non-built in frameworks, you can manipulate and modify the checks which belong to the framework you are customizing and the control you selected. When you use the **Add Checks** panel, you cannot change the currently selected check.

Checks can be added to a Framework, created in a framework, edited or removed. To add an existing check to a framework, click **Add Checks** on the left tool bar and then click **Add Existing Check** to specify desired checks. To create a Check to be added to a framework, click **Add Checks** on the left tool bar and then click **Create a Check**. To edit checks in a framework, click **Edit Check** on the left tool bar. To remove a check, click **Remove** on the left tool bar.

System Settings

System Settings allow you to configure users of the product, run ASAP Updates, see the version of the product, change log file trace settings, and view licensing information. The following sections are available:

- **About:** displays the versions of each component of AppDetectivePRO. You may need to provide this information to the Customer Support team if working on an issue.
- **ASAP Updater** allows you to stay up to date with the latest product version and SHATTER Knowledgebase. When logged in as an administrator, you can launch the update to download the latest available versions. You can also configure a proxy if needed. The **disable ASAP Updates** checkbox will disable this functionality ensuring the AppDetectivePRO installation will not change (updates may drop support for older database versions).



- **Log Files:** allows you to change the tracing level for log files and collect the files in a zip file to send to the Customer Support team if needed to help troubleshoot an issue.

AppDetectivePRO Sessions Policies

About

ASAP Updater

Log Files

User Configuration

Backend Configuration

Licensing

Password Scan Settings

Log Files Settings

Tracing Level:

Debug

Informational

Warning

Error

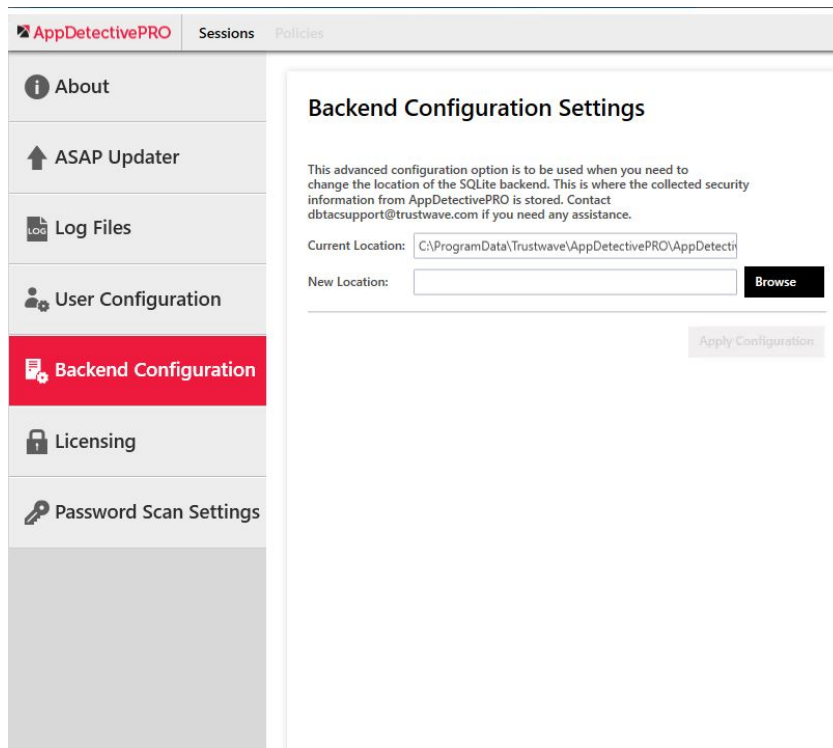
File Path Destination:

C:\Users\Administrator\AppData\Local\AppSecInc\AppDetectivePRO\logs\AppDetectivePRO_Logs_2023-7-6-181932... [Browse...](#) [Collect All Files](#)

Log Files: As of 2023-07-06 18:19 UTC-04:00

Log Name	Log Type	File Path	Date Modified	Size
AppDetectivePRO.log	Application	C:\Users\Administrator\AppData\Local\Ap...	2023-07-06 18:19...	43 KB
AppDetectivePRO_[EE8545...	Installation/Upgrade	C:\Users\Administrator\AppData\Local\Te...	2023-07-06 18:18...	791 KB
AppDetectivePRODataCo...	Installation/Upgrade	C:\Users\Administrator\AppData\Local\Te...	2023-07-06 18:18...	194 KB
AppDetectivePROBootstra...	Installation/Upgrade	C:\Users\Administrator\AppData\Local\Te...	2023-07-06 18:18...	23 KB
AppDetectivePROSetupIns...	Installation/Upgrade	C:\Users\Administrator\AppData\Local\Te...	2023-07-06 18:16...	106 KB
UserRights.log	Scan Engine	C:\Program Files (x86)\Trustwave\ScanEng...	2023-07-06 18:19...	4 KB
ScanEngineHostNTService...	Scan Engine	C:\Program Files (x86)\Trustwave\ScanEng...	2023-07-06 18:19...	5 KB
Discovery.log	Scan Engine	C:\Program Files (x86)\Trustwave\ScanEng...	2023-07-06 18:19...	1 KB
Checks.log	Scan Engine	C:\Program Files (x86)\Trustwave\ScanEng...	2023-07-06 18:19...	1 KB

- **User Configuration:** allows you to configure any Windows Login to access the application after an Administrator has installed it.
- **Backend Configuration** (advanced feature): allows you to change the location where the backend database file is stored.



- **Licensing:** allows you to view licensing information and apply the license to the application. You are able to see how many UUT's you have available for scans and other information about the licenses.
- **Password Scan Settings:** configures whether passwords are displayed and stored in clear text, or masked.

The screenshot shows the AppDetectivePRO interface. At the top, there is a navigation bar with the AppDetectivePRO logo, 'Sessions', and 'Policies'. A left sidebar contains several menu items: 'About', 'ASAP Updater', 'Log Files', 'User Configuration', 'Backend Configuration', 'Licensing', and 'Password Scan Settings' (which is highlighted in red). The main content area is titled 'Password Scan Settings' and features a checked checkbox for 'Mask Passwords'. Below the checkbox, there is explanatory text and an 'Apply' button.

AppDetectivePRO Sessions Policies

Password Scan Settings

Mask Passwords

Unchecking the box will disable the Mask Passwords option.

Any new policy scan containing password checks performed after this change will display and store passwords in clear text for any occurrences found. Any results (previous or future) with the Mask Passwords option enabled will display and store passwords as masked for any occurrences found.

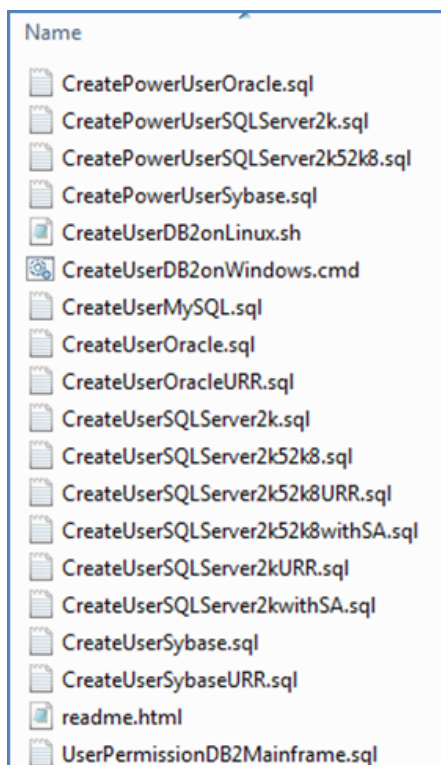
Apply

User Account Privileges Needed for Audit and User Rights Review Scans

Audit policy scans and User Rights Review scans require read-only access to the asset. While you can use an Administrator account to run the scans, it is not required. To setup the appropriate databases access on the assets, **User Creation Scripts** are provided within the product, specifically from the SHATTER Knowledgebase component.



Note: On 64-bit systems the default installation location is within `C:\Program Files (x86)`



In the directory, you see a readme file that provides you more information about each script. The basic guidance is as follows, where [Asset] = asset type and version (where needed):

- **CreateUser[Asset].sql**: creates a user called 'aduser' and will grant read-only permissions needed to run Audit policy scans.
- **CreateUser[Asset]URR.sql**: creates a user called 'aduserURR' and will grant read-only permissions needed to run Audit policy and User Rights Review scans.
- **CreatePowerUser[Asset].sql**: creates a user called 'aduser_admin' will grant elevated privileges (i.e. SYSDBA for Oracle).

- **CreateUser[Asset]SA.sql**: specific for Microsoft SQL Server and create a user called 'aduser' and grant sysadmin rights.
- **UserPermissionsDB2Mainframe.sql**: creates a user called 'aduser' and will grant read-only permissions needed to run Audit policy scans against IBM DB2 z/OS.

To understand if you should use the PowerUser or SA script, read the CheckPermissions.txt file located in the following directory as there are some checks that do require elevated privileges:

C:\Program Files (x86)\Trustwave\AppDetectivePRODataComponent\Resources



Note: On 64-bit systems, the default installation location is within C:\Program Files (x86).

In addition to setting up database access on the asset, OS access may also be needed if you are running OS integrity checks or checks that do require OS access (such as Oracle Critical Patch Update checks). See the readme file for complete instructions on setting up WMI and DCOM permissions. Beyond the information in the readme file here is more guidance on OS access:

Permissions for OS Access

Check	Windows Permission Needed
Not Using NTFS Partition	Permission to read the installation disk type
Registry Permissions	Remote registry access
Services Runs as Local System	Permission to list the system services
Permissions on Files	Permission to read files in the installation directory of the database

Permissions for Unix Access

Check	Unix Permissions Needed
Permissions on Files	Permission to list files in the installation directories of the database
Setgid Bit Enabled	See above
Setuid Bit Enabled	See above

Specifically for certain target databases need to have system variables to specify the location of the database instances.

Target Database Permissions for Unix

Target Database	Unix Permissions Needed
Oracle	Make sure the \$ORACLE_HOME variable is correct. Note: The OS account needs to have privileges of Oracle Software Owner.
Sybase ASE	Make sure the \$SYBASE variable is correct.
MySQL	Define a datadir or basedir variable to point to the database root.

For Microsoft SQL Server, you can also choose to use Windows Authentication for database credentials. You will need to enter the domain or hostname, username, and password. (for example, if your Windows login is domain\aduser, you enter domain in the **Domain or IP/Hostname** field, and aduser in the **User Name** field).



Note: If any fields are encrypted and the account used for the Audit policy scan does not have access to those fields, some checks may not work properly.

Additional Information

Beyond opening and checking on any tickets, the Fusion platform is a resource for product downloads, including SHATTER Knowledgebase releases, product documentation, and provides solutions for common user errors and other troubleshooting information.

If you require more detailed information that is not covered in the User Guide you can contact Customer Support or login to Fusion.

For contact information, by region, go to <https://www.trustwave.com/Company/Support/>, select **All Trustwave Products and Services** from the **Global Product and Service Support** drop-down list, and select the appropriate country.

Legal Notice

Copyright 2023 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.

The authors 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.

More information may be obtained by contacting: Trustwave Technical Support using the details here:

<https://www.trustwave.com/en-us/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.