DbProtect™

DbProtect 6.1
User’s Guide

Last Modified June 15, 2010

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

Contents

Introduction

What you will find in this chapter:

- *Product, Guide, and Documentation Suite Overview*
- *Intended Audience*
- *DbProtect Components*
- *Logging Into the DbProtect Console (and DbProtect Console Login Troubleshooting)*
- *Global Navigation in DbProtect*
- *DbProtect Administration: Content/Compliance Packs, Data Sources, and System Information*
- *DbProtect Organizations, Users, and User Roles*
- *Customer Support.*

Product, Guide, and Documentation Suite Overview

What you will find in this section:

- *About DbProtect*
- *What you will find in this guide*
- *If you need more help*.

About DbProtect

The Industry's Only Complete Database Security Solution

A centrally-managed enterprise solution for comprehensive database security, DbProtect combines discovery, vulnerability scanning, real-time audit and threat management to help organizations reduce risk and enhance compliance. The integrated suite is comprised of the company's flagship solutions for database vulnerability management and real-time database audit and threat management which protect enterprise organizations around the world from all internal and external threats, while also ensuring that those organizations meet or exceed regulatory compliance requirements.

Applying the proven security industry best practices of **vulnerability management** and real-time **audit and threat management**, coupled with extensive enterprise features (including fine-grained access controls, and centralized management and reporting), DbProtect delivers comprehensive security and auditing capabilities to complex, diverse enterprise database environments.

Address Database Threats and Provide Protection with Proven Technology

- **Tamper Evident Privileged Audit and Threat Management** defends against misuse, fraud and abuse from internal and external users.
- **Comprehensive Vulnerability Management** identifies and reduces risk.
- **Real-Time Monitoring and Intrusion Detection** immediately identifies database attacks or misuse.
- **Compensating Controls**, including Patch Gap management, assists with prioritizing of database security patches and defending against attack.
- **Improved Integration** enables reporting on security patch progress, risk mitigation impact, and overall compliance status.
- **Application Awareness** provides critical insight into IT infrastructure enabling organizations to better understand their database inventory, and thereby mitigate compliance risk factors, as well as addressing database security needs.

- **Industry-leading Knowledgebase** utilizes the most comprehensive catalog of database-specific threats, many discovered by Team SHATTER, our own research and development team.
- **DbProtect's ASAP Update** mechanism ensures protection remains up to date. This allows users to immediately identify and detect worms, buffer overflows, and privilege escalation exposures and attacks enabling a timely, informed, and fast response.

Enhance Regulatory Compliance Efforts

DbProtect enables enterprises to ground compliance efforts in the database applications that house regulated data – be it material financial transactions, critical intellectual property, or sensitive personal information. The solution also supports forensic investigations and analysis. This approach to database security includes:

- Robust access and authentication controls
- Privileged and non-privileged user monitoring
- Vulnerability management
- Audit and threat management with proactive real-time alerts
- Defined security Policies to guide user activity.

These security components collectively facilitate regulatory compliance and create active and intelligent protection mechanisms for databases. By grounding efforts in the databases where sensitive data spends the bulk of its existence, the suite helps customers comply with a variety of business and regulatory requirements including the PCI Data Security Standard, HIPAA, GLBA, California Security Breach Information Act (SB 1386), Sarbanes-Oxley Act, Basel II, ISO 27001/17799, DISA-STIG, FISMA, NIST 800-53, PIPEDA, Canada's Bill 198, and MITS.

What you will find in this guide

This guide consists of the following high-level chapters:

- *Vulnerability Management*
- *Audit and Threat Management.*

If you need more help

You can contact Application Security, Inc. Customer Support any time by emailing `support@appsecinc.com`, or by calling 1-866-9APPSEC or 1-212-912-4100.

Intended Audience

This guide intended for persons responsible for day-to-day usage of Db Protect. Typically, those responsible for installing DbProtect have the following (sometimes overlapping) job roles:

- system administrators; for more information, see *System administrators*
- network administrators; for more information, see *Network administrators*
- database administrators; for more information, see *Database administrators*.

System administrators

The **system administrator** maintains and operates a computer system and/or network. System administrators are often members of an Information Technology (IT) department. Their duties are wide-ranging, and vary from one organization to another. System administrators are usually charged with installing, supporting, and maintaining servers or other computer systems, and planning for and responding to service outages and other problems. Other duties may include scripting or light programming, project management for systems-related projects, supervising or training computer operators, and being the consultant for computer problems beyond the knowledge of technical support staff.

Network administrators

The **network administrator** is a professional responsible for the maintenance of computer hardware and software that comprises a computer network. This normally includes the deployment, configuration, maintenance and monitoring of active network equipment.

Network administration commonly includes activities and tasks such as network address assignment, assignment of routing protocols and routing table configuration, as well as configuration of authentication and authorization-directory services. A network administrator’s duties often also include maintenance of network facilities in individual machines, such as drivers and settings of personal computers, as well as printers and so on.

Network administration also sometimes entails maintenance of certain network servers, e.g., file servers, VPN gateways, intrusion detection systems, etc. Network specialists and analysts concentrate on the network design and security, particularly troubleshooting and/or debugging network-related problems. Their work can also include the maintenance of the network's authorization infrastructure, as well as network backup systems.

In addition, the network administrator is responsible for the security of the network and for assigning IP addresses to the devices connected to the networks. Assigning IP addresses gives the subnet administrator some control over the professional who connects to the subnet. It also helps to ensure that the administrator knows each system that is connected and who personally is responsible for the system. When network administrators give a system an IP address, they also delegate certain security responsibilities to the system administrator.

Database administrators

A **database administrator** (DBA) is responsible for the environmental aspects of a database. In general, these include:

- **Recoverability.** Creating and testing backups.
- **Integrity.** Verifying or helping to verify data integrity.
- **Security.** Defining and/or implementing access controls to the data.
- **Availability.** Ensuring maximum uptime.
- **Performance.** Ensuring maximum performance.
- **Development and testing support.** Helping programmers and engineers to efficiently utilize the database.

The role of a DBA has changed according to the technology of database management systems (DBMSs), as well as the needs of the database owners.

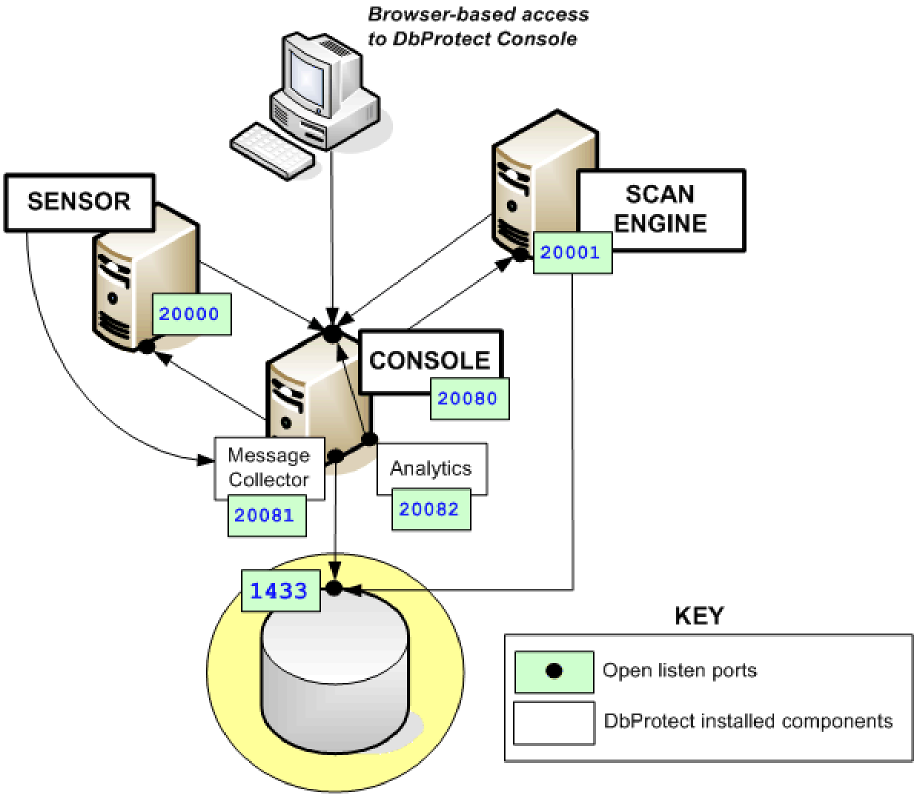
DbProtect Components

What you will find in this section:

- *Conceptual diagram*
- *Console*
- *Scan Engines*
- *Sensors.*

Conceptual diagram

The following **conceptual diagram** illustrates how the DbProtect components interact, and indicates which standard listen ports must be open in order for DbProtect to work.



Console

The **Console** is the web browser-based, graphical component of DbProtect that allows you to navigate to the various features of the two DbProtect portals: **DbProtect Audit and Threat Management** and **DbProtect Vulnerability Assessment**.

Accordingly, this guide refers to the Console as the DbProtect Audit and Threat Management UI and/or the DbProtect Vulnerability Assessment UI, depending which part of the enterprise product you are using.

If you are working with:

- **DbProtect Vulnerability Assessment** see *Vulnerability Management*
- **DbProtect Audit and Threat Management**, see *Audit and Threat Management*.

Note: In previous versions of DbProtect, you could use the **Configuration Manager Tool** to modify the Console's logging level. Now, you must manually change logging level values in the `log4j.properties` files; for more information, see *Appendix H: Manually Changing the Logging Level for the Console by Modifying the log4j.properties File.*

For information on minimum system requirements and installation instructions for the Console, see the *DbProtect Installation Guide*.

Scan Engines

DbProtect's network-based, vulnerability management **Scan Engines** discover database applications within your infrastructure and assesses their security strength. Backed by a proven security methodology and extensive knowledge of application-level vulnerabilities, DbProtect locates, examines, reports, and fixes security holes and misconfigurations. Scan Engines scan your databases for vulnerabilities, and allow you to perform Penetration (Pen) Tests and Audits against them.

Target databases (on Windows) include:

- Oracle
- Oracle Application Server
- SQL Server
- Lotus Notes/Domino
- Sybase
- DB2
- DB2 on the Mainframe
- MySQL.

For information on minimum system requirements and installation instructions for the Sensors, see the *DbProtect Installation Guide*.

Sensors

Sensors deliver database-specific protection and alerting for best-in-class protection of enterprise organizations. You can fine-tune your event detection parameters and customize which audit and security events to monitor. This helps you focus security efforts on information that is relevant while bypassing false positives and irrelevant events. DbProtect's ASAP Update mechanism ensures protection remains up-to-date as new vulnerabilities are identified and patches are released. Comprehensive Policies and rules definitions informed by industry best practices enable security auditing and documentation specific to enterprise environments.

There are two types of **Sensors** available:

- *Host-based Sensors*, which monitor SQL Server, Oracle, Sybase, or DB2 databases on the host server
- *Network-based Sensors*, which monitor your Oracle, DB2 or Sybase databases on the network.

Sensors fire Alerts when they detect a violation of rules, and a monitored event occurs. For more information on Sensors and Alerts, see *Sensors* and *Alerts*, respectively.

HOST-BASED SENSORS

Host-based Sensors allow you to monitor the following databases on a host server:

- **SQL Server** on Windows
- **Oracle** on Solaris, AIX, HP-UX, and Linux
- **DB2** on Linux, Windows, Solaris, and AIX
- **Sybase** Solaris and AIX.

The table below lists all supported host-based database/OS combinations, and links you to the installation steps.

DB	OS
SQL SERVER	WINDOWS
DB2	LINUX
	SOLARIS
	AIX
	WINDOWS

DB	OS
ORACLE	LINUX
	SOLARIS
	AIX
	HP-UX
	WINDOWS
SYBASE	SOLARIS
	AIX

For information on **specific** supported database and operating system versions -- as well as minimum system requirements and installation instructions for the Sensors -- see the *DbProtect Installation Guide*.

NETWORK-BASED SENSORS

Network-based Sensors allow you to monitor Windows-based **Sybase**, **Oracle**, and **DB2** on the network. If you want to install a **network-based Sensor**, the table below lists supported database/OS combinations, and links you to the installation steps.

DB	OS
DB2	WINDOWS
SYBASE	
ORACLE	

For information on **specific** supported database and operating system versions -- as well as minimum system requirements and installation instructions for the Sensors -- see the *DbProtect Installation Guide*.

Logging Into the DbProtect Console (and DbProtect Console Login Troubleshooting)

What you will find in this section:

- *Logging Into the DbProtect Console*
- *Logging Into the DbProtect Console Using SSO*
- *DbProtect Console Login Troubleshooting.*

Logging Into the DbProtect Console

Caution! Some older versions of Google Desktop (5.1 and earlier) may cause problems when loading the DbProtect Console applet in Internet Explorer. You should turn off Google Desktop, or re-install a newer (5.2 or greater) version.

Note: You must have the Java Runtime Environment (JRE) SE 6 Update 11 installed in order to connect to the DbProtect Console via a web browser.

To log into the DbProtect Console:

1. Do one of the following:

- Open Internet Explorer 6.0 or greater with JavaScript enabled, and the screen resolution set to a minimum of 1024x768.
- Enter `https://YourMachineName: InstallPort` in the **Address** line, where:

  -`YourMachineName` is the computer name of your Console machine

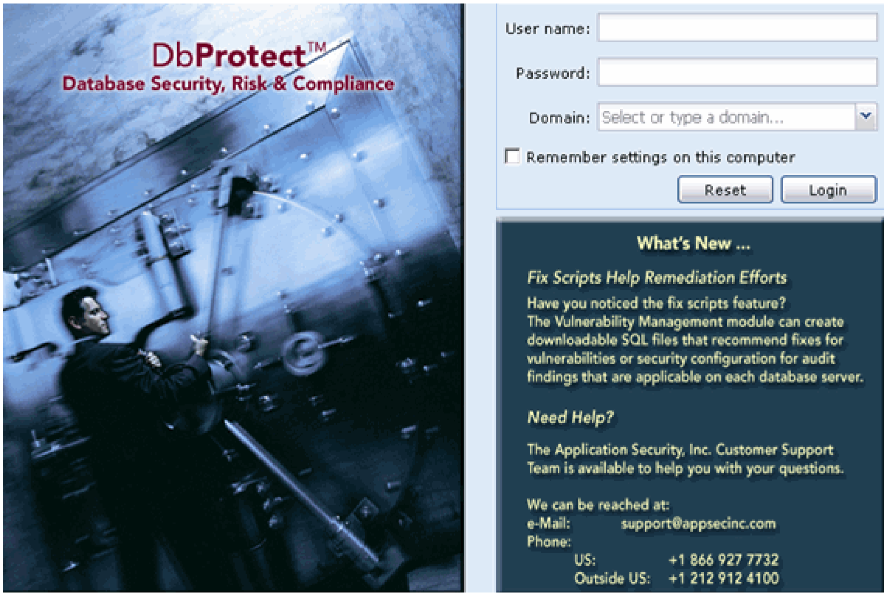
  -`InstallPort` is the port number entered during installation.

A **Security Alert** pop up displays, prompting you to accept a security certificate from Application Security, Inc. DbProtect uses this certificate to communicate with users over a secure channel.

Note: If you experience difficulty logging into the DbProtect Console and connecting to DbProtect, you may need to troubleshoot the Java Runtime Environment (JRE) security settings on your Internet Explorer 6 or greater web browser. For more information on a workaround, see *Troubleshooting the Java Run Time Environment (JRE) Security Settings on Internet Explorer 6* or *Troubleshooting the Java Run Time Environment (JRE) Security Settings on Internet Explorer 7*.

Another possible solution is to clear your Java cache. For more information, see *Appendix O: Clearing Your Java Cache* in the *DbProtect Installation Guide*.

2. Click the **OK** button to display the DbProtect Console login page.


DbProtect™
Database Security, Risk & Compliance
User name:
Password:
Domain:
Select or type a domain...
□ Remember settings on this computer
Reset
Login

What's New ...

Fix Scripts Help Remediation Efforts

Have you noticed the fix scripts feature? The Vulnerability Management module can create downloadable SQL files that recommend fixes for vulnerabilities or security configuration for audit findings that are applicable on each database server.

Need Help?

The Application Security, Inc. Customer Support Team is available to help you with your questions.

We can be reached at:
e-Mail: support@appsecinc.com
Phone:
US: +1 866 927 7732
Outside US: +1 212 912 4100

FIGURE: DbProtect Console login page

3. Do the following:

- In the **Username:** field, enter your DbProtect user name. You can use any of the following formats:

```
-username: local user
-<computername>\username
-<netbios domain name>\username
-<dns domain name>\username
-username@<dns domain name>
```

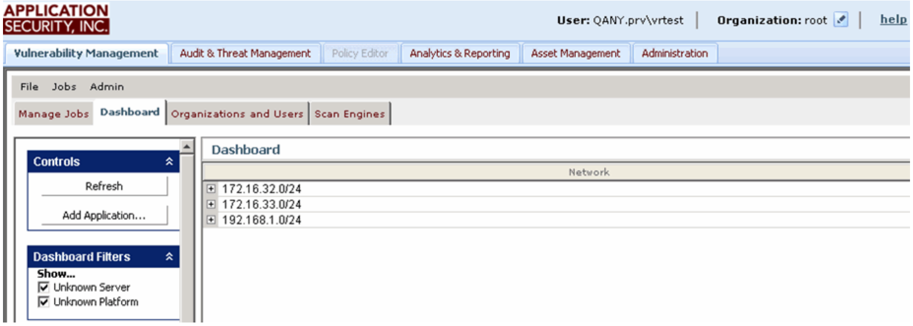
- In the **Password:** field, enter your DbProtect password.

- Use the **Domain:** drop-down to select your domain, or manually enter a domain in the **Domain:** field.

Note: DbProtect is designed to use only Secure Sockets Layer (SSL) communication, which encrypts your user name and credentials prior to transmission to DbProtect. DbProtect then uses the Windows Authentication subsystem to verify the credentials.

Hint: You can check the **Remember settings on this computer** checkbox to store your **Username:**, **Password:** and **Domain:** login values. You can click the button to reset the entered **Username:**, **Password:** and **Domain:** login values.

4. Click the **Login** button to display the DbProtect Console. For more information on navigating the DbProtect Console, see *Global Navigation in DbProtect*.



User: QANY.prv\vrtest | Organization: root

Network
172.16.32.0/24
172.16.33.0/24
192.168.1.0/24

FIGURE: DbProtect Console (**Vulnerability Management** / **Dashboard** selected)

Every DbProtect Console page includes global navigation elements. They are:

- **Application tabs** (in the upper portion of every Console page) which allow you to toggle between the different components of DbProtect. Specifically, you can click the:

  -**Vulnerability Management** tab to display and use DbProtect Vulnerability Management; for more information, see *Vulnerability Management*

  -**Audit & Threat Management** tab to display and use DbProtect Audit & Threat Management; for more information, see *Audit and Threat Management*

  -**Analytics & Reporting** tab to use DbProtect Analytics and run DbProtect reports; for more information, see *DbProtect Analytics*

  -**Asset Management tab** to view and manage all your database assets; for more information, see *Asset Management*

  -**Administration tab** to use Content Packs and view your DbProtect system information; for more information, see *DbProtect Administration: Content/ Compliance Packs, Data Sources, and System Information*

-**User/Organization information**, i.e., your logged-in **user ID** and your associated "effective" **Organization** (in the upper right portion of every DbProtect Console page). If you are a Super User or an Admin User, and your User ID is associated with multiple Organizations, you can toggle between Organizations. For more information, see *Setting Your "Effective" Organization*

- **help** and **logout** links (in the upper right portion of every DbProtect Console page). Clicking these links allows you to display the DbProtect online help and log out of DbProtect, respectively.

Logging Into the DbProtect Console Using SSO

Starting with version 6.1, DbProtect allows you to use Windows authentication to log into the DbProtect Console using a login mechanism known as **single sign-on (SSO)**.

Note: SSO capability only works on Microsoft Windows systems.

If Windows authentication is properly configured, you can log into the DbProtect Console via Internet Explorer 6.0 or greater without having to enter a username and password. For security purposes, SSO is ideally combined with strong authentication methods like smart cards or one-time password tokens.

There are numerous benefits to implementing SSO. For example, SSO reduces the proliferation of user accounts and passwords and enables a more secure environment. SSO also eliminates the need for DbProtect users to remember an additional password. Other benefits include:

- reducing time spent re-entering passwords for the same identity
- reducing IT costs due to lower number of IT help desk calls about passwords
- security on all levels of entry/exit/access to systems without the inconvenience of re-prompting users
- centralized reporting for compliance adherence.

In order to implement SSO, you (or your administrator) must modify several configuration files. For more information, see the *DbProtect Administrator's Guide*.

To log into the DbProtect Console using SSO:

1. Do the following:

   - Open Internet Explorer 6.0 or greater with JavaScript enabled, and the screen resolution set to a minimum of 1024x768.
   - Enter `https://YourMachineName: InstallPort` in the **Address** line, where:

     -`YourMachineName` is the computer name of your DbProtect Console machine

     -`InstallPort` is the port number entered during installation.

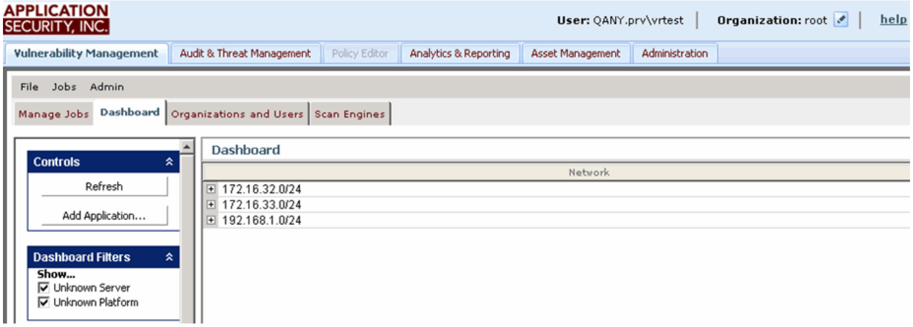
A **Security Alert** pop up displays, prompting you to accept a security certificate from Application Security, Inc. DbProtect uses this certificate to communicate with users over a secure channel.

Caution! If an "access denied" pop-up displays, prompting you to enter your credentials, this means you don't have access to the DbProtect system, even though you're a valid Windows user. If this happens, contact your DbProtect administrator to obtain access to the DbProtect system.

Hint: If you experience difficulty logging into the DbProtect Console and connecting to DbProtect, you may need to troubleshoot the Java Runtime Environment (JRE) security settings on your Internet Explorer 6 or greater web browser. For more information on a workaround, see ***Troubleshooting the Java Run Time Environment (JRE) Security Settings on Internet Explorer 6*** or ***Troubleshooting the Java Run Time Environment (JRE) Security Settings on Internet Explorer 7***.

Another possible solution is to clear your Java cache. For more information, see ***Clearing Your Java Cache***.

2. The DbProtect Console displays; more information on navigating the Console, see *Global Navigation in DbProtect*.



User: QANY.prv\vrtest | **Organization:** root

Show...
☑ Unknown Server
☑ Unknown Platform

⊞ 172.16.32.0/24
⊞ 172.16.33.0/24
⊞ 192.168.1.0/24

FIGURE: DbProtect Console (**Vulnerability Management** / **Dashboard** selected)

Every DbProtect Console page includes global navigation elements. They are:

- **Application tabs** (in the upper portion of every DbProtect Console page) which allow you to toggle between the different components of DbProtect. Specifically, you can click the:

  -**Vulnerability Management** tab to display and use DbProtect Vulnerability Management; for more information, see *Vulnerability Management*

  -**Audit & Threat Management** tab to display and use DbProtect Audit & Threat Management; for more information, see *Audit and Threat Management*

  -**Analytics & Reporting** tab to use DbProtect Analytics and run DbProtect reports; for more information, see *DbProtect Analytics*

  -**Asset Management tab** to view and manage all your database assets; for more information, see *Asset Management*

-**Administration tab** to use Content Packs and view your DbProtect system information; for more information, see *DbProtect Administration: Content/ Compliance Packs, Data Sources, and System Information*

-**User/Organization information**, i.e., your logged-in **user ID** and your associated "effective" **Organization** (in the upper right portion of every DbProtect Console page). If you are a Super User or an Admin User, and your User ID is associated with multiple Organizations, you can toggle between Organizations. For more information, see *Setting Your "Effective" Organization*.

- **help** and **logout** links (in the upper right portion of every DbProtect Console page). Clicking these links allows you to display the DbProtect online help and log out of DbProtect, respectively.

DbProtect Console Login Troubleshooting

This topic consists of the following sub-topics:

- *Troubleshooting the Java Run Time Environment (JRE) Security Settings on Internet Explorer 6*
- *Troubleshooting the Java Run Time Environment (JRE) Security Settings on Internet Explorer 7*
- *Clearing Your Java Cache*
- *Adding the DbProtect URL to Your List of Trusted Intranet Sites In Internet Explorer.*

TROUBLESHOOTING THE JAVA RUN TIME ENVIRONMENT (JRE) SECURITY SETTINGS ON INTERNET EXPLORER 6

If you are experiencing difficulty logging into the DbProtect Console, you may need to troubleshoot the Java Runtime Environment (JRE) security settings on your Internet Explorer (IE) 6 or greater web browser.

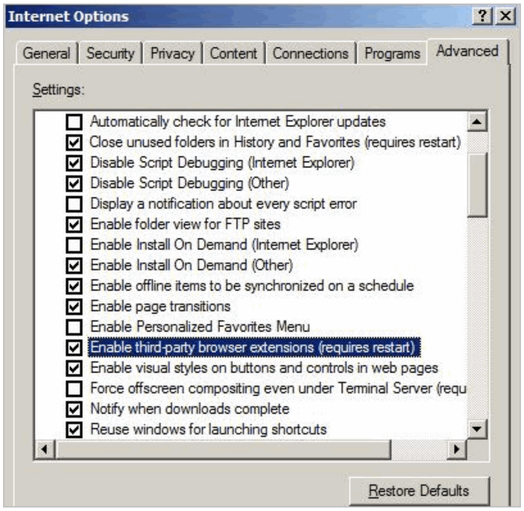
If your web browser is IE 6, Active X controls and "enable third-party browser extensions" security settings may not be enabled on your IE 6 browser. If this is the case, you will encounter an error message you attempt to authenticate, and you can't log in to the DbProtect Console.

Note: The following security settings **should** be the default values in your IE 6 web browser. You should only change the settings if you're experiencing difficulty logging into the DbProtect Console.

To enable proper Active X controls and "enable third-party browser extensions" security settings on IE 6, do the following:

1. Launch IE 6.
2. Do the following to display the **Security Settings** dialog box:
   - Choose: **Tools** > **Internet Options**.
   - Click the Security tab.
   - Click the **Custom Level** button.
3. Set the following security settings to **Enable** or **Prompt**:
   - **Download signed ActiveX controls**
   - **Run ActiveX controls and plug-ins**.
4. Click the **OK** button.
5. Click the **Advanced** tab.

The **Security Settings** dialog box displays.



☐ Automatically check for Internet Explorer updates
☑ Close unused folders in History and Favorites (requires restart)
☑ Disable Script Debugging (Internet Explorer)
☑ Disable Script Debugging (Other)
☐ Display a notification about every script error
☑ Enable folder view for FTP sites
☐ Enable Install On Demand (Internet Explorer)
☑ Enable Install On Demand (Other)
☑ Enable offline items to be synchronized on a schedule
☑ Enable page transitions
☐ Enable Personalized Favorites Menu
☑ Enable third-party browser extensions (requires restart)
☑ Enable visual styles on buttons and controls in web pages
☐ Force offscreen compositing even under Terminal Server (requ
☑ Notify when downloads complete
☑ Reuse windows for launching shortcuts

FIGURE: Internet Explorer **Advanced Settings** dialog box

6. Check **Enable Third-party browser extensions (requires restart)**.
7. Click the **OK** button.
8. Close and re-launch IE 6.

Try to log back into the DbProtect Console. If you continue to experience trouble, contact Application Security, Inc. Customer Support at support@appsecinc.com.

TROUBLESHOOTING THE JAVA RUN TIME ENVIRONMENT (JRE) SECURITY SETTINGS ON INTERNET EXPLORER 7

If your web browser is IE 7, JRE 1.6 may be disabled and/or multiple JREs may be enabled on your client (i.e., the location from which your **IE 7** browser is running). JRE 1.6 **must** be enabled in order for you to connect to the DbProtect Console. If JRE 1.6 is disabled, or if multiple JREs of different versions are enabled on your client, then you will encounter an error message when you attempt to authenticate, and you can't log in to the DbProtect Console.

To ensure JRE 1.6 is enabled, and to temporarily disable multiple JREs on your client machine (using IE 7), do the following:

1. Launch IE 7.
2. Do the following to display the **Settings** dialog box:
   - Choose: **Tools** > **Internet Options**.
   - Click the **Advanced** tab.
3. Scroll down to the Java (Sun) portion of the dialog box and verify the following:
   - JRE 1.6 is enabled (i.e., the box must be checked)
   - multiple JRE installations are listed.

JRE 1.6 **must** be enabled in order for you to connect to the DbProtect Console. If it is **not**, check the JRE 1.6 box.

If JRE 1.6 is enabled, and **other** JRE versions are also enabled, then you must temporarily disable them by un-checking the boxes.

4. Click the **Apply** button.
5. Click the **OK** button.
6. Close and re-launch IE 7.

Try to log back into the DbProtect Console. If you continue to experience trouble, contact Application Security, Inc. Customer Support at support@appsecinc.com.

CLEARING YOUR JAVA CACHE

If you are experiencing difficulty logging into the DbProtect Console, you may need to clear your Java cache. Application Security, Inc. also recommends you clear your Java cache after an upgrade. The Java cache does **not** get automatically cleared following a reboot.

To clear your Java cache:

1. Choose **Start > Control Panel** to display the Control Panel.
2. Double click the **Java** icon to display the **Java Control Panel** dialog box.

3. With the default **General** tab selected, click the **Settings...** button (in the **Temporary Internet Files** section of the dialog box) to display the **Temporary Files Settings** dialog box.
4. Click the **Delete Files...** button to clear your Java cache.

Close your web browser and attempt to log into the DbProtect Console again.

ADDING THE DBPROTECT URL TO YOUR LIST OF TRUSTED INTRANET SITES IN INTERNET EXPLORER

In order for single sign-on (SSO) to function properly, you may need to configure Internet Explorer by adding the DbProtect URL to your list of trusted intranet sites.

Note: The following steps explain how to configure Internet Explorer 7. Steps may vary slightly for other browser versions.

In Internet Explorer, do the following:

1. Choose **Tools > Internet Options** to display the **Internet Options** dialog box.
2. Select the **Security** tab.
3. Select **Local Intranet** from the list of zone sites (at the top of the **Internet Options** dialog box).
4. Click the **Sites** button to display a **Local intranet** pop up.
5. Click the **Advanced** button to display a second **Local intranet** pop up.
6. Add `https://<dbprotecturl>` to the **Add this website to the zone:** field, where `<dbprotecturl>` is the DbProtect Console URL; for more information, see *Logging Into the DbProtect Console Using SSO*.
7. Click the **Add** button to add DbProtect to your list of trusted local intranet sites.
8. Click the **Close** button to close the second **Local intranet** pop up.
9. Click the **Close** button to close the first **Local intranet** pop up.
10. Click the **Apply** button on the **Internet Options** dialog box to apply your changes.
11. Click the **OK** button to close the **Internet Options** dialog box.

Global Navigation in DbProtect

What you will find in this section:

Every Console page includes **global navigation elements**. They are:

- *Application Tabs*
- *User ID and Associated “Effective” Organization*
- *Help and Logout Links.*

Application Tabs

Application tabs display in the upper left portion of every DbProtect Console page. These tabs allow you to toggle between the different components of DbProtect.

FIGURE: Application tabs

You can click the:

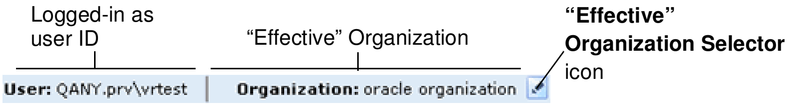
- **Vulnerability Management** tab to display and use DbProtect Vulnerability Management; for more information, see *Vulnerability Management*
- **Audit & Threat Management** tab to display and use DbProtect Audit & Threat Management; for more information, see *Audit and Threat Management*
- **Analytics & Reporting** tab to use DbProtect Analytics and run DbProtect reports; for more information, see the *DbProtect Analytics User’s Guide*
- **Asset Management tab** to view and manage all of your database assets; for more information, see *Asset Management*.
- **Administration tab** to import content packs and enable compliance pack functionality in DbProtect, to view your DbProtect system information; for more information, see *DbProtect Administration: Content/Compliance Packs, Data Sources, and System Information*.

User ID and Associated "Effective" Organization

The upper right portion of every Console page displays your **User/Organization information**, i.e., your logged-in **user ID** and your associated "effective" **Organization.**

Every User ID is associated with at least one Organization. An **Organization** is a logical grouping of applications that allows you to manage User rights and capabilities within DbProtect. If you are a DbProtect Super Admin, DbProtect Admin, Vulnerability Management Admin, or an Audit and Threat Management Admin, then DbProtect allows you to create Organizations and define a set of IP ranges and Policies for each Organization (which you can override at the User or Group level). For more information, see*DbProtect Organizations, Users, and User Roles*.

If you are a DbProtect Super Admin, DbProtect Admin, Vulnerability Management Admin, or an Audit and Threat Management Admin -- and your User ID is associated with multiple Organizations -- you can click the **"Effective" Organization Selector** icon (labeled below) to display the **"Effective" Organization Selector** dialog box and change your "effective" Organization.



User: QANY.prv\vrtest | **Organization:** oracle organization

FIGURE: User/"effective" Organization info

For more information, on:

- using the **"Effective" Organization Selector** dialog box to change your "effective" Organization, see *Setting Your "Effective" Organization*
- how Organizations work in DbProtect, see *DbProtect Organizations, Users, and User Roles*
- user roles in DbProtect, see *DbProtect Organizations, Users, and User Roles*.

Help and Logout Links

The upper right portion of every Console page displays **Help** and **Logout** links, which allow you to display the online help and log out of DbProtect, respectively.

FIGURE: **Help** and **Logout** links

DbProtect Administration: Content/Compliance Packs, Data Sources, and System Information

What you will find in this section:

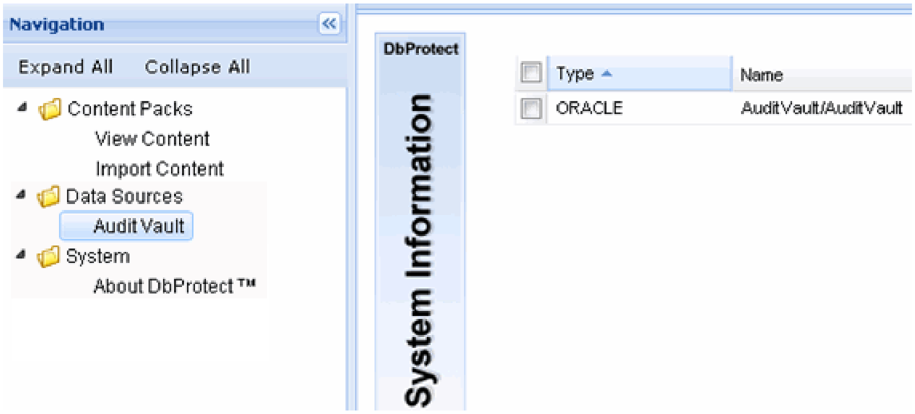
- *Displaying, Understanding, and Navigating the DbProtect Administration Page*
- *Working with Content and Compliance Packs*
- *Working with Data Sources*
- *Viewing Your DbProtect System Information.*

Displaying, Understanding, and Navigating the DbProtect Administration Page

When you click the **Administration** application tab from any DbProtect Console page (for more information, see *Application Tabs*), the DbProtect **Administration** page displays. This page allows you to import content packs and enable compliance pack and data source functionality in DbProtect, and to view your DbProtect system information.

For more information on:

- content packs and compliance packs, see *Working with Content and Compliance Packs*
- data sources, see *Working with Data Sources*
- viewing your DbProtect system information, see *Viewing Your DbProtect System Information*.



□	Type ▲	Name
□	ORACLE	AuditVault/AuditVault

FIGURE: **Administration** page

The **Administration** page consists of two panes: the **navigation pane** and the **viewing pane**.

The **navigation pane** allows you to select whether you want to work with **Content Packs**, **Data Sources**, or view your DbProtect **System** information.

Hint: In the navigation pane, you can click the **Expand All** link to expand all viewable content pack and system information, or click the **Collapse All** link to collapse viewable content pack and system information.

The **viewing pane** displays information about:

- Your imported **content packs** (if you click the **Content Packs > View Content** link in the navigation pane); for more information, see *Viewing Your Available Imported Compliance Content Packs.*

  The viewing pane also allows you to import content packs (if you click the **Content Packs > Import Content** link in the navigation pane); for more information, see *Importing a Compliance Content Pack.*

- **Data Sources**, such as Oracle Audit Vault; for information, see *Working with Data Sources*. The viewing pane also allows you to register data sources (for example, you can register Oracle Audit Vault by clicking the **Data Sources > Audit Vault** link in the navigation pane); for more information, see *Registering Oracle Audit Vault as a DbProtect Data Source*.
- The specific versions of your installed DbProtect suite components (if you click the **System > About DbProtect** link in the navigation pane); for more information, see *Viewing Your DbProtect System Information*.

Working with Content and Compliance Packs

Compliance packs are optional DbProtect add-ons that contain regulatory compliance-level views of your database environment designed to help you track, manage, and meet compliance requirements. **Compliance packs** work in conjunction with DbProtect Analytics (version 1.3 or higher of which **must** be installed), allowing you to review and analyze compliance progress with additional high-level Dashboards and report the results of testing of database security controls in the correct compliance language context (e.g., information assurance controls and identifiers).

Compliance packs simplify the mapping between established test controls and the automated methods and procedures within DbProtect, which helps to save a tremendous amount of analysis time. Moreover, content packs offer additional Policies, Dashboards, reports, export formats, and independent resource information where applicable.

In order to enable compliance packs within DbProtect, you must first obtain and import **content packs**, Application Security, Inc.-provided `.zip` files that, when successfully imported into DbProtect, add reports geared toward helping you achieve regulation-specific compliance (for example, DISA-STIG). Once you import a content pack, a new displays on the DbProtect Console; for more information on the application tabs, see *Application Tabs*.

The *Compliance Packs* chapter provides detailed information about importing content packs, working with compliance packs, running compliance pack reports, and more.

Working with Data Sources

TBA

Viewing Your DbProtect System Information

You can click the **System > About DbProtect** link (in the navigation pane of the **Administration** page) to display your current DbProtect system information (including component name, version, and last update).

Note: Not all of the following components may be installed. For more information on DbProtect and DbProtect Analytics components, including minimum system requirements, see the *DbProtect Installation Guide* and the *DbProtect Analytics Installation and User's Guide*.

Specifically, you can view the current version of:

- DbProtect (e.g., **DbProtect 6.0**)
- the Data Component (e.g., **Data Component 2.4.6164.0**)
- the Database Component (e.g., **Data Component 2.4.6161.0**)
- DbProtect Analytics (e.g., **DbProtect Analytics 1.4.6176**)
- DbProtect Console (e.g., **DbProtect Console 4.3.5815**)
- Java (e.g., **Java 1.6.0_11**)
- your Windows operating system (e.g., **Windows 200x 5.2**)
- the SHATTER Knowledgebase (e.g., **2.5.10815.1**)
- SHATTER schema (e.g., **2.4.0.0**)
- Scan Engine (e.g., **6.2.8176**)
- Sensor (e.g., **AppRadar Sensor_3.11.10_Win32.exe**).

DbProtect Organizations, Users, and User Roles

This chapter consists of the following topics:

- *What are DbProtect Organizations, Users, and User Roles?*
- *DbProtect User Roles and Associated Privileges*
- *Adding an Organization*
- *Editing an Organization*
- *Removing an Organization*
- *Setting Your “Effective” Organization*
- *Configuring SMTP Mail Server Information for Your Organization*
- *Adding a Group*
- *Editing a Group*
- *Removing a User*
- *Adding a User*
- *Editing a User*
- *Removing a User*
- *Creating a DbProtect Audit and Threat Management Policy.*

What are DbProtect Organizations, Users, and User Roles?

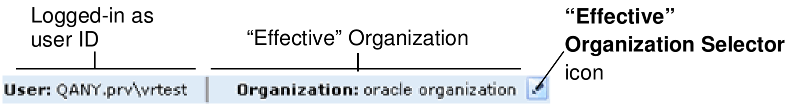
This topic consists of the following sub-topics:

- *What are Organizations?*
- *What are Users?*
- *What are User Roles?*

WHAT ARE ORGANIZATIONS?

An **Organization** is a logical grouping of applications that allows you to manage User rights and capabilities within DbProtect and define a set of IP ranges and Policies for each Organization (which you can override at the User or Group level).

As explained in *User ID and Associated “Effective” Organization*, the upper right portion of every Console page displays your User/Organization information, i.e., your logged-in **user ID** and your associated “effective” **Organization.**



User: QANY.prv\vrtest | Organization: oracle organization

FIGURE: User/”effective” Organization info

Every User ID is associated with at least one Organization, and all Users can change their "effective" Organization.

WHAT ARE USERS?

DbProtect **Users** are individuals that have certain rights within the DbProtect system. You can also add Groups to DbProtect. Users and Groups are Windows entities taken from either the Active Directory[1] or your local system. You **must** explicitly add Users and Groups to DbProtect in order for these individuals to use the product.

The following conceptual diagram illustrates three differently-configured **Organizations**, and the subordinate Groups/Users that belong to each Organization.

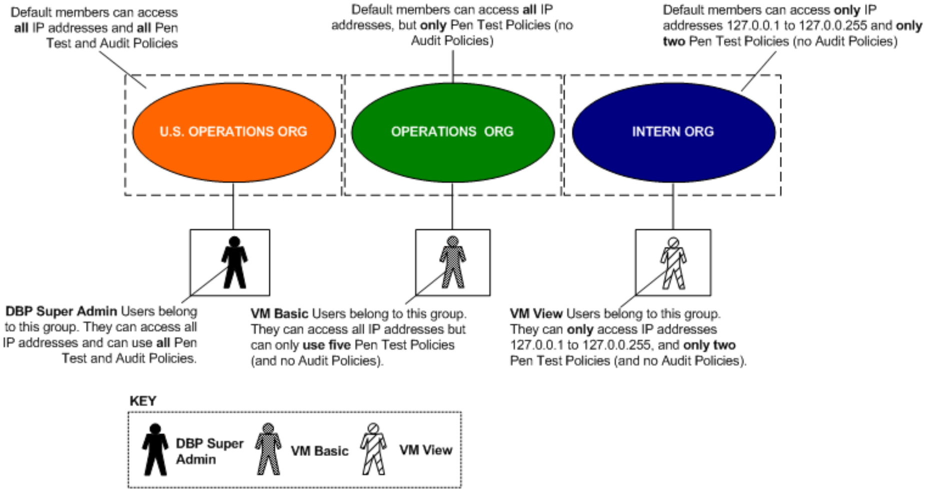

Default members can access **all** IP addresses and **all** Pen Test and Audit Policies
Default members can access **all** IP addresses, but **only** Pen Test Policies (no Audit Policies)
Default members can access **only** IP addresses 127.0.0.1 to 127.0.0.255 and **only** **two** Pen Test Policies (no Audit Policies)
U.S. OPERATIONS ORG
OPERATIONS ORG
INTERN ORG
DBP Super Admin Users belong to this group. They can access all IP addresses and can use **all** Pen Test and Audit Policies.
VM Basic Users belong to this group. They can access all IP addresses but can only **use five** Pen Test Policies (and no Audit Policies).
VM View Users belong to this group. They can **only** access IP addresses 127.0.0.1 to 127.0.0.255, and **only two** Pen Test Policies (and no Audit Policies).
KEY
DBP Super Admin
VM Basic
VM View

FIGURE: Users and Organizations example

If you are a DbProtect Super Admin, DbProtect Admin, Vulnerability Management Admin, or an Audit and Threat Management Admin you can create Organizations and add Users and Groups to them.

Note: If the `DbProtect Scan Engine` service does **not** run as a domain User, then all Users **must** be non-domain Users.

WHAT ARE USER ROLES?

Each User (or Group) added to an Organization has an assigned User Role which has inherent privileges. The next topic, *DbProtect User Roles and Associated Privileges*, explains User Roles and associated privileges in detail.

[1] Active Directory is an implementation of LDAP directory services for Windows environments. Active Directory allows administrators to assign enterprise-wide Policies, deploy programs to many computers, and apply critical updates to an entire Organization. Active Directory stores information and settings relating to an Organization in a central, organized, accessible database. Active Directory networks can vary from a small installation with a few hundred objects, to a large installation with millions of objects.

DbProtect User Roles and Associated Privileges

DbProtect is comprised of Organizations, and within those Organizations, assigned **Users**; for more information, see *Working with Scan Engines*.

Each User has an assigned **User Role**. The available User Roles are:

- DbProtect (DBP) Super Admin
- DBP Admin
- DBP View
- Vulnerability Management (VM) Admin
- VM Basic
- VM View
- Audit and Threat Management (ATM) Admin
- ATM View.

The following table lists privileges associated with each User role.

Caution! If the Console is running as a local administrator, there are User management/authentication limitations. When adding a Group/ User, you can only populate the list of Groups from your "local system", **not** from other domains. In addition, you **cannot** log on to the Console as a domain User. For more information, see ***Working with Scan Engines***.

DBP = DbProtect, **VM** = Vulnerability Management, **ATM** = Audit and Threat Management

Privileges	DBP Super Admin	DBP Admin	VM Admin	ATM Admin	VM Basic	DBP View	VM View	ATM View
Register a Scan Engine.	✓							
Unregister a Scan Engine.	✓							
Edit a Scan Engine.	✓							
Export Vulnerability Management credentials to file via a Job template or Credential Profile.	✓	✓	✓		✓			
Import Vulnerability Management credentials from file via a Job template or Credential Profile.	✓	✓	✓		✓			
Create or modify a Vulnerability Management Credential Profile.	✓	✓	✓		✓			
Set an effective Organization.	✓	✓	✓	✓	✓	✓	✓	✓

Privileges	DBP Super Admin	DBP Admin	VM Admin	ATM Admin	VM Basic	DBP View	VM View	ATM View
Add, edit, and remove an Organization.	✓	✓	✓	✓				
Add, edit, and remove a User or Group. **Note:** Login user must have a higher/ equal privilege to edit or remove the selected user.	✓	✓	✓					
Edit or remove an application from the Vulnerability Management Dashboard.	✓	✓	✓					
Add an application to the Vulnerability Management Dashboard.	✓	✓	✓		✓			
Create, edit, delete, schedule, manage, or cancel a Vulnerability Management Job.	✓	✓	✓		✓			
Delete a Report.	✓	✓	✓	✓	✓			
Create, view, edit, or schedule a Report.	✓	✓	✓	✓	✓	✓	✓	✓
View Vulnerability Management Job results and Job history.	✓	✓	✓		✓	✓	✓	
View Sensors.	✓	✓		✓				
Register a Sensor.	✓	✓		✓				
Configure a Sensor and deploy the configuration information.	✓	✓		✓				
Delete configured Sensors.	✓	✓		✓				
Perform an ASAP Update of Rules in Sensors.	✓	✓		✓				
View and monitor the "health" of Sensors (via the Sensor Manager).	✓	✓		✓		✓		✓
Unregister a Sensor.	✓	✓		✓				

Privileges	DBP Super Admin	DBP Admin	VM Admin	ATM Admin	VM Basic	DBP View	VM View	ATM View
Manually remove a Sensor.	✓	✓		✓				
Monitor Alerts.	✓	✓		✓		✓		✓
Acknowledge and archive Alerts.	✓	✓		✓				
View Policies.	✓	✓		✓		✓		✓
Create a Policy.	✓	✓		✓				
Edit a Policy.	✓	✓		✓				
Import a Policy.	✓	✓		✓				
Export a Policy.	✓	✓		✓				
Deploy a Policy.	✓	✓		✓				
Delete a Policy.	✓	✓		✓				
View Filters.	✓	✓		✓		✓		✓
Edit a Filter.	✓	✓		✓				
Delete a Filter.	✓	✓		✓				
Import a Filter.	✓	✓		✓				
Export a Filter.	✓	✓		✓				
Install and use Compliance Packs.	✓	✓	✓	✓				

DbProtect User Role Inheritance

In DbProtect, Users may belong to multiple Organizations. Their membership may be defined as the role appropriate for a given Organization (i.e., DbProtect Super Admin, DbProtect Admin, DbProtect View, Vulnerability Management Admin, Vulnerability Management Basic, Vulnerability Management View, and Audit and Threat Management Admin). A User’s membership to an Organization may be defined directly by explicit enumeration, or inherited by group membership; for more information, see *What are DbProtect Organizations, Users, and User Roles?*

There are cases where more than one role or membership may be valid for a user -- depending on the User’s Organizational membership and roles. When Users have more than one possible Organizational membership, they are initially placed in a default “effective” Organization. All Users, regardless of User Role, can change their “effective” Organization, as explained in *User ID and Associated “Effective”*

Organization. You can also set a newly-selected Organization as your default "effective" Organization.

Once Users sets their "effective" Organization, DbProtect determines whether the Users' membership to the "effective" Organization can be obtained via multiple paths. If so, DbProtect grants the *highest possible User Role* defined for the User -- within the selected "effective" Organization -- to the User.

The following tables illustrate the effective User Role and Organizational membership under a variety of conditions.

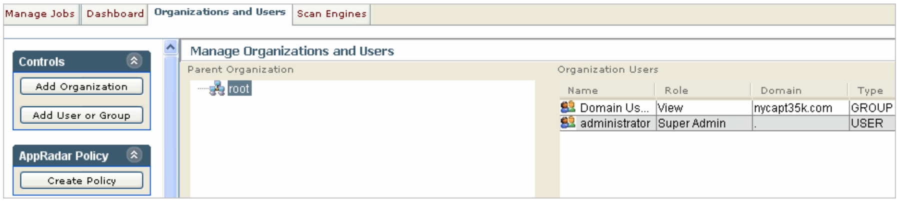
Organization	Parent Organization	User/group	User Role
US Operations	Global Operations	Auditors (Joe, Jane, Mary)	Vulnerability Management Basic User
US Operations	Global Operations	Administrators (Joe, Jim, Mike)	DbProtect Admin
Operations	Corporate	Administrators (Joe, John, Sue)	DbProtect Super Admin

User logging in	"Effective" Organization	User Role granted
Jane	US Operations	Vulnerability Management Basic User
Jim	US Operations	DbProtect Super Admin
Joe	Global Operations	Super Admin
	US Operations	DbProtect Admin

Understanding the Manage Organizations and Users page

The **Organizations and Users** page allows you to create logical and hierarchical Organizations. You can define a set of IP ranges and Policies for each Organization (which you can override at the User or Group level). Your Organizations can be exclusive and isolated from other Organizations.

After you create Organizations, you can create subordinate **Users** and **Groups**. Users and Groups are Windows entities taken from either the Active Directory or your local system.



Name	Role	Domain	Type
Domain Us...	View	nycapt35k.com	GROUP
administrator	Super Admin	.	USER

FIGURE: Organizations and Users page

The pane of the Organizations and Users page is divided into two portions:

- **Parent Organization.** This portion of the pane displays your parent Organization. You can right click the parent Organization to add child Organizations, add Users and Groups, edit Organizations, and remove Organizations.
- **Organization Users and Groups.** The columns in this portion of the pane display the following information about Users and Groups in the Organization you have highlighted (in the **Parent Organization** portion of the pane):

  -**Username.** The usernames of all Users in your Organization.

  -**Role.** The role of the associated Group (i.e., **DbProtect Super Admin**, **DbProtect Admin**, **DbProtect View**, **Vulnerability Management Admin**, **Vulnerability Management Basic**, **Vulnerability Management View**, and **Audit and Threat Management Admin**)

  -**Domain.** The associated User's network domain.

  -**Type.** The role of the associated User (i.e., **DbProtect Super Admin**, **DbProtect Admin**, **DbProtect View**, **Vulnerability Management Admin**, **Vulnerability Management Basic**, **Vulnerability Management View**, and **Audit and Threat Management Admin**).

  You can right click a User or Group to edit or remove the User or Group.

Note: For more information on the pane and other DbProtect Vulnerability Management UI components, see *Understanding the DbProtect Vulnerability Management Portal User Interface (UI).*

Specifically, the **Organizations and Users** page allows you to:

- add an Organization; for more information, see *Adding an Organization*
- edit an Organization; for more information, see *Editing an Organization*
- remove an Organization; for more information, see *Removing an Organization*
- toggle between Organizations, also known as setting your "effective" Organization; for more information, see *Setting Your "Effective" Organization*
- add a Group; for more information, see *Adding a Group*
- edit a Group; for more information, see *Editing a Group*
- remove a Group; for more information, see *Removing a Group*
- add a User; for more information, see *Adding a User*
- edit a User; for more information, see *Editing a User*
- remove a User; for more information, see *Removing a User*.

Adding an Organization

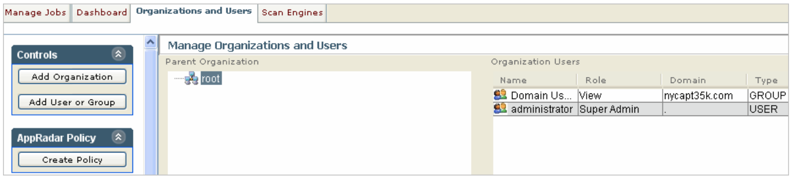
To add an Organization:

1. Do one of the following to display the **Manage Organizations and Users** page:
   - Choose **Admin** > **Organizations and Users** from the menu
   - Click the **Organizations and Users** tab.

The **Manage Organizations and Users** page displays your existing:

- Organizations (in the **Parent Organization** portion of the **Manage Organizations and Users** page)
- Users and Groups (in the **Organization Users** portion of the **Manage Organizations and Users** page).

Hint: Highlight an Organization in the **Parent Organization** portion of the **Manage Organizations and Users** page to display its subordinate Users and Groups, and to activate the Control buttons and menu items.

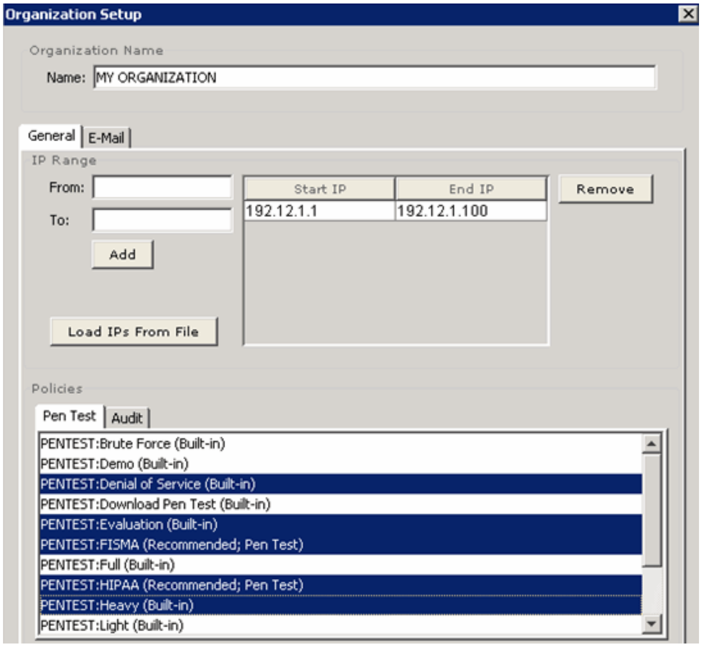


Name	Role	Domain	Type
Domain Us...	View	nycapt35k.com	GROUP
administrator	Super Admin	.	USER

FIGURE: **Manage Organizations and Users** page

2. Do one of the following to display the **Organization Setup** dialog box:

- Click the **Add Organization** button in the **Controls** Toolbar on the **Manage Organizations and Users** page
- Right click an Organization (in the **Parent Organization** portion of the **Manage Organizations and Users** page) and choose **Add Organization**.



Name: MY ORGANIZATION

Start IP	End IP
192.12.1.1	192.12.1.100

PENTEST:Brute Force (Built-in)
PENTEST:Demo (Built-in)
PENTEST:Denial of Service (Built-in)
PENTEST:Download Pen Test (Built-in)
PENTEST:Evaluation (Built-in)
PENTEST:FISMA (Recommended; Pen Test)
PENTEST:Full (Built-in)
PENTEST:HIPAA (Recommended; Pen Test)
PENTEST:Heavy (Built-in)
PENTEST:Light (Built-in)

FIGURE: **Organization Setup** dialog box (**General** tab selected)

Select the **General** tab (selected by default).

Note: You can click the **E-Mail** tab to configure your Organization's SMTP email server information; for more information, see *Configuring SMTP Mail Server Information for Your Organization*.

3. In the **Organization Name** portion of the **Organization Setup** dialog box, enter the name of your new Organization in the **Name:** field.

4. In the **IP Range** portion of the **Organization Setup** dialog box:

- Enter an IP address range in the **From:** and **To:** fields. This is the IP range that members of your Organization are permitted to work within when they schedule a Discovery, Audit, Penetration Test, or Report Job.

  Example: If you specify the range `127.0.0.1` through `127.0.0.255`, then members of your Organization are only permitted to schedule Jobs within this range of IP addresses.

- Click the **Add** button to add the IP addresses to the list of IP addresses that members of your Organization are permitted to work within.
- Click the **Load IPs From File** button to display an **Open** dialog box and upload a standard, line-delimited text file. Unlike the format described in *Creating a Discovery Job*, IP addresses for Organizations do not require ports. You can use any of the following formats:

  -`ip` (for example, `192.168.1.1`)

  -`ip-ip` (for example, `192.168.1.1-192.168.1.255`)

  -Classless Inter Domain Routing (CIDR) notation, i.e., `ip/network prefix` (for example, `192.9.205.22/18`); for more information on CIDR notation, see *http://infocenter.guardiandigital.com/manuals/IDDS/node9.html*

Note: To remove an IP address range from the list, highlight the range, then click the Remove button.

5. In the **Policies** portion of the **Create Organization** dialog box, highlight which Penetration Test and Audit Policies the Users in your Organization can use (or un-highlight restricted Policies).

You can click the:

- **Pen Test** tab, and highlight which Penetration Test Policies the Organization Users can use (or un-highlight restricted Penetration Test Policies)
- **Audit** tab, and highlight which Audit Policies the Organization Users can use (or un-highlight restricted Audit Policies).

Hint: You can *further* restrict/enable Penetration Test and Audit Policy access at the individual User level. For more information, see ***Adding a User*** and ***Editing a User***.

Hint: Click <CTRL> to highlight non-sequential Policies.

6. Click the **Create** button to create your new Organization.

The new Organization displays in the **Parent Organization** portion of the **Manage Organizations and Users** page.

Editing an Organization

To edit an Organization:

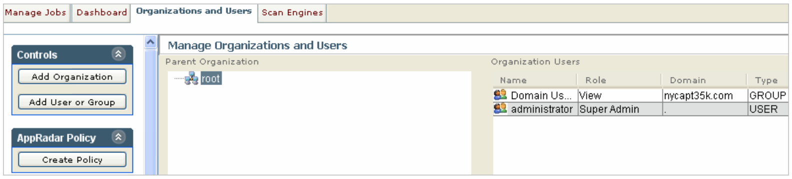
1. Do one of the following to display the **Manage Organizations and Users** page:

- Choose **Admin** > **Organizations and Users** from the menu
- Click the **Organizations and Users** tab.

The the **Manage Organizations and Users** page displays your existing:

- Organizations (in the **Parent Organization** portion of the **Manage Organizations and Users** page)
- Users and Groups (in the **Organization Users** portion of the **Manage Organizations and Users** page).

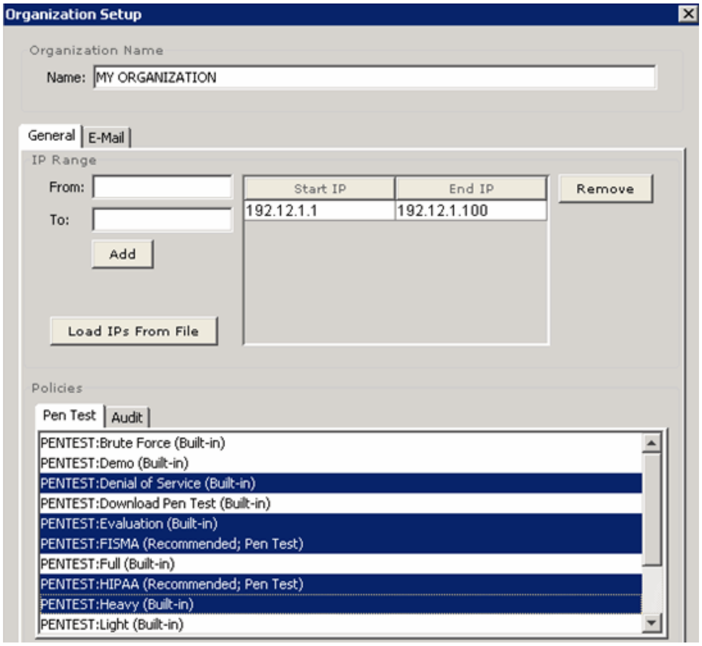
Hint: Highlight an Organization in the **Parent Organization** portion of the **Manage Organizations and Users** page to display its subordinate Users and Groups, and to activate the Control buttons and menu items.



Name	Role	Domain	Type
Domain Us...	View	nycapt35k.com	GROUP
administrator	Super Admin	.	USER

FIGURE: **Manage Organizations and Users** page

2. Right click an Organization (in the **Parent Organization** portion of the **Manage Organizations and Users** page) and choose **Edit Organization** to display the **Organization Setup** dialog box.



Name: MY ORGANIZATION

Start IP	End IP
192.12.1.1	192.12.1.100

PENTEST:Brute Force (Built-in)
PENTEST:Demo (Built-in)
PENTEST:Denial of Service (Built-in)
PENTEST:Download Pen Test (Built-in)
PENTEST:Evaluation (Built-in)
PENTEST:FISMA (Recommended; Pen Test)
PENTEST:Full (Built-in)
PENTEST:HIPAA (Recommended; Pen Test)
PENTEST:Heavy (Built-in)
PENTEST:Light (Built-in)

FIGURE: **Organization Setup** dialog box (**General** tab selected)

Select the **General** tab (selected by default).

Note: You can click the **E-Mail** tab to configure your Organization's SMTP email server information; for more information, see *Configuring SMTP Mail Server Information for Your Organization.*

3. In the **Organization Name** portion of the **Organization Setup** dialog box, you can edit the name of your Organization in the **Name:** field.

4. In the **IP Range** portion of the **Organization Setup** dialog box:

- You can edit the IP address range in the **From:** and **To:** fields. This is the IP range that members of your Organization are permitted to work with when they schedule a Discovery, Audit, Penetration Test, or Report Job.

  Example: If you specify the range `127.0.0.1` through `127.0.0.255`, then members of this Organization are only permitted to schedule Jobs within this range of IP addresses.
- Click the **Add** button to add the IP addresses to the list of IP addresses that members of the Organization are permitted to work within.
- Click the **Load IPs From File** button to display an **Open** dialog box and upload a standard, line-delimited text file. Unlike the format described in *Creating a Discovery Job*, IP addresses for Organizations do not require ports. You can use any of the following formats:

  -`ip` (for example, `192.168.1.1`)

  -`ip-ip` (for example, `192.168.1.1-192.168.1.255`)

  -Classless Inter Domain Routing (CIDR) notation, i.e., `ip/network prefix` (for example, `192.9.205.22/18`); for more information on CIDR notation, see *http://infocenter.guardiandigital.com/manuals/IDDS/node9.html*

Note: To remove an IP address range from the list, highlight the range, then click the Remove button.

5. In the **Policies** portion of the **Organization Setup** dialog box, highlight which Penetration Test and Audit Policies the Users in your Organization can use (or un-highlight restricted Policies).

You can click the:

- **Pen Test** tab, and highlight which Penetration Test Policies the Organization Users can use (or un-highlight restricted Penetration Test Policies)
- **Audit** tab, and highlight which Audit Policies the Organization Users can use (or un-highlight restricted Audit Policies).

Note: You can further restrict/enable Penetration Test and Audit Policy access at the individual User level. For more information, see *Adding a User* and *Editing a User*.

6. Click the **Save** button to save your edited Organization.

The edited Organization displays in the **Parent Organization** portion of the **Manage Organizations and Users** page.

Removing an Organization

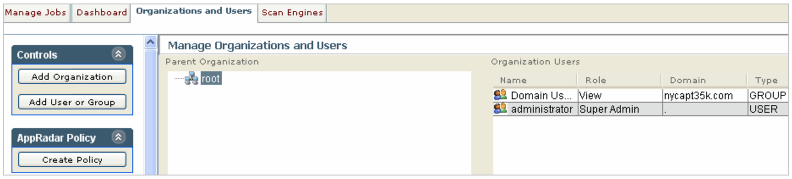
To remove an Organization:

1. Do one of the following to display the **Manage Organizations and Users** page:
   - Choose **Admin** > **Organizations and Users** from the menu
   - Click the **Organizations and Users** tab.

The **Manage Organizations and Users** page displays your existing:

- Organizations (in the **Parent Organization** portion of the **Manage Organizations and Users** page)
- Users and Groups (in the **Organization Users** portion of the **Manage Organizations and Users** page).

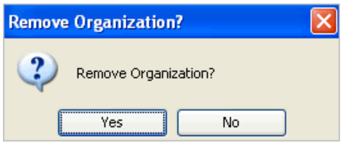
Hint: Highlight an Organization in the **Parent Organization** portion of the **Manage Organizations and Users** page to display its subordinate Users and Groups, and to activate the Control buttons and menu items.



Name	Role	Domain	Type
Domain Us...	View	nycapt35k.com	GROUP
administrator	Super Admin	.	USER

FIGURE: **Manage Organizations and Users** page

2. Right click an Organization (in the **Parent Organization** portion of the **Manage Organizations and Users** page) and choose **Edit** to display the **Remove Organization?** pop up.



Remove Organization?

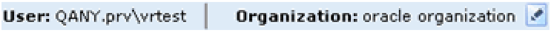
FIGURE: **Remove Organization?** pop up

Click the **Yes** button to remove the Organization (and all its members).

The Organization is removed from the **Parent Organization** portion of the **Manage Organizations and Users** page.

Setting Your "Effective" Organization

As explained in *User ID and Associated "Effective" Organization*, the upper right portion of every Console page displays your **User** and **"effective" Organization information**, i.e., your logged-in **user ID** and your associated "effective" **Organization.**



User: QANY.prv\vrtest

Organization: oracle organization

FIGURE: User/"effective" Organization info

Every User ID is associated with at least one Organization. If you are a Super User or an Admin User, and your User ID is associated with multiple Organizations, you can toggle between Organizations.

To set your "effective" Organization:

1. Do one of the following to display the **Effective Organization Selector** dialog box:
   - Click the **Effective Organization Selector** icon located in the upper right corner of every Console page; for more information, see *User ID and Associated "Effective" Organization*
   - Choose **File > Organization Selector** from the menu.

   The **Effective Organization Selector** dialog box is shown below.

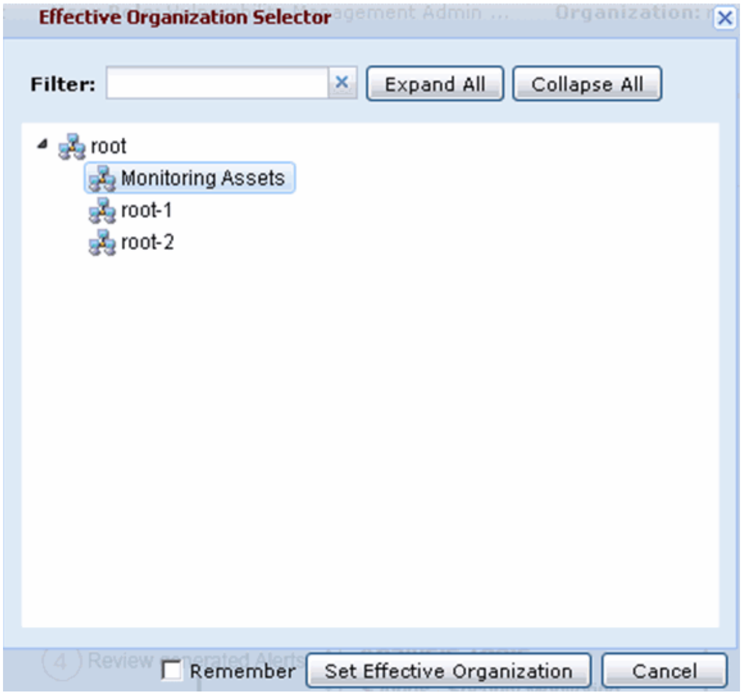


FIGURE: **Effective Organization Selector** dialog box

2. Your current "effective" Organization is highlighted. To change your "effective" Organization, do the following:
   - Highlight a different "effective" Organization.
   - Click the **Set Effective Organization** button.

As a result, your User ID and your new, associated "effective" Organization display at the top of every DbProtect portal page.

Configuring SMTP Mail Server Information for Your Organization

DbProtect Vulnerability Management allows you to notify others via email when DbProtect Vulnerability Management completes a Job. This feature works for all types of Jobs, i.e., Discovery, Penetration Test, Audit, and Report Jobs. For more information, see *Scheduling email notification upon Job completion*.

However, in order to notify others via email when DbProtect Vulnerability Management completes a Job, an Admin or Super Admin **must** first properly configure your Organization's SMTP mail server information. Otherwise, the email notification of Job completion feature will **not** work.

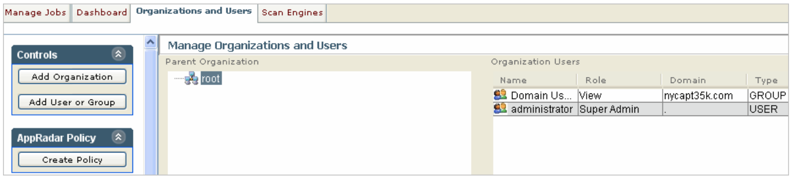
To configure your Organization's SMTP mail server information:

1. Do one of the following to display the **Manage Organizations and Users** page:
   - Choose **Admin > Organizations and Users** from the menu
   - Click the **Organizations and Users** tab.

The **Manage Organizations and Users** page displays your existing:

- Organizations (in the **Parent Organization** portion of the **Manage Organizations and Users** page)
- Users and Groups (in the **Organization Users** portion of the **Manage Organizations and Users** page).

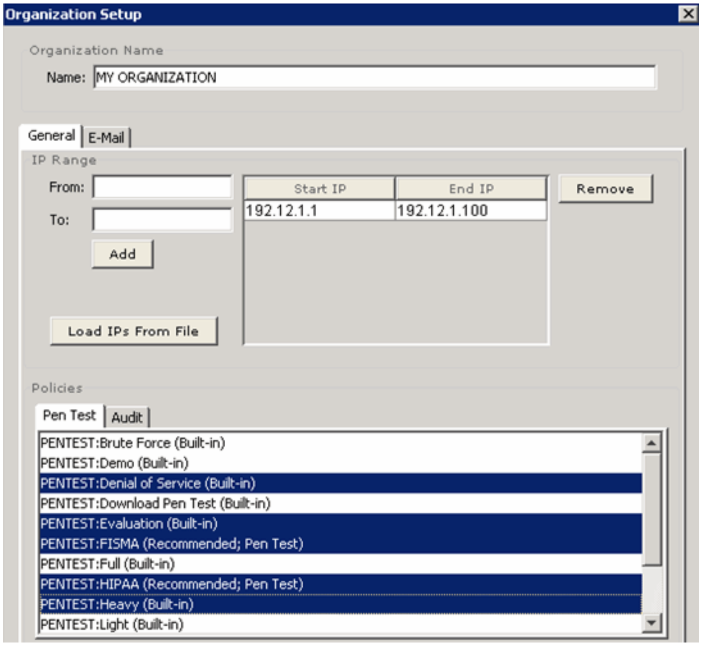
Hint: Highlight an Organization in the **Parent Organization** portion of the **Manage Organizations and Users** page to display its subordinate Users and Groups, and to activate the Control buttons and menu items.



Name	Role	Domain	Type
Domain Us...	View	nycapt35k.com	GROUP
administrator	Super Admin	.	USER

FIGURE: **Manage Organizations and Users** page

2. Right click an Organization (in the **Parent Organization** portion of the **Manage Organizations and Users** page) and choose **Edit Organization** to display the **Organization Setup** dialog box.



Name: MY ORGANIZATION

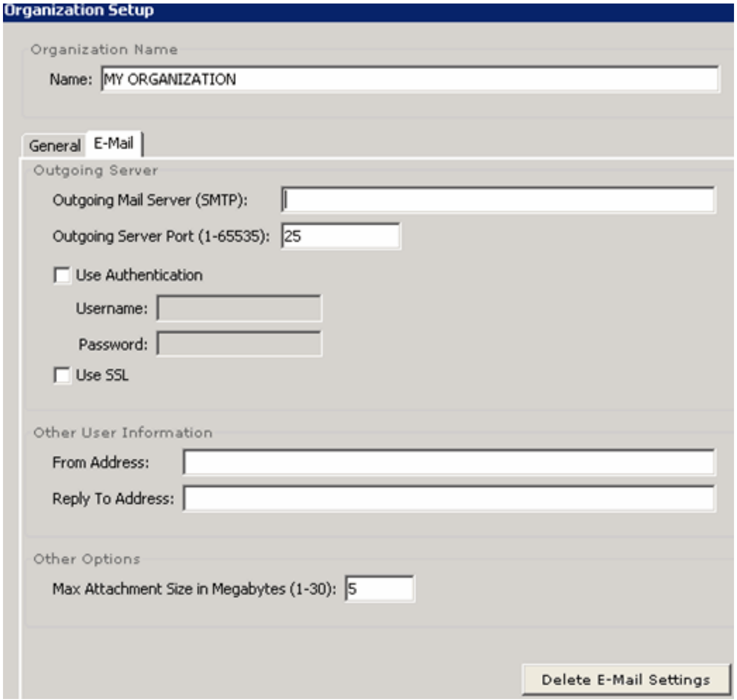
Start IP	End IP
192.12.1.1	192.12.1.100

- PENTEST:Brute Force (Built-in)
- PENTEST:Demo (Built-in)
- PENTEST:Denial of Service (Built-in)
- PENTEST:Download Pen Test (Built-in)
- PENTEST:Evaluation (Built-in)
- PENTEST:FISMA (Recommended; Pen Test)
- PENTEST:Full (Built-in)
- PENTEST:HIPAA (Recommended; Pen Test)
- PENTEST:Heavy (Built-in)
- PENTEST:Light (Built-in)

FIGURE: **Organization Setup** dialog box (**General** tab selected)

3. Click the **E-Mail** tab to display the The **E-Mail** portion of the **Organization Setup** dialog box.

Note: You can click the **General** tab to specify your Organization’s general information. General information includes the IP range that members of your Organization are permitted to work within when they schedule a Job (Discovery, Audit, Penetration Test, or Report). You can also specify which Penetration Test and Audit Policies the Users in your Organization can use. For more information, see *Adding an Organization* or *Editing an Organization*.



Organization Setup

Name: MY ORGANIZATION

Outgoing Mail Server (SMTP):

Outgoing Server Port (1-65535): 25

☐ Use Authentication

Username:

Password:

☐ Use SSL

From Address:

Reply To Address:

Max Attachment Size in Megabytes (1-30): 5

FIGURE: **Organization Setup** dialog box (**E-Mail** tab selected)

If you want to:

- configure your outgoing SMTP server information, see Step 4
- configure your “from” and “reply to” addresses, see Step 5
- specify a maximum attachment size in megabytes (1-30), see Step 6.

4. Configure your outgoing SMTP server information.

In the **Outgoing Server** portion of the dialog box:

- Enter the name of your outgoing SMTP server in the **Outgoing Mail Server (SMTP)** field

- Enter the port number you want to use on your outgoing SMTP server in the **Outgoing Server Port (1-65535)** field.
- Check the **Use Authentication** checkbox if your SMTP server requires authentication in order to send email.

Note: Some SMTP servers require authentication in order to send email. Depending on what kind of SMTP server you are using, and how it is configured, this may or may not be the case. If your SMTP server requires authentication in order to send email, then you must enter a valid login/ password pair, and check the Use Authentication checkbox. However, if you are not sure whether your SMTP server requires authentication, check with your mail administrator.

If you check the **Use Authentication** checkbox, you must also enter a valid:

-Username:

-Password:

- Check the **Use SSL** checkbox if want to use Secure Sockets Layer (SSL) to encrypt your User name and credentials prior to transmission.

5. Specify your **"from"** and **"reply to"** email addresses.

In the **Other User Information** portion of the dialog box, enter your:

- "from" email address in the **From Addess:** field (i.e., when DbProtect Vulnerability Management completes a Job and notifies your email recipienets via email, this is the "from" email address)
- "reply to" email address in the **Reply To Address:** field (i.e., when DbProtect Vulnerability Management completes a Job and notifies your email recipienets via email, this is the "reply to" email address).

6. Specify a maximum attachment size in megabytes (1-30).

In the **Other Options** portion of the dialog box, enter the maximum allowable size of email attachments (0-30 megabytes) in the **Max Attachment Size in Megabytes (1-30):** field. The default value is 3 megabytes.

Note: When DbProtect Vulnerability Management completes a Report, the generated email always includes link to the Report -- even if there is no attachment. In other words, even if the generated Report exceeds the maximum attachment size, your email recipients can still view the Report online.

7. Review your SMTP server settings.

Hint: You can click the **Delete E-Mail Settings** button any time to delete all configured email settings.

8. Click the **Save** button to save your SMTP server settings.

The **Organization Setup** dialog box closes and your SMTP server settings are saved.

Adding a Group

Note: If DbProtect Vulnerability Management does **not** run as a domain User, you must also add local (i.e., non-domain) Users.

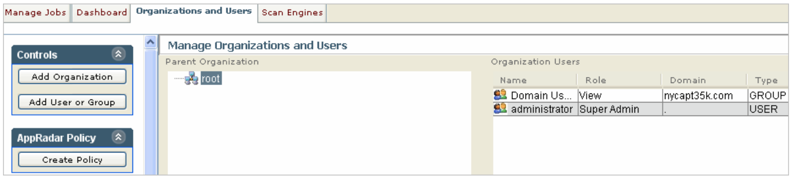
To add a Group:

1. Do one of the following to display the **Manage Organizations and Users** page:
   - Choose **Admin > Organizations and Users** from the menu
   - Click the **Organizations and Users** tab.

The **Manage Organizations and Users** page displays your existing:

- Organizations (in the **Parent Organization** portion of the **Manage Organizations and Users** page)
- Users and Groups (in the **Organization Users** portion of the **Manage Organizations and Users** page).

Hint: Highlight an Organization in the **Parent Organization** portion of the **Manage Organizations and Users** page to display its subordinate Users and Groups, and to activate the Control buttons and menu items.

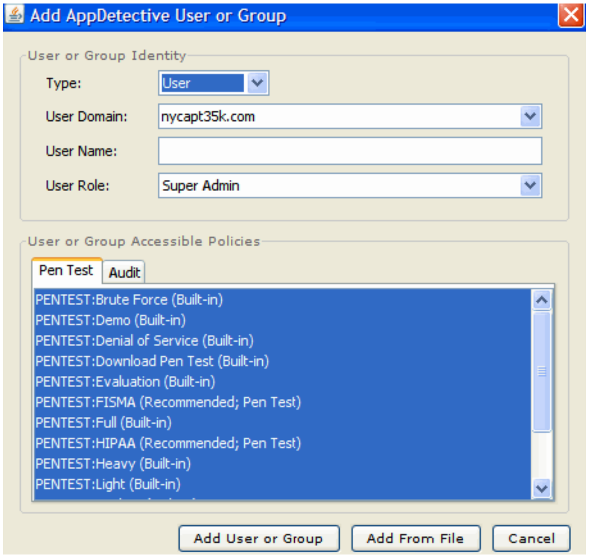


Name	Role	Domain	Type
Domain Us...	View	nycapt35k.com	GROUP
administrator	Super Admin	.	USER

FIGURE: **Manage Organizations and Users** page

2. Do one of the following to display the **Add AppDetective User or Group** dialog box:

- Click the **Add User or Group** button in the Toolbars portion of the **Manage Organizations and Users** page (**Controls** portion)
- Right click an Organization (in the **Parent Organization** portion of the **Manage Organizations and Users** page) and choose **Add User**.



Type: User

User Domain: nycapt35k.com

User Name:

User Role: Super Admin

PENTEST:Brute Force (Built-in)
PENTEST:Demo (Built-in)
PENTEST:Denial of Service (Built-in)
PENTEST:Download Pen Test (Built-in)
PENTEST:Evaluation (Built-in)
PENTEST:FISMA (Recommended; Pen Test)
PENTEST:Full (Built-in)
PENTEST:HIPAA (Recommended; Pen Test)
PENTEST:Heavy (Built-in)
PENTEST:Light (Built-in)

FIGURE: **Add AppDetective User or Group** dialog box

3. In the **User or Group Identity** portion of the **Add AppDetective User or Group** dialog box, do the following:

- Use the **Type:** drop-down to select **Group**.
- Use the **Group Domain:** drop-down to select the Group's network domain.

Hint: Click the **Populate** button to display a list of available Groups.

- Enter or select a Group name. You can:

  -manually enter a Group name in the **Group Name:** field (for example, `AUDIT - U.S.`)

  -click the **Populate** button to display a list of available Groups, then select an available Group using the **Group Name:** drop-down.

- Use the **Group Role:** drop-down to associate the Group with a role (i.e., **Super Admin**, **Admin**, **Basic User**, **View User**); for more information, see the *DbProtect Administrator's Guide*.

4. In the **User or Group Accessible Policies** portion of the **Add AppDetective User or Group** dialog box, highlight which Penetration Test and Audit Policies the Group can use (or un-highlight restricted Policies).

You can click the:

- **Pen Test** tab, and highlight which Penetration Test Policies the Group can use (or un-highlight restricted Penetration Test Policies)
- **Audit** tab, and highlight which Audit Policies the Group can use (or un-highlight restricted Audit Policies).

5. Click the **Add User or Group** button to save your new Group.

The new Group displays in the **Organization Users** portion of the **Manage Organizations and Users** page.

Editing a Group

Note: If DbProtect Vulnerability Management does **not** run as a domain User, you must also add local (i.e., non-domain) Users.

To edit a Group:

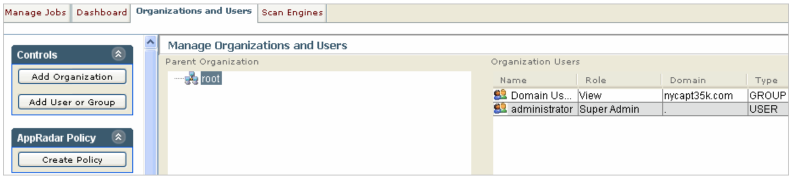
1. Do one of the following to display the **Manage Organizations and Users** page:

- Choose **Admin** > **Organizations and Users** from the menu
- Click the **Organizations and Users** tab.

The **Manage Organizations and Users** page displays your existing:

- Organizations (in the **Parent Organization** portion of the **Manage Organizations and Users** page)
- Users and Groups (in the **Organization Users** portion of the **Manage Organizations and Users** page).

Hint: Highlight an Organization in the **Parent Organization** portion of the **Manage Organizations and Users** page to display its subordinate Users and Groups, and to activate the Control buttons and menu items.

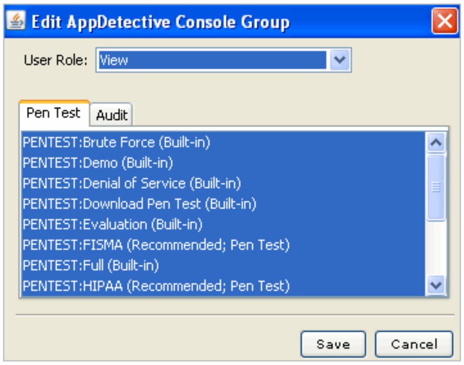


Name	Role	Domain	Type
Domain Us...	View	nycapt35k.com	GROUP
administrator	Super Admin	.	USER

FIGURE: **Manage Organizations and Users** page

2. Do one of the following to display the **Edit DbProtect AppDetective portal Group** dialog box:

- Highlight a Group in the **Organization Users and Groups** portion of the **Manage Organizations and Users** page, and choose **Organizations and Users > Edit User or Group** from the menu
- Right click a Group (in the **Organization Users** portion of the **Manage Organizations and Users** page) and choose **Edit**.
- Double click a Group (in the **Organization Users** portion of the **Manage Organizations and Users** page).



Edit AppDetective Console Group

User Role: View

PENTEST:Brute Force (Built-in)
PENTEST:Demo (Built-in)
PENTEST:Denial of Service (Built-in)
PENTEST:Download Pen Test (Built-in)
PENTEST:Evaluation (Built-in)
PENTEST:FISMA (Recommended; Pen Test)
PENTEST:Full (Built-in)
PENTEST:HIPAA (Recommended; Pen Test)

FIGURE: **Edit DbProtect AppDetective Console Group** dialog box

3. Do the following:

- Use the **User Role:** drop-down to associate the Group with a different role (i.e., **Super Admin**, **Admin**, **Basic User**, **View User**); for more information, see the *DbProtect Administrator's Guide*.
- In the lower portion of the **Edit AppDetective Console Group** dialog box, highlight which Penetration Test and Audit Policies the Group can use (or un-highlight restricted Policies).

  You can click the:

  -**Pen Test** tab, and highlight which Penetration Test Policies the Group can use (or un-highlight restricted Penetration Test Policies)

  -**Audit** tab, and highlight which Audit Policies the Group can use (or un-highlight restricted Audit Policies).

4. Click the **Save** button to save your edited Group.

The edited Group displays in the **Organization Users** portion of the **Manage Organizations and Users** page.

Removing a Group

To remove a Group:

1. Do one of the following to display the **Manage Organizations and Users** page:

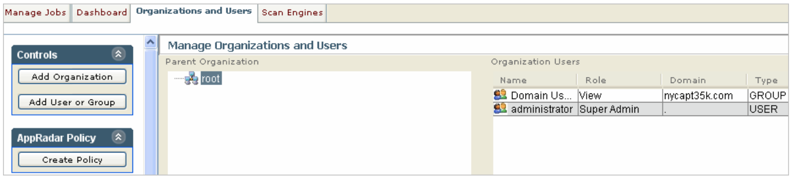
- Choose **Admin** > **Organizations and Users** from the menu
- Click the **Organizations and Users** tab.

The **Manage Organizations and Users** page displays your existing:

Organizations (in the **Parent Organization** portion of the **Manage Organizations and Users** page)

Users and Groups (in the **Organization Users** portion of the **Manage Organizations and Users** page).

Hint: Highlight an Organization in the **Parent Organization** portion of the **Manage Organizations and Users** page to display its subordinate Users and Groups, and to activate the Control buttons and menu items.



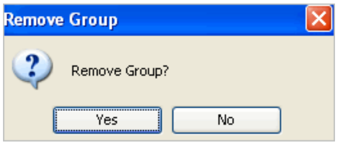
Name	Role	Domain	Type
Domain Us...	View	nycapt35k.com	GROUP
administrator	Super Admin	.	USER

FIGURE: **Manage Organizations and Users** page

2. Do one of the following:

- Highlight a Group in the **Organization Users** portion of the **Manage Organizations and Users** page, and choose **Organizations and Users** > **Remove User or Group** from the menu
- Right click the Group (in the **Organization Users** portion of the **Manage Organizations and Users** page) and choose **Remove**.

The **Remove User?** or **Remove Group?** pop up displays, accordingly, prompting you to confirm the removal.



Remove Group?

FIGURE: **Remove Group?** pop up

Click the **Yes** button to remove the Group.

The Group is removed from the **Organization Users** portion of the **Manage Organizations and Users** page.

Adding a User

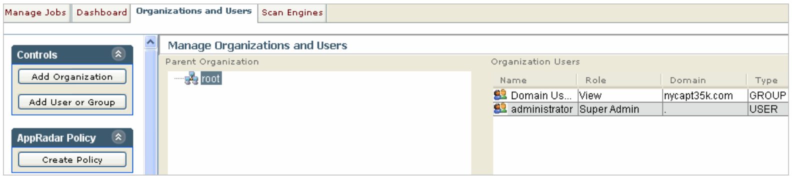
To add a User:

1. Do one of the following to display the **Manage Organizations and Users** page:
   - Choose **Admin** > **Organizations and Users** from the menu
   - Click the **Organizations and Users** tab.

The **Manage Organizations and Users** page displays your existing:

- Organizations (in the **Parent Organization** portion of the **Manage Organizations and Users** page)
- Users and Groups (in the **Organization Users** portion of the **Manage Organizations and Users** page).

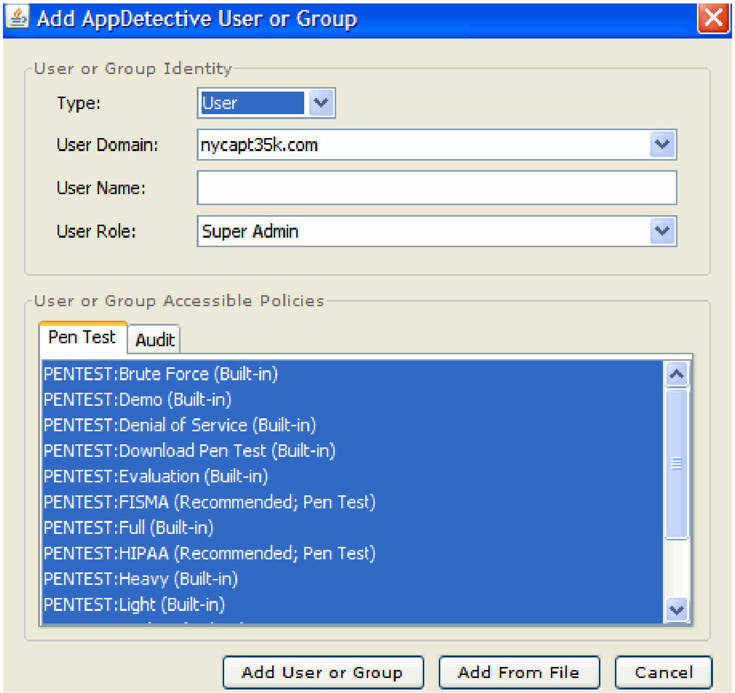
Hint: Highlight an Organization in the **Parent Organization** portion of the **Manage Organizations and Users** page to display its subordinate Users and Groups, and to activate the Control buttons and menu items.



Name	Role	Domain	Type
Domain Us...	View	nycapt35k.com	GROUP
administrator	Super Admin	.	USER

FIGURE: **Manage Organizations and Users** page

2. Do one of the following to display the Add AppDetective User or Group dialog box:
   - Choose **Organizations and Users > Add User or Group** from the menu
   - Click the **Add User or Group** button in the Controls portion of the **Manage Organizations and Users** page
   - Right click an Organization (in the **Parent Organization** portion of the **Manage Organizations and Users** page) and choose **Add User**.



Add AppDetective User or Group

User or Group Identity

Type: User

User Domain: nycapt35k.com

User Name:

User Role: Super Admin

User or Group Accessible Policies

PENTEST:Brute Force (Built-in)
PENTEST:Demo (Built-in)
PENTEST:Denial of Service (Built-in)
PENTEST:Download Pen Test (Built-in)
PENTEST:Evaluation (Built-in)
PENTEST:FISMA (Recommended; Pen Test)
PENTEST:Full (Built-in)
PENTEST:HIPAA (Recommended; Pen Test)
PENTEST:Heavy (Built-in)
PENTEST:Light (Built-in)

FIGURE: **Add AppDetective User or Group** dialog box

3. Do the following:
   - Use the **Type:** drop-down to select **User**.
   - Enter a User name in the **User Name:** field (for example, `jsmith`).
   - Use the **User Domain:** drop-down to select the User's network domain.
   - Use the **User Role:** drop-down to associate the User with a role (i.e., **Super Admin**, **Admin**, **Basic User**, **View User**); for more information, see the *DbProtect Administrator's Guide*.

- In the **User or Group Accessible Policies** portion of the **Add AppDetective User or Group** dialog box, highlight which Penetration Test and Audit Policies the User or Group can use (or un-highlight restricted Policies).

  You can click the:

  -**Pen Test** tab, and highlight which Penetration Test Policies the User can use (or un-highlight restricted Penetration Test Policies)

  -**Audit** tab, and highlight which Audit Policies the User can use (or un-highlight restricted Audit Policies).

4. Click the **Add User or Group** button to save your new User.

The new User displays in the **Organization Users** portion of the **Manage Organizations and Users** page.

Editing a User

Note: If DbProtect Vulnerability Management does **not** run as a domain User, you must also add local (i.e., non-domain) Users.

To edit a User:

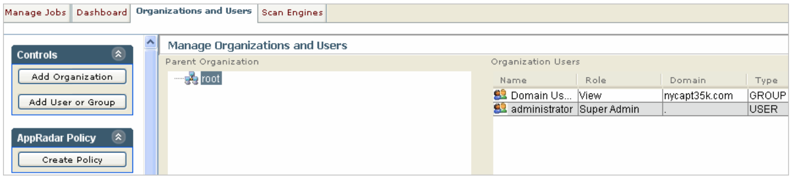
1. Do one of the following to display the **Manage Organizations and Users** page:

- Choose **Admin** > **Organizations and Users** from the menu
- Click the **Organizations and Users** tab.

The **Manage Organizations and Users** page displays your existing:

- Organizations (in the **Parent Organization** portion of the **Manage Organizations and Users** page)
- Users and Groups (in the **Organization Users** portion of the **Manage Organizations and Users** page).

Hint: Highlight an Organization in the **Parent Organization** portion of the **Manage Organizations and Users** page to display its subordinate Users and Groups, and to activate the Control buttons and menu items.



Name	Role	Domain	Type
Domain Us...	View	nycapt35k.com	GROUP
administrator	Super Admin	.	USER

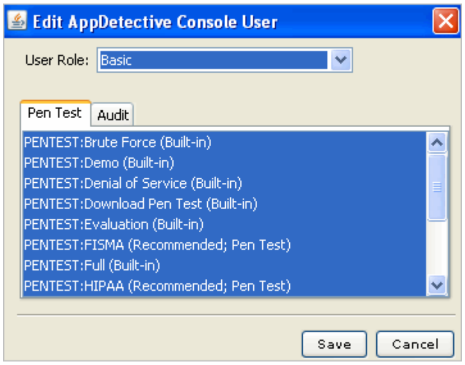
FIGURE: **Manage Organizations and Users** page

2. Do one of the following:

- Highlight a User in the **Organization Users** portion of the **Manage Organizations and Users** page, and choose **Organizations and Users** > **Edit User or Group** from the menu

- Right click a User (in the **Organization Users** portion of the **Manage Organizations and Users** page) and choose **Edit**.
- Double click a User (in the **Organization Users** portion of the **Manage Organizations and Users** page).

The **Edit DbProtect Console User** dialog box displays.



Edit AppDetective Console User
User Role:
Basic
Pen Test
Audit
PENTEST:Brute Force (Built-in)
PENTEST:Demo (Built-in)
PENTEST:Denial of Service (Built-in)
PENTEST:Download Pen Test (Built-in)
PENTEST:Evaluation (Built-in)
PENTEST:FISMA (Recommended; Pen Test)
PENTEST:Full (Built-in)
PENTEST:HIPAA (Recommended; Pen Test)
Save
Cancel

FIGURE: **Edit AppDetective Console User** dialog box

3. Use the **User Role:** drop-down to associate the User with a different User or Group type (i.e., **Super Admin**, **Admin**, **Basic User**, **View User**); for more information, see the *DbProtect Administrator's Guide*.
4. In the **User or Group Accessible Policies** portion of the **Edit AppDetective Console User** dialog box, highlight which Penetration Test and Audit Policies the User can use (or un-highlight restricted Policies).

You can click the:

- **Pen Test** tab, and highlight which Penetration Test Policies the User can use (or un-highlight restricted Penetration Test Policies)
- **Audit** tab, and highlight which Audit Policies the User can use (or un-highlight restricted Audit Policies).

5. Click the **Save** button to save your edited User.

The edited User displays in the **Organization Users** portion of the **Manage Organizations and Users** page.

Removing a User

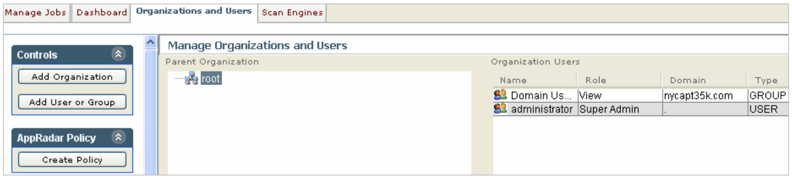
To remove a User:

1. Do one of the following to display the **Manage Organizations and Users** page:
   - Choose **Admin > Organizations and Users** from the menu
   - Click the **Organizations and Users** tab.

The **Manage Organizations and Users** page displays your existing:

- Organizations (in the **Parent Organization** portion of the **Manage Organizations and Users** page)
- Users and Groups (in the **Organization Users** portion of the **Manage Organizations and Users** page).

Hint: Highlight an Organization in the **Parent Organization** portion of the **Manage Organizations and Users** page to display its subordinate Users and Groups, and to activate the Control buttons and menu items.



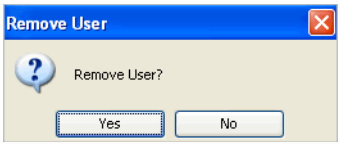
Name	Role	Domain	Type
Domain Us...	View	nycapt35k.com	GROUP
administrator	Super Admin	.	USER

FIGURE: **Manage Organizations and Users** page

2. Do one of the following:

- Highlight a User in the **Organization Users** portion of the **Manage Organizations and Users** page, and choose **Organizations and Users > Remove User** from the menu
- Right click User (in the **Organization Users** portion of the **Manage Organizations and Users** page) and choose **Remove**.

The **Remove User?** or **Remove Group?** pop up displays, prompting you to confirm the removal.



Remove User?

FIGURE: **Remove User?** pop up

3. Click the **Yes** button to remove the User.

The User is removed from the **Organization Users** portion of the **Manage Organizations and Users** page.

Creating a DbProtect Audit and Threat Management Policy

You can create a DbProtect Audit and Threat Management Policy based on vulnerabilities detected in applications using DbProtect Vulnerability Management.

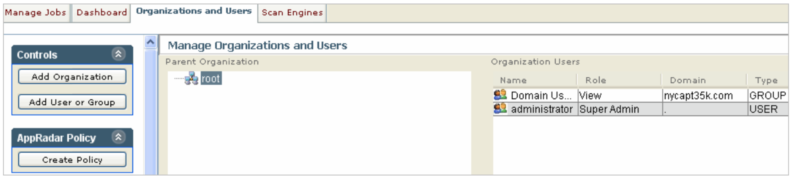
To create a DbProtect Audit and Threat Management Policy:

1. Do one of the following to display the **Manage Organizations and Users** page:
   - Choose **Admin** > **Organizations and Users** from the menu
   - Click the **Organizations and Users** tab.

The **Manage Organizations and Users** page displays your existing:

- Organizations (in the **Parent Organization** portion of the **Manage Organizations and Users** page)
- Users and Groups (in the **Organization Users** portion of the **Manage Organizations and Users** page).

Hint: Highlight an Organization in the **Parent Organization** portion of the **Manage Organizations and Users** page to display its subordinate Users and Groups, and to activate the Control buttons and menu items.



Name	Role	Domain	Type
Domain Us...	View	nycapt35k.com	GROUP
administrator	Super Admin	.	USER

FIGURE: **Manage Organizations and Users** page

2. Locate the **AppRadar Policy** Toolbar on the **Manage Jobs** page; for more information, see *Understanding the Manage Jobs page*.
3. Click the **AppRadar Policy** button to display the **AppRadar Policy Generator** dialog box.

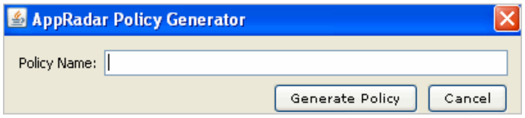


FIGURE: **AppRadar Policy Generator** dialog box

4. Enter a DbProtect Audit and Threat Management Policy name in the **Policy Name:** field.

5. Click the **Generate Policy** button.

DbProtect Vulnerability Management creates a DbProtect Audit and Threat Management Policy based on vulnerabilities detected in applications in your selected Organization. This new Policy is dynamically created on the **Policies** page in DbProtect Audit and Threat Management. You do **not** have to import the Policy.

Customer Support

Customer Support is available from 9 A.M. to 9 P.M. (GMT -5) Monday through

Friday, except for company holidays. You may contact technical support for the list of company holidays.

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

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

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

Email: `support@appsecinc.com`

Vulnerability Management

DbProtect’s **Vulnerability Management** Scan Engines discover database applications within your infrastructure and assesses their security strength. Backed by a proven security methodology and extensive knowledge of application-level vulnerabilities, DbProtect locates, examines, reports, and fixes security holes and misconfigurations.

DbProtect assesses your database vulnerabilities and customizes Policies based on each deployment’s unique parameters and requirements.

This chapter of the *DbProtect User’s Guide* discusses how to use the **DbProtect Vulnerability Management** UI to perform Vulnerability Management tasks on your enterprise database applications.

This section consists of the following chapters:

- *Understanding the DbProtect Vulnerability Management Portal User Interface (UI)*
- *Vulnerability Management User Roles*
- *Working with Jobs*
- *Working with the Dashboard*
- *Working with Scan Engines*
- *Working with Policies*
- *Working with Credential Profiles and User Credential Files*
- *Working with Fix Scripts.*

Understanding the DbProtect Vulnerability Management Portal User Interface (UI)

This chapter consists of the following topics:

- *What is the DbProtect Vulnerability Management UI?*
- *DbProtect Vulnerability Management UI components*
- *Understanding the DbProtect Vulnerability Management UI menus*.

What is the DbProtect Vulnerability Management UI?

The **DbProtect Vulnerability Management UI** is the web browser-based, graphical component of DbProtect that allows you to navigate to the various features of DbProtect Vulnerability Management.

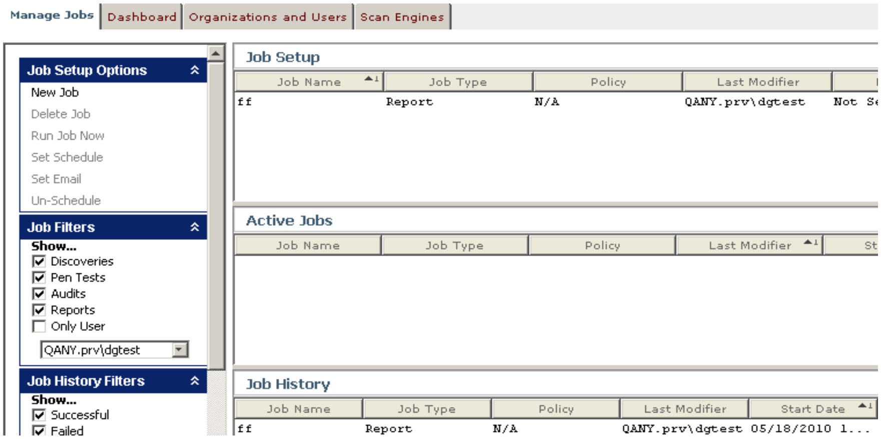
The **DbProtect Vulnerability Management UI** is comprised of the:

- **Manage Jobs** page; for more information, see *Understanding the Manage Jobs page*
- **Dashboard**; for more information, see *Understanding the Dashboard*
- **Manage Organizations and Users** page (for Admins and Super Admins only); for more information, see *Understanding the Manage Organizations and Users page*
- **Scan Engines** page (for Super Admins only); for more information, see *Understanding the Scan Engines page*.

UNDERSTANDING THE MANAGE JOBS PAGE

The **Manage Jobs** page (shown below) allows you to create, schedule, run, filter, refresh, and delete Jobs. DbProtect Vulnerability Management allows you to run the following Job types: Audit, Penetration Test, Discovery, and Report.

For more information, see *Working with Jobs*.



Job Filters
Show...
☑ Discoveries
☑ Pen Tests
☑ Audits
☑ Reports
☐ Only User
QANY.prv\dgtest

Job History Filters
Show...
☑ Successful
☑ Failed

Job Setup

Job Name	Job Type	Policy	Last Modifier	
ff	Report	N/A	QANY.prv\dgtest	Not Se

Active Jobs

Job Name	Job Type	Policy	Last Modifier	St

Job History

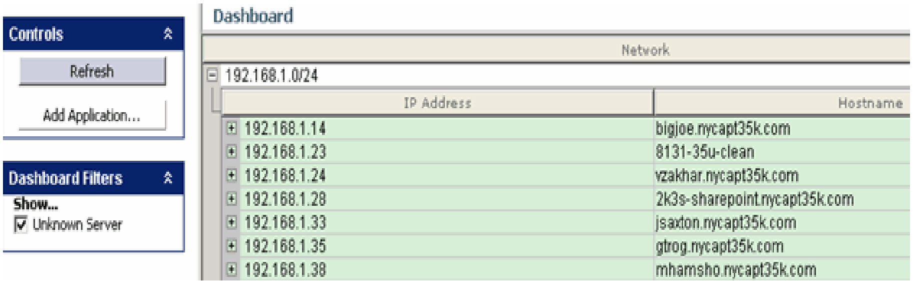
Job Name	Job Type	Policy	Last Modifier	Start Date
ff	Report	N/A	QANY.prv\dgtest	05/18/2010 1...

FIGURE: **Manage Jobs** page

UNDERSTANDING THE DASHBOARD

The **Dashboard** (shown below) displays detailed data about applications Discovered on your network, recent Penetration Tests and Audits performed, and the number of vulnerabilities detected.

For more information, see *Working with the Dashboard*.



Dashboard Filters
Show...
☑ Unknown Server

192.168.1.0/24

IP Address	Hostname
192.168.1.14	bigjoe.nycapt35k.com
192.168.1.23	8131-35u-clean
192.168.1.24	vzakhar.nycapt35k.com
192.168.1.28	2k3s-sharepoint.nycapt35k.com
192.168.1.33	jsaxton.nycapt35k.com
192.168.1.35	gtrog.nycapt35k.com
192.168.1.38	mhamsho.nycapt35k.com

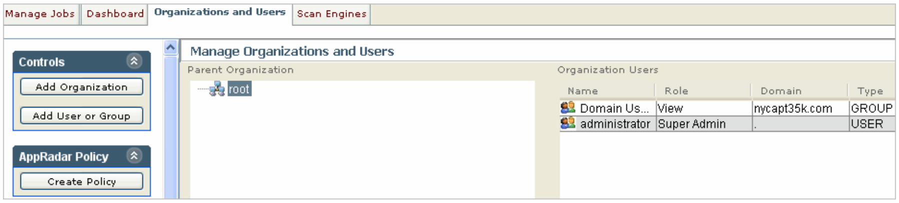
FIGURE: **Dashboard**

UNDERSTANDING THE MANAGE ORGANIZATIONS AND USERS PAGE

The **Manage Organizations and Users** page (shown below) allows you to create logical and hierarchical Organizations (for example, `AUDIT`, `RISK`, `PRIVATE BANKING`, etc.). You can define a set of IP ranges and Policies for each Organization (which you can modify at the User or Group level). Your Organizations can be exclusive and isolated from other Organizations.

After you create Organizations, you can create subordinate **Users** and **Groups**. Users and Groups are Windows entities taken from either the Active Directory or your local system. You must explicitly add Users and Groups as DbProtect Vulnerability Management Users in order to authorize them to use DbProtect Vulnerability Management.

For more information, see *Working with Scan Engines*.



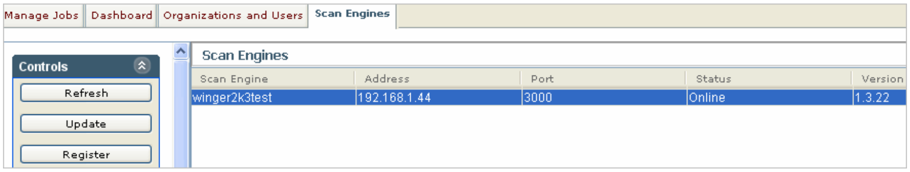
Name	Role	Domain	Type
Domain Us...	View	nycapt35k.com	GROUP
administrator	Super Admin	.	USER

FIGURE: **Organizations and Users** page

UNDERSTANDING THE SCAN ENGINES PAGE

The **Scan Engines** page (shown below) allows you to manage your installed and configured Scan Engines. Specifically, the **Scan Engines** page allows you to register (and unregister) your installed/configured Scan Engines, refresh the Scan Engine, monitor the “health” of your installed/configured/registered Scan Engines, or run an ASAP Update to obtain the latest Scan Engine software.

For more information, see *Working with Scan Engines*.



Scan Engine	Address	Port	Status	Version
winger2k3test	192.168.1.44	3000	Online	1.3.22

FIGURE: **Scan Engines** page

DbProtect Vulnerability Management UI components

A portion of the DbProtect Vulnerability Management UI (i.e., the **Dashboard**) is shown below, with its parts labeled.

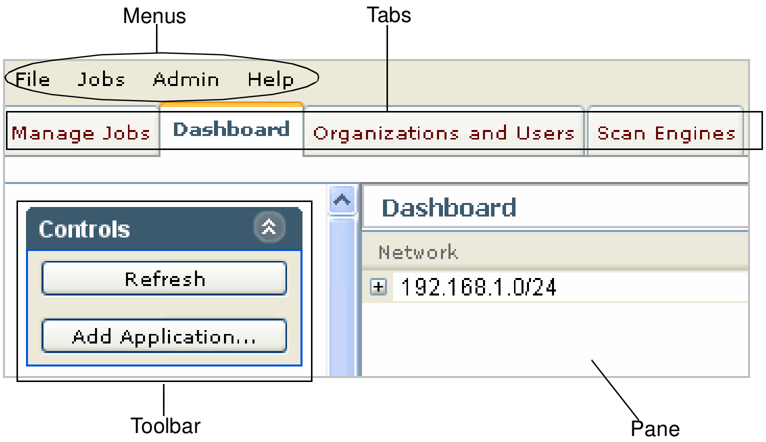


FIGURE: DbProtect Vulnerability Management UI components (example from the **Dashboard**)

Every DbProtect Vulnerability Management UI page consists of the following components:

- *Tabs*
- *Menus*
- *Toolbars*
- *Pane*.

TABS

The **tabs** allow you to toggle between the DbProtect Vulnerability Management UI pages. The tabs are global, meaning they display no matter what DbProtect Vulnerability Management UI page you are on.

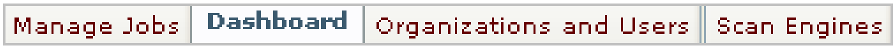


FIGURE: Tabs

Note: The **Organizations and Users** and **Scan Engines** tabs only displays for Super Users. For more information, see the *DbProtect Administrator's Guide*.

MENUS

The **menus** allow you to perform tasks such as creating Job templates (for Discovery, Penetration Test, Audit, and Report Jobs), managing Credential Profiles, configuring your Scan Engines, managing your Organizations and Users, etc. The menus are global, meaning they display no matter what DbProtect Vulnerability Management UI page you are on.

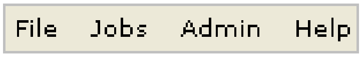


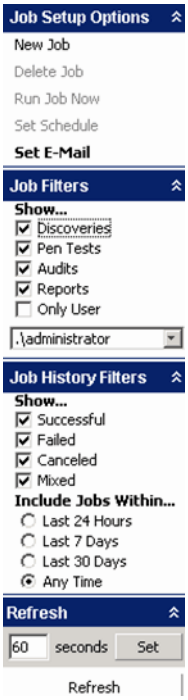
FIGURE: Menus

Note: The **Admin** menu only displays for Super Users and Admin Users. For more information, see the *DbProtect Administrator's Guide*.

For more information on the DbProtect Vulnerability Management UI menus, see *Understanding the DbProtect Vulnerability Management Portal User Interface (UI)*.

TOOLBARS

Depending which tab you click and page you select, the DbProtect Vulnerability Management UI displays a corresponding set of page-specific **Toolbars**. The Toolbars allow you to perform such tasks as creating/running Jobs, refreshing and updating data on a page, registering Scan Engines, adding applications to Discover, manually refreshing a Scan Engine, setting the Scan Engine refresh rate, etc.



Show...
☑ Discoveries
☑ Pen Tests
☑ Audits
☑ Reports
□ Only User
.\administrator

Show...
☑ Successful
☑ Failed
☑ Canceled
☑ Mixed

Include Jobs Within...
○ Last 24 Hours
○ Last 7 Days
○ Last 30 Days
● Any Time

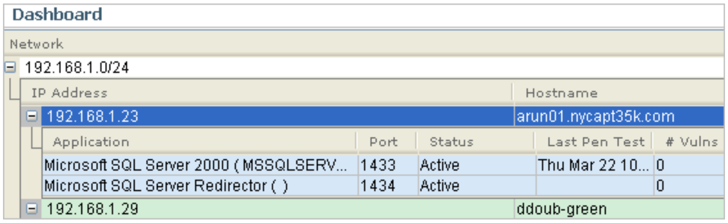
60 seconds

FIGURE: Toolbar (example from the **Manage Jobs** page)

PANE

Depending which tab you click and page you select, the DbProtect Vulnerability Management UI displays a page-specific **pane**. The pane displays your DbProtect Vulnerability Management data.

For example, the **Dashboard** pane (shown below) displays data about your networks, Discovered applications, last Penetration Test, etc.



Dashboard

Network

⊟ 192.168.1.0/24

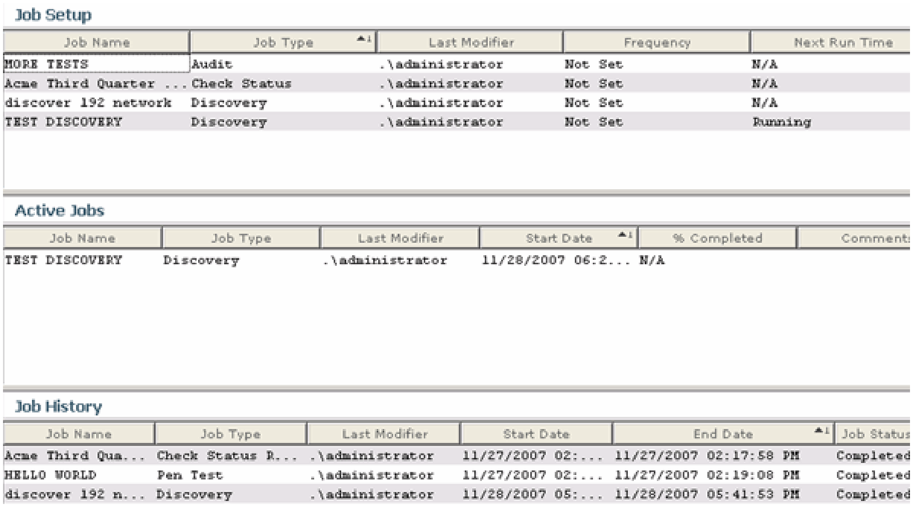
IP Address	Hostname
⊟ 192.168.1.23	arun01.nycapt35k.com

Application	Port	Status	Last Pen Test	# Vulns
Microsoft SQL Server 2000 (MSSQLSERV...	1433	Active	Thu Mar 22 10...	0
Microsoft SQL Server Redirector ( )	1434	Active		0

⊟ 192.168.1.29	ddoub-green

FIGURE: Pane (example from the **Dashboard**)

However, on the **Manage Jobs** page, the pane is different (shown below). The pane on the **Manage Jobs** page consists of three portions (**Job Setup**, **Active Jobs**, and **Job History**), each of which contain different information about created/scheduled Jobs, active (i.e., currently-running) Jobs, and completed Jobs, respectively.



Job Setup

Job Name	Job Type	Last Modifier	Frequency	Next Run Time
MORE TESTS	Audit	.\administrator	Not Set	N/A
Acme Third Quarter ...	Check Status	.\administrator	Not Set	N/A
discover 192 network	Discovery	.\administrator	Not Set	N/A
TEST DISCOVERY	Discovery	.\administrator	Not Set	Running

Active Jobs

Job Name	Job Type	Last Modifier	Start Date	% Completed	Comment
TEST DISCOVERY	Discovery	.\administrator	11/28/2007 06:2...	N/A	

Job History

Job Name	Job Type	Last Modifier	Start Date	End Date	Job Status
Acme Third Qua...	Check Status R...	.\administrator	11/27/2007 02:...	11/27/2007 02:17:58 PM	Completed
HELLO WORLD	Pen Test	.\administrator	11/27/2007 02:...	11/27/2007 02:19:08 PM	Completed
discover 192 n...	Discovery	.\administrator	11/28/2007 05:...	11/28/2007 05:41:53 PM	Completed

FIGURE: Pane (example from the **Manage Jobs** page)

Understanding the DbProtect Vulnerability Management UI menus

The DbProtect Vulnerability Management UI consists of the following **menus**:

- *File menu*
- *Jobs menu*
- *Admin menu*

Note: The **Admin** menu only displays for DbProtect Super Admins, DbProtect Admins, and Vulnerability Management Admins.

FILE MENU

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

- **File** > **Credential Profile Manager** to view and modify your Organization's Audit credentials; for more information, see *Setting and testing your database and operating system credentials*.

JOBS MENU

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

- **Jobs** > **Templates** > **New Discovery** to create a new Discovery Job; for more information, see *Discovery Jobs*.
- **Jobs** > **Templates** > **New Audit** to create a new Audit Job; for more information, see *Audit Jobs*.
- **Jobs** > **Templates** > **New Pentest** to create a new Penetration Test Job; for more information, see *Penetration Test Jobs*.
- **Jobs > Templates > New Report** to create a new Report Job; for more information, see *Report Jobs*.
- **Jobs > Manage** to view, schedule, and apply filters to your Discovery, Penetration Test, Audit, and Report Jobs; for more information, see *Working with Jobs*.

ADMIN MENU

Note: The **Admin** menu item only displays for Super Users and Admin Users; for more information, see the *DbProtect Administrator's Guide*.

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

- **Admin** > **Dashboard** to display the **Dashboard**; for more information, see *Working with the Dashboard*
- **Admin** > **Organizations and Users** to display the **Organizations and Users** page; for more information, see *Working with Scan Engines*
- **Admin** > **Scan Engines** to display the **Select Scan Engine** page and view information about your registered Scan Engines; for more information, see *Working with Scan Engines*.

Vulnerability Management User Roles

For information on **Vulnerability Management user roles**, and all other roles (and associated privileges) in DbProtect, see *DbProtect Organizations, Users, and User Roles* in the *DbProtect Organizations, Users, and User Roles* section of this guide.

Working with Jobs

This chapter consists of the following topics:

- *What are Jobs?*
- *Understanding the Manage Jobs page*
- *Discovery Jobs*
- *Penetration Test Jobs*
- *Audit Jobs*
- *Report Jobs*
- *"Run Job Now"*
- *Editing a Job*
- *Scheduling a Job*
- *Unscheduling a Job*
- *Viewing a completed Report*
- *Saving a completed Report*
- *Filtering Jobs*
- *Filtering Job history*
- *Deleting a set up Job*
- *Purging a completed Job*
- *Cancelling an active Job*
- *Deleting an application to Discover*
- *Viewing Job details*
- *Viewing the properties of a completed Job*
- *Viewing individual vulnerabilities detected during an Audit*
- *Setting the refresh rate of data on the Manage Jobs page*
- *Manually refreshing data on the Manage Jobs Page*
- *Scheduling email notification upon Job completion.*

What are Jobs?

DbProtect Vulnerability Management allows you to create and schedule any of the following types of **Jobs**. They are:

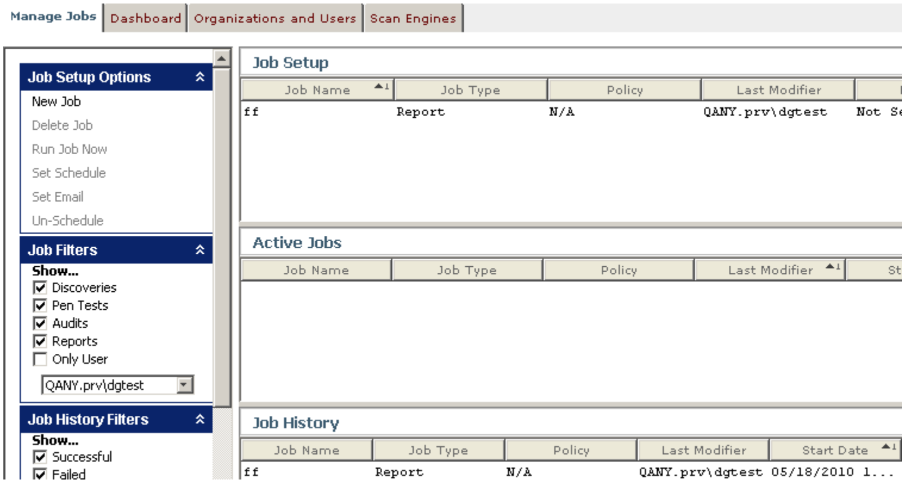
- **Discovery Jobs.** A Discovery locates applications on your network, and identifies the applications' IP addresses (as well as ports used to provide network services). For more information, see *Discovery Jobs*.
- **Penetration Test Jobs and Audit Jobs.** Penetration Tests assess the security of your applications by running security checks (based on a Policy you choose). Penetration Tests perform a non-authenticated but non-intrusive test against your applications. They also commonly uncover misconfiguration errors, in addition to well-known application vulnerabilities.

  Audits test the security of your applications (which requires system credentials on databases such as Oracle). The Audit checks your Discovered applications for password configurations, table access, User roles, and other vulnerabilities.

  For more information, see *Penetration Test Jobs* and *Audit Jobs*.
- You can install the Scan Engine on the same server as the DbProtect Console, where the Scan Engine (by default) can run a maximum of three Penetration Tests and Audits concurrently. Or, you can install the Scan Engine on a *remote* server, where the Scan Engine (by default) can run a maximum of 10 Penetration Tests and Audits concurrently. You can modify these default values, post-installation; for more information, see *Editing a Scan Engine*.
- **Report Jobs.** These are designed to communicate vulnerabilities Discovered by DbProtect Vulnerability Management to all levels of your Organization. For more information, see *Report Jobs*.

Understanding the Manage Jobs page

The **Manage Jobs** page is shown below.



Job Filters

Show...

☑ Discoveries

☑ Pen Tests

☑ Audits

☑ Reports

□ Only User

QANY.prv\dgtest

Job History Filters

Show...

☑ Successful

☑ Failed

Job Setup

Job Name	Job Type	Policy	Last Modifier	
ff	Report	N/A	QANY.prv\dgtest	Not Se

Active Jobs

Job Name	Job Type	Policy	Last Modifier	St

Job History

Job Name	Job Type	Policy	Last Modifier	Start Date
ff	Report	N/A	QANY.prv\dgtest	05/18/2010 1...

FIGURE: **Manage Jobs** page

The pane of the **Manage Jobs** page is divided into three portions:

- **Job Setup.** The columns in this portion of the pane display the following information about set up Jobs:

  -Job Name. The name of the set up Discovery, Penetration Test, Audit, or Report Job.

  -Job Type. The type of the set up Job (i.e., **Discovery**, **Penetration Test, Audit**, or **Report**).

  -**Policy.** The Policy associated with the Job; for more information, see *Working with Policies*.

  -Last Modifier. The ID of the last person to modify the set up Discovery, Penetration Test, Audit, or Report Job.

  -Frequency. The frequency of the set up Discovery, Penetration Test, Audit, or Report Job (i.e., **Daily**, **Weekly**, **Monthly**, etc.).

  -Next Run Time. The next scheduled run time of the set up Discovery, Penetration Test, Audit, or Report Job.

- **Active Jobs.** The columns in this portion of the pane display the following information about active Jobs:

  -Job Name. The name of the active Discovery, Penetration Test, Audit, or Report Job.

  -Job Type. The type of the active Job (i.e., **Discovery**, **Penetration Test, Audit**, or **Report**).

  -Last Modifier. The ID of the last person to modify the active Discovery, Penetration Test, Audit, or Report Job.

  -Start Date. The date the active Job started.

  -% Completed. The completion percentage of the active Job as it processes.

-**Comments.** If you cancel a Job, this column displays a cancellation message. Otherwise, this column remains blank.

- **Job History.** The columns in this portion of the pane display the following information about completed Jobs:

  -**Job Name.** The name of the completed Discovery, Penetration Test, Audit, or Report Job.

  -**Job Type.** The type of completed Job (i.e., **Discovery**, **Penetration Test, Audit**, or **Report**).

  -**Last Modifier.** The ID of the last person to modify the completed Discovery, Penetration Test, Audit, or Report Job.

  -**Start Date.** The date the completed Job started.

  -**End Date.** The date the completed Job finished.

  -**Job Status.** The status of the completed Job (i.e., **Completed**, **Canceled**, **Failed**, and **Click for details**).

Note: For more information on the pane and other DbProtect Vulnerability Management UI components, see *Understanding the DbProtect Vulnerability Management Portal User Interface (UI).*

Specifically, the **Manage Jobs** page allows you to:

- **create** Discovery, Audit, Penetration Test, and Report Jobs; for more information, see *Creating a Discovery Job*, *Creating an Audit Job*, *Creating a Penetration Test Job*, and *Creating a Report Job*, respectively
- **edit** Jobs; for more information, see *Editing a Job*
- **run** a Job now; for more information, see *"Run Job Now"*
- **schedule** Jobs; for more information, see *Scheduling a Job*
- **view** and **save** completed Reports for any type of Job; for more information, see *Viewing a completed Report* and *Saving a completed Report*, respectively
- **filter** Jobs and Job history; for more information, see *Filtering Jobs* and *Filtering Job history*, respectively
- **delete** a set up Job; for more information, see *Deleting a set up Job*
- **cancel** an active Job; for more information, see *Cancelling an active Job*
- **purge** a completed Job; for more information, see *Purging a completed Job*
- view the **details** of an active or completed Job; for more information, see *Viewing Job details*
- view the **properties** of a completed Job; for more information, see *Viewing the properties of a completed Job*
- set the **Manage Jobs** page data **refresh rate**; for more information, see *Setting the refresh rate of data on the Manage Jobs page*
- manually **refresh** the data on the **Manage Jobs** page; for more information, see *Manually refreshing data on the Manage Jobs Page*
- schedule **email notification** upon Job completion; for more information, see *Scheduling email notification upon Job completion*.

Discovery Jobs

This topic consists of the following sub-topics:

- *What is a Discovery Job?*
- *Manually Adding Oracle SIDs and DB2 Databases to Discover*
- *Creating a Discovery Job*.

WHAT IS A DISCOVERY JOB?

When DbProtect Vulnerability Management performs a **Discovery Job**, it:

- locates applications on your network
- identifies the applications' IP addresses (as well as ports used to provide network services).

Note: Discovery does **not** identify vulnerabilities. This is the function of Penetration Tests and Audits. For more information, see *What is a Penetration Test?* and *What is an Audit?*, respectively.

MANUALLY ADDING ORACLE SIDS AND DB2 DATABASES TO DISCOVER

When you run an Oracle Discovery, DbProtect only detects the Oracle Listener (unless you specified a listener password during Scan Engine installation; for more information, see the *DbProtect Installation Guide*). In order to run an Audit on a Discovered Oracle database, the Oracle SID **must** display in the **Dashboard**. Therefore, in most cases, you must manually add the Oracle SID to the **Dashboard** before you run an Audit.

The same is true for running an Audit Jobs on DB2. When you run a DB2 Discovery, DbProtect only detects the DB2 instance. In order to run an Audit on a Discovered DB2 database, the DB2 database **must** display in the **Dashboard**. Therefore, in most cases, you must manually add the DB2 database to the Dashboard by following the steps in this topic.

For more information on:

- running an Audit Job, see *Audit Jobs*
- running a Penetration Test Job, see *Penetration Test Jobs*
- manually adding an application to Discover, see *Adding an application to Discover*.

CREATING A DISCOVERY JOB

To create a Discovery Job:

1. Do one of the following to display the **Discovery Job Template** dialog box:

- Choose **Jobs > Templates > New Discovery** from the menu.
- Click the **Manage Jobs** tab, and choose **New Job > New Discovery** in the **Job Setup Options** Toolbar on the **Manage Jobs** page; for more information, see *Toolbars*.

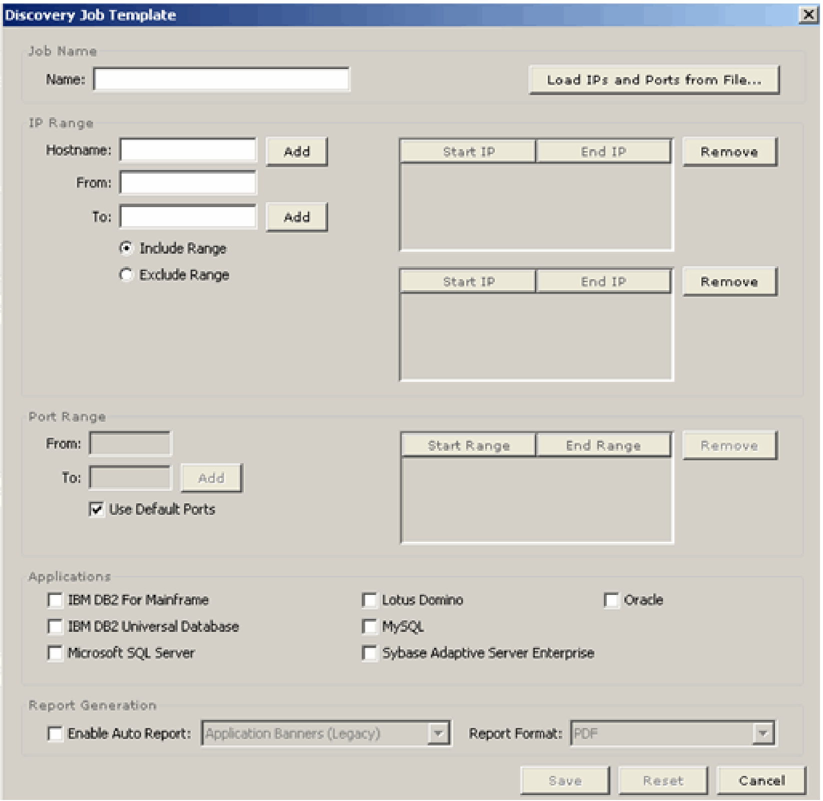


FIGURE: **Discovery Job Template** dialog box

2. In the **Job Name:** portion of the **Discovery Job Template** dialog box:

- Enter the name of your new Discovery Job in the **Name:** field (required).
- Click the **Load IPs and Ports from file...** button to display an **Open** dialog box and upload a standard, comma-delimited text file. You can use any of the following formats:

  -`ip` (for example, `192.168.1.1`)

  -`ip, port` (for example, `192.168.1.1, 8080`)

-`ip-ip` (for example, `192.168.1.1-192.168.1.255`)

-`ip-ip,port` (for example, `192.168.1.1-192.168.1.255, 8080`)

-Classless Inter Domain Routing (CIDR) notation, i.e., `ip/network prefix` (for example, `192.9.205.22/18`); for more information on CIDR notation, see *http://infocenter.guardiandigital.com/manuals/IDDS/node9.html*

Caution! When running a Discovery for IBM DB2 (using either file identification method described above), you **must** include the DB2 Administration Server (DAS) port (`523` by default) to ensure DbProtect Vulnerability Management will Discover all databases. Otherwise, DbProtect Vulnerability Management will only Discover the default databases (i.e. `SAMPLE`).

Note: The DbProtect Vulnerability Management does **not** support NMAP. However, AppDetectivePro **does** support NMAP; for more information, see the *AppDetectivePro User's Guide*.

3. In the **IP Range** portion of the **Discovery Job Template** dialog box:

- Specify the IP addresses you want to **include** (and **exclude**) in your Discovery.

  If you want to specify IP addresses to **include** in your Discovery, then:

  -Manually enter the host name of the machine where you want to perform a Discovery in the **Hostname:** field.

  -Click the **Add** button.

  -Select **Include Range**.

If you want to specify IP addresses to **exclude** from your Discovery, then:

-Manually enter the host name of the machine where you want to perform a Discovery in the **Hostname:** field.

-Click the **Add** button.

-Select **Exclude Range**.

- Optionally, you can highlight one or more individual IP address ranges from the include/exclude list, and click the **Remove** button to remove them.

Hint: Click <CTRL> to highlight non-sequential IP address ranges.

4. In the **Port Range** portion of the **Discovery Job Template** dialog box:

- Check **Use Default Ports** if you want DbProtect Vulnerability Management to probe standard default installation ports for applications (that you **must** select below). For example, SQL Server is installed, by default, on port `1433`. Oracle is installed, by default, on port `1521`.
- Check one or more of the following application types to Discover:

  -IBM DB2 for Mainframe

  -IBM DB2 Universal Database

  -Microsoft SQL Server

  -Lotus Domino

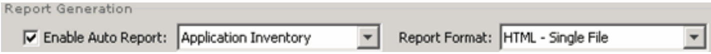
-**MySQL**

-**Sybase Advance Server Enterprise**

-**Oracle**.

5. Auto-generate a Report upon completion of your Discovery Job.

The **Report Generation** portion of the **Discovery Job Template** dialog box allows you to automatically generate an **Application Inventory** Report upon completion of your Discovery Job. For more information on Report types, see *Report types*.



Report Generation

☑ Enable Auto Report: Application Inventory

Report Format: HTML - Single File

FIGURE: **Report Generation** section of the **Discovery Job Template** dialog box

If you want to use the Report auto-generation feature, do the following:

- Check the **Enable Auto Report** checkbox in the **Report Generation** portion of the **Discovery Job Template** dialog box. The **Job History** portion of the pane displays the status of your auto Report Job after your Discovery Job completes. The format that displays is: `"for JOB_TYPE JOB_NAME [ran at 11/29/2007 12:23:20]"`
- Use the Report type drop-down to select an **Application Inventory** Report for auto-generation upon completion of your Discovery Job; for more information on Report types, see *Report types*.
- Use the **Report Format** drop-down to select whether you want to auto-generate your Report in any of the following formats:

  -**HTML - Single File**

  -**Text**

  -**XML**

  -**PDF**.

For more information on Report formats, see *Report formats*.

If you use the Report auto-generation feature to generate a Report for a Discovery Job, you can:

- view the completed Report (when the Job is complete) in whatever format you specified in this step; for more information, see *Viewing a completed Report*
- save the completed Report (when the Job is complete) in whatever format you specified in this step; for more information, see *Saving a completed Report*.

6. Click the **Save** button to save your Discovery Job.

7. You can:

- run the Discovery Job now; for more information, see *"Run Job Now"*
- schedule the Discovery Job to run later; for more information, see *Scheduling a Job*.

8. After your Discovery Job completes, you can:

- view the completed Job details; for more information, see *Viewing Job details*
- view the completed Job properties; for more information, see *Viewing the properties of a completed Job*.

Penetration Test Jobs

This topic consists of the following sub-topics:

- *What is a Penetration Test?*
- *Manually Adding Oracle SIDs and DB2 Databases to Discover (Pre-Penetration Test)*
- *What Does a Penetration Test Do to My System?*
- *Creating a Penetration Test Job*.

WHAT IS A PENETRATION TEST?

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

- are run from an "outside-in" perspective
- gives a good analysis of what a hacker or intruder might discover when attempting to bypass your application's defenses
- commonly uncover misconfiguration errors in addition to well-known application vulnerabilities.

This section explains how to create Penetration Test and Audit Jobs using DbProtect Vulnerability Management. Penetration Tests may only be performed after you have performed a Discovery Job.

MANUALLY ADDING ORACLE SIDS AND DB2 DATABASES TO DISCOVER (PRE-PENETRATION TEST)

When you run an Oracle Discovery, DbProtect only detects the Oracle Listener (unless you specified a listener password during Scan Engine installation; for more information, see the *DbProtect Installation Guide*). In order to run a Penetration Test (or an Audit) on a Discovered Oracle database, the Oracle SID **must** display in the **Dashboard**. Therefore, in most cases, you must manually add the Oracle SID to the **Dashboard** before you run a Penetration Test (or an Audit).

The same is true for running Penetration Test (or an Audit) Jobs on DB2. When you run a DB2 Discovery, DbProtect only detects the DB2 instance. In order to run a Penetration Test (or an Audit) Job against a Discovered DB2 database, the DB2 database **must** display in the **Dashboard**. Again, in most cases, you must manually add the DB2 database to the **Dashboard** before you run a Penetration Test (or an Audit).

For more information on:

- running a Discovery Job, see *Discovery Jobs*
- running an Audit Job, see *Audit Jobs*
- manually adding an application to Discover, see *Adding an application to Discover*.

WHAT DOES A PENETRATION TEST DO TO MY SYSTEM?

A Penetration Test externally probes your database. Inherent to this activity is anonymous querying of network services for a variety of information. The User running DbProtect Vulnerability Management 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 Penetration Test, DbProtect Vulnerability Management can run tests which may result in acquiring a valid username and password that attackers can potentially use to authenticate to the application. In such cases, DbProtect Vulnerability Management performs the authentication in order to gather additional information from the application. It may connect to the database and gather username and password hashes, or configuration values. A Penetration Test does **not** make any updates or changes to your database. It may, however, read data such as the password hashes from the system.

CREATING A PENETRATION TEST JOB

To create a Penetration Test Job:

1. Do one of the following to display the **Pen Test Template Editor** dialog box:
   - Choose **Jobs > Templates > New Pentest** from the menu.
   - Click the **Manage Jobs** tab, and choose **New Job** > **New Pentest** in the **Job Setup Options** Toolbar on the **Manage Jobs** page; for more information, see *Toolbars*.

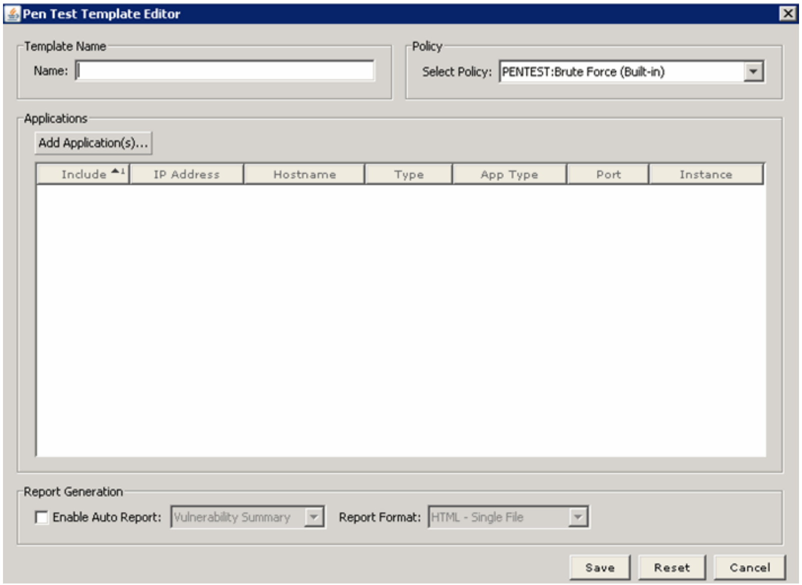
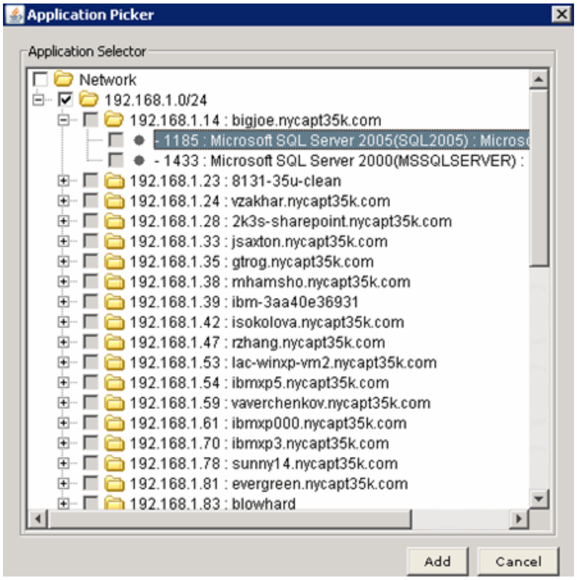


FIGURE: **Pen Test Template Editor** dialog box

2. In the **Template Name** portion of the **Pen Test Template Editor** dialog box, enter the name of your new Penetration Test Job in the **Name:** field.
3. In the **Policy** portion of the **Pen Test Template Editor** dialog box, use the **Select Policy:** drop-down to select your Penetration Test Policy.

4. Pick Applications to Penetration Test.

Click the **Add Application(s)...** button to display the **Application Picker**, which allows you to select which applications you want to Penetration Test.



- □ Network
  - ☑ 192.168.1.0/24
    - □ 192.168.1.14 : bigjoe.nycapt35k.com
      - □ ● - 1185 : Microsoft SQL Server 2005(SQL2005) : Micros
      - □ ● - 1433 : Microsoft SQL Server 2000(MSSQLSERVER) :
    - □ 192.168.1.23 : 8131-35u-clean
    - □ 192.168.1.24 : vzakhar.nycapt35k.com
    - □ 192.168.1.28 : 2k3s-sharepoint.nycapt35k.com
    - □ 192.168.1.33 : jsaxton.nycapt35k.com
    - □ 192.168.1.35 : gtrog.nycapt35k.com
    - □ 192.168.1.38 : mhamsho.nycapt35k.com
    - □ 192.168.1.39 : ibm-3aa40e36931
    - □ 192.168.1.42 : isokolova.nycapt35k.com
    - □ 192.168.1.47 : rzhang.nycapt35k.com
    - □ 192.168.1.53 : lac-winxp-vm2.nycapt35k.com
    - □ 192.168.1.54 : ibmxp5.nycapt35k.com
    - □ 192.168.1.59 : vaverchenkov.nycapt35k.com
    - □ 192.168.1.61 : ibmxp000.nycapt35k.com
    - □ 192.168.1.70 : ibmxp3.nycapt35k.com
    - □ 192.168.1.78 : sunny14.nycapt35k.com
    - □ 192.168.1.81 : evergreen.nycapt35k.com
    - □ 192.168.1.83 : blowhard

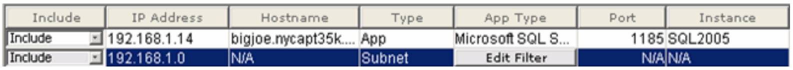
FIGURE: Application Picker

You can check:

- the **Network** checkbox to select all IPs (and subordinate subnets and applications) on a network
- a **subnet** checkbox to select all subordinate host and applications within a subnet (e.g., **192.168.1.0/24**)
- a **host** checkbox to select all subordinate applications within a host (e.g., **192.168.1.23 testing**)
- an individual **application** beneath a parent host (e.g., **Microsoft SQL Server 2000**).

Hint: Click the **+** icons to display subordinate subnets and applications.

5. Click the **Add** button to close the **Application Picker**. Your selected networks, subnets, hosts, and applications display in the **Pen Test Template Editor** dialog box.

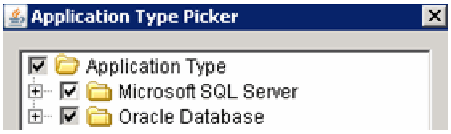


Include	IP Address	Hostname	Type	App Type	Port	Instance
Include	192.168.1.14	bigjoe.nycapt35k....	App	Microsoft SQL S...	1185	SQL2005
Include	192.168.1.0	N/A	Subnet	Edit Filter	N/A	N/A

FIGURE: Selected networks, subnets, hosts, and applications in the **Pen Test Template Editor** dialog box

For each application you selected with the **Application Picker**, the following fields display:

- The **Include** drop-down, which allows you to select whether to **Include** or **Exclude** the application in your Penetration Test Job. (**Include** selected by default.)
- The **IP Address** of your selected application (if applicable).
- The **Hostname** of your selected application (if applicable).
- The **Type** of application you selected with the **Application Picker**, i.e., **App**, **Subnet**, **Host**, **Network**.
- The **Add Filter** button under the **App Type** column, which you can click to display the **Application Type Picker** pop up (shown below).



Application Type Picker

☑ Application Type
⊞ ☑ Microsoft SQL Server
⊞ ☑ Oracle Database

FIGURE: Application Type Picker

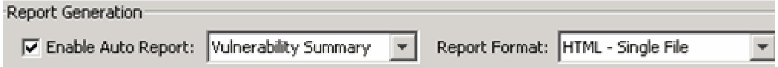
The **Application Type Picker** pop up allows you to filter which application types you want to filter from Penetration Testing at the network, subnet, or host level. (Does **not** apply at the application level.)

For example, if you used the **Application Picker** in Step 4 to select the subnet **192.168.1.1/50**, and you want to exclude all Auditing of Oracle Database applications, then you can uncheck the **Oracle Database** checkbox in the **Application Picker** to filter Penetration Testing of Oracle in this particular Penetration Test Job.

- The **Port** number of your selected application (if applicable)
- The **Instance** name of your selected application (if applicable).

6. Auto-generate a Report upon completion of your Penetration Test Job.

The **Report Generation** portion of the **Pen Test Template Editor** dialog box allows you to automatically generate a **Vulnerability Details** or **Vulnerability Summary** Report upon completion of your Penetration Test Job. For more information on Report types, see *Report types*.



Report Generation

☑ Enable Auto Report: Vulnerability Summary Report Format: HTML - Single File

FIGURE: **Report Generation** section of the **Pen Test Template Editor** dialog box

If you want to use the Report auto-generation feature, do the following:

- Check the **Enable Auto Report** checkbox in the **Report Generation** portion of the **Pen Test Template Editor** dialog box. The **Job History** portion of the pane displays the status of your auto Report Job after your Penetration Test Job completes. The format that displays is: `"for JOB_TYPE JOB_NAME [ran at 11/29/2007 12:23:20]"`.
- Use the Report type drop-down to select whether you want to auto-generate a **Vulnerability Details** or **Vulnerability Summary** Report upon completion of your Penetration Test Job; for more information on Report types, see *Report types*.
- Use the **Report Format** drop-down to select whether you want to auto-generate your Report in any of the following formats:

  -HTML - Single File

  -Text

  -XML

  -PDF.

For more information on Report formats, see *Report formats*.

If you use the Report auto-generation feature to generate a Report for a Penetration Test Job, you can:

- view the completed Report (when the Job is complete) in whatever format you specified in this step; for more information, see *Viewing a completed Report*
- save the completed Report (when the Job is complete) in whatever format you specified in this step; for more information, see *Saving a completed Report*.

7. Click the **Save** button to save your Penetration Test Job.

8. You can:

- run the Penetration Test Job now; for more information, see *"Run Job Now"*
- schedule the Penetration Test Job to run later; for more information, see *Scheduling a Job*.

9. After your Penetration Test Job completes, you can:

- view the completed Job details; for more information, see *Viewing Job details*
- view the completed Job properties; for more information, see *Viewing the properties of a completed Job*.

Audit Jobs

This topic consists of the following sub-topics:

- *What is an Audit?*
- *Manually Adding Oracle SIDs and DB2 Databases to Discover (Pre-Audit)*
- *Windows OS Audit Check Requirements*
- *UNIX OS Audit Check Requirements*
- *IBM DB2 z/OS Considerations*
- *Running an Audit Using Currently Logged-On Windows User Credentials (Instead of Oracle Database User Credentials)*
- *DISA Check Requirements*
- *Required Open Ports on Machines Running Microsoft SQL Server*
- *Auditing Multiple Database Instances on a Single Host*
- *Important Pre-Audit Security Consideration*
- *Auditing Microsoft SQL Server (Using Windows Authentication) Against a Machine on a Different or Untrusted Domain*
- *Creating an Audit Job.*

WHAT IS AN AUDIT?

An **Audit** tests the security of your application using an "inside out" approach. Audits require that you already have access to a system, such as Oracle. In accordance with your associated Policies, an Audit checks your Discovered applications for password configurations, table access, User roles, and other vulnerabilities.

Note: In order to Audit DB2, Sybase, or Lotus Notes/Domino applications, you **must** have a working client installed. For more information, see the *DbProtect Installation Guide*.

MANUALLY ADDING ORACLE SIDS AND DB2 DATABASES TO DISCOVER (PRE-AUDIT)

When you run an Oracle Discovery, DbProtect only detects the Oracle Listener (unless you specified a listener password during Scan Engine installation; for more information, see the *DbProtect Installation Guide*). In order to run an Audit (or a Penetration Test) on a Discovered Oracle database, the Oracle SID **must** display in the **Dashboard**. Therefore, in most cases, you must manually add the Oracle SID to the **Dashboard** before you run an Audit (or a Penetration Test).

The same is true for running an Audit (or a Penetration Test) Jobs on DB2. When you run a DB2 Discovery, DbProtect only detects the DB2 instance. In order to run an Audit (or a Penetration Test) Job against a Discovered DB2 database, the DB2 database **must** display in the **Dashboard**. Again, in most cases, you must manually add the DB2 database to the **Dashboard** before you run an Audit (or a Penetration Test).

For more information on:

- running a Discovery Job, see *Discovery Jobs*
- running a Penetration Test Job, see *Penetration Test Jobs*
- manually adding an application to Discover, see *Adding an application to Discover*.

WINDOWS OS AUDIT CHECK REQUIREMENTS

DbProtect Vulnerability Management performs Windows OS checks via Windows authentication. Make sure the `DbProtect Scan Engine` service where you are running DbProtect Vulnerability Management has the appropriate permissions for the following checks:

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

The Scan Engine uses the credentials it is running as to run these checks. For more information on:

- services, see the *DbProtect Administrator's Guide*
- Scan Engines, see *Working with Scan Engines*.

UNIX OS AUDIT CHECK REQUIREMENTS

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

If you run the following checks:	Then you must have permission to:
Permissions on Files	List files in the installation directories of the database.
Setgid Bit Enabled	
Setuid Bit Enabled	

Properly-Configured Environment Variables

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

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

IBM DB2 Z/OS CONSIDERATIONS

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

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

For more information, see *Configuring the properties of a Scan Engine*.

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

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

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

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

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

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

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

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

DISA CHECK REQUIREMENTS

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

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

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

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

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

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

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

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

For more information, see Step 7 of *Creating an Audit Job*.

REQUIRED OPEN PORTS ON MACHINES RUNNING MICROSOFT SQL SERVER

In order to run an Audit against a Microsoft SQL Server database, certain ports on the machine running Microsoft SQL Server **must** be open. For more information, see *Appendix L: Open Ports (on Computers Running Microsoft SQL Server) Required to Run Discoveries, Pen Tests, and Audits*.

AUDITING MULTIPLE DATABASE INSTANCES ON A SINGLE HOST

If you have multiple database instances installed on a single host, and you want to Audit them all, you can enter separate credentials for each instance. However, you can only enter a single (per Scan Engine) global listener password in order to Discover Oracle database instances.

DB2 Admin Client Considerations:

If you install the DB2 Admin Client *after* you already have the Scan Engine installed and running, you **must** re-start the Scan Engine service to perform an Audit against a DB2 application.

IMPORTANT PRE-AUDIT SECURITY CONSIDERATION

DbProtect requires database and operating system (OS) credentials to be stored in DbProtect to successfully perform Audits. When using SSH for OS connections, a private key and passphrase is stored within DbProtect and passed on to the Scan Engine for performing the actual Audit. The private key and the passphrase are encrypted and stored in the Data Repository.

You can remove the private key and passphrase; for more information, see Step 2 of *Setting your operating system credentials (for Unix-based operating systems)*.

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

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

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

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

1. Establish a connection to the target server.

Enter the appropriate Net Use syntax. For a remote host that is a:

- member of domain, enter: `net use \\ip /user:domain\username`
- workgroup member (standalone computer), enter: `net use \\ip /user:username` or `net use \\ip /user:computername\username`

2. Use named pipes to connect to an untrusted domain.

Select the **Properties** branch option **Connect to Microsoft SQL Servers via Named Pipes**. You must check this option when Auditing a Microsoft SQL Server database in an untrusted domain. For more information on:

- displaying the **Properties** branch, see *Displaying the Properties branches*
- the **Properties** branch options, see *Understanding the Properties branches*.

Important: You **must** enable the named pipes protocol on *both* the DbProtect host and the Microsoft SQL Server target server when using this option.

Note: DbProtect does **not** support Pen Testing any Microsoft SQL Server instances which use named pipes for connection.

3. Make sure of the following:
    - That the `Server` and `Remote Registry` services on your remote host are running
    - That the Net Use set of credentials file being used is a member of either the domain hosting the target server, or a domain that is trusted by that domain
    - the login provides remote registry access and read-only file access to the remote machine. To check this, do the following:
    - enter `net use \\server` with your credentials, and expand `HKEY_LOCAL_MACHINE` on the target server
    - enter `net use \\server\c$` to verify you can access files on the target server.
    - That access to the remote host can be restricted by firewall, which is common on Windows 2003/XP/Vista. You can verify this on the remote host by looking into the firewall settings/logs for rejects packets. This means there should be connectivity on port 445 or 139 on the target host.
4. Do the following to create and test a DSN connection to the target host:
    - Choose **Control Panel > Administrative Tools > Data Sources (ODBC)**.
    - Open the **System DSN** tab and click the **Add** button.
    - Choose **Microsoft SQL Server** from the list.
    - Click the **Finish** button.
    - Enter a **Name** and **Description** for this data source entry.
    - In the **Server** field, enter the IP address and listening port of the target server, e.g., `172.27.190.58,1756`.
    - Click the **Next** button.
    - Select **SQL Server Authentication** and enter your database credentials in the **Login ID** and **Password** fields.
    - Click the **Next** button.
    - Follow the steps in the wizard.

You should be able to test the connection to the data source. If this test is successful, you should also be able to perform the Audit with DbProtect. If you are unable to connect, try using the other IP address, or use Windows Authentication rather than the SQL credentials (after connecting with Net Use).

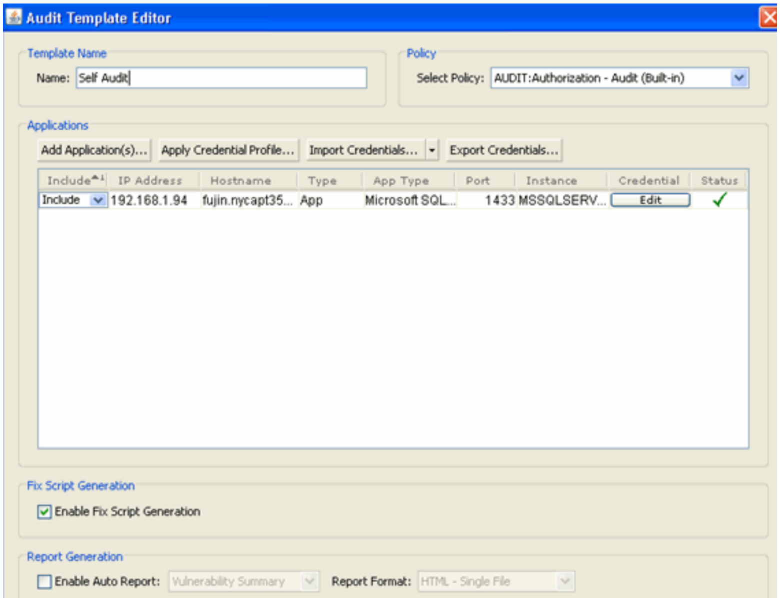
CREATING AN AUDIT JOB

Note: DbProtect requires database and operating system (OS) credentials to be stored in DbProtect to successfully perform Audits. When using SSH for OS connections, a **private key and passphrase** is stored within DbProtect and passed on to the Scan Engine for performing the actual Audit. The private key and the passphrase are encrypted and stored in the Data Repository. **You can remove the private key and passphrase**; for more information, see Step 2 of *Setting your operating system credentials (for Unix-based operating systems).*

You can set your database and operation system authentication credentials manually (see Step 7), apply a Credential Profile (see Step 8), or import credentials from a properly-formatted User Credentials File (see Step 9). For more information on Credential Profiles and User Credentials Files, see *Working with Credential Profiles and User Credential Files.*

To create an Audit Job:

1. Do one of the following to display the **Audit Template Editor** dialog box:
   - Choose **Jobs** > **Templates** > **New Audit** from the menu.
   - Click the **Manage Jobs** tab, and choose **New Job > New Audit** in the **Job Setup Options** Toolbar on the **Manage Jobs** page; for more information, see *Toolbars*.



Name: Self Audit

Select Policy: AUDIT:Authorization - Audit (Built-in)

Include	IP Address	Hostname	Type	App Type	Port	Instance	Credential	Status
Include	192.168.1.94	fujin.nycapt35...	App	Microsoft SQL...	1433	MSSQLSERV...	Edit	✓

☑ Enable Fix Script Generation

☐ Enable Auto Report: Vulnerability Summary Report Format: HTML - Single File

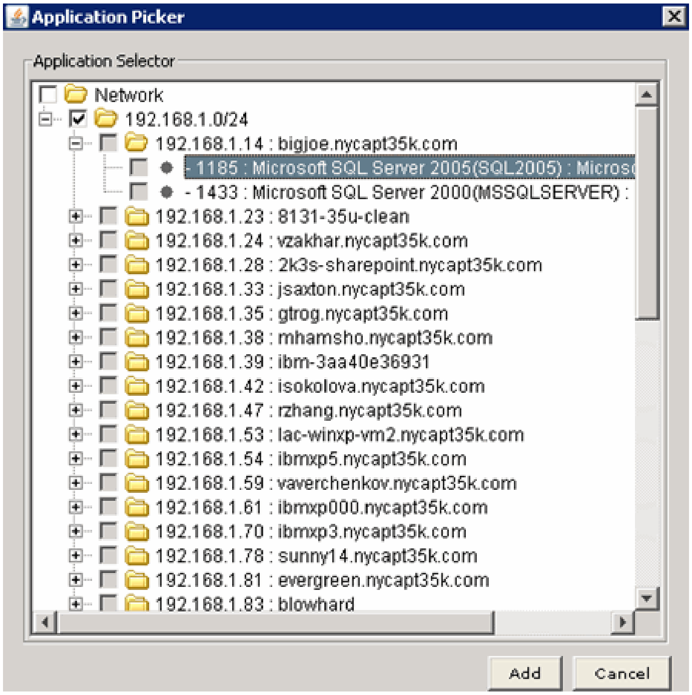
FIGURE: **Audit Template Editor** dialog box

2. In the **Template Name** portion of the **Audit Template Editor** dialog box, enter the name of your new Audit Job in the **Name:** field.

3. In the **Policy** portion of the **Audit Template Editor** dialog box, use the **Select Policy:** drop-down to select your Audit Policy.

4. Pick applications to Audit.

Click the **Add Application(s)...** button in the **Audit Template Editor** dialog box to display the **Application Picker**, which allows you to select which applications you want to Audit.



□ Network
☑ 192.168.1.0/24
□ 192.168.1.14 : bigjoe.nycapt35k.com
□ ● - 1185 : Microsoft SQL Server 2005(SQL2005) : Micros
□ ● - 1433 : Microsoft SQL Server 2000(MSSQLSERVER) :
□ 192.168.1.23 : 8131-35u-clean
□ 192.168.1.24 : vzakhar.nycapt35k.com
□ 192.168.1.28 : 2k3s-sharepoint.nycapt35k.com
□ 192.168.1.33 : jsaxton.nycapt35k.com
□ 192.168.1.35 : gtrog.nycapt35k.com
□ 192.168.1.38 : mhamsho.nycapt35k.com
□ 192.168.1.39 : ibm-3aa40e36931
□ 192.168.1.42 : isokolova.nycapt35k.com
□ 192.168.1.47 : rzhang.nycapt35k.com
□ 192.168.1.53 : lac-winxp-vm2.nycapt35k.com
□ 192.168.1.54 : ibmxp5.nycapt35k.com
□ 192.168.1.59 : vaverchenkov.nycapt35k.com
□ 192.168.1.61 : ibmxp000.nycapt35k.com
□ 192.168.1.70 : ibmxp3.nycapt35k.com
□ 192.168.1.78 : sunny14.nycapt35k.com
□ 192.168.1.81 : evergreen.nycapt35k.com
□ 192.168.1.83 : blowhard

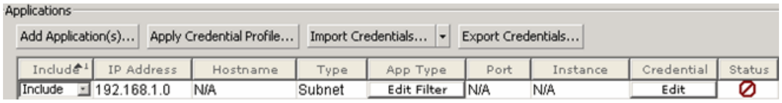
FIGURE: Application Picker

You can check:

- the **Network** checkbox to select all IPs (and subordinate subnets and applications) on a network
- a **subnet** checkbox to select all subordinate host and applications within a subnet (e.g., **192.168.1.0/24**)
- a **host** checkbox to select all subordinate applications within a host (e.g., **192.168.1.23 testing**)
- an individual **application** beneath a parent host (e.g., **Microsoft SQL Server 2000**).

Hint: Click the **+** icons to display subordinate subnets and applications.

5. Click the **Add** button to close the **Application Picker**. Your selected applications display in the **Audit Template Editor** dialog box.

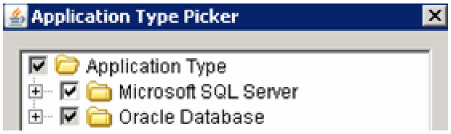


Include	IP Address	Hostname	Type	App Type	Port	Instance	Credential	Status
Include	192.168.1.0	N/A	Subnet	Edit Filter	N/A	N/A	Edit	⊘

FIGURE: Selected networks, subnets, hosts, and applications in the **Audit Template Editor** dialog box

For each application you selected with the **Application Picker**, the following fields display:

- The **Include** drop-down, which allows you to select whether to **Include** or **Exclude** the application in your Audit Job. (**Include** selected by default.)
- The **IP Address** of your selected application (if applicable).
- The **Hostname** of your selected application (if applicable).
- The **Type** of application you selected with the **Application Picker**, i.e., **App**, **Subnet**, **Host**, **Network**.
- The **Add Filter** button under the **App Type** column, which you can click to display the **Application Type Picker** pop up (shown below).



- ☑ Application Type
  - ☑ Microsoft SQL Server
  - ☑ Oracle Database

FIGURE: Application Type Picker

The **Application Type Picker** pop up allows you to filter which application types you want to filter from an Audit at the network, subnet, or host level. (Does **not** apply at the application level.)

For example, if you used the **Application Picker** in Step 4 to select the subnet **192.168.1.1/50**, and you want to exclude all Auditing of Oracle Database applications, then you can uncheck the **Oracle Database** checkbox in the **Application Picker** to filter Auditing of Oracle in this particular Audit Job.

- The **Port** number of your selected application (if applicable)
- The **Instance** name of your selected application (if applicable)
- The **Edit** button under the **Credential** column, which you can click to display the **Set Credentials** dialog box, and set credentials only for this Audit Job (see Step 6). Or, you can apply a Credential Profile to this Audit Job (see Step 7).

- The icon under the **Status** column indicates whether your credentials are **incomplete** ⊘, **partial** ⚠, or **complete** ✓. If your credentials are incomplete or partial, click the **Edit** button under the **Credential** column, and set credentials only for this Audit Job (see Step 6).

6. You must provide database and operation system authentication credentials in order to run an Audit Job. If you want to:

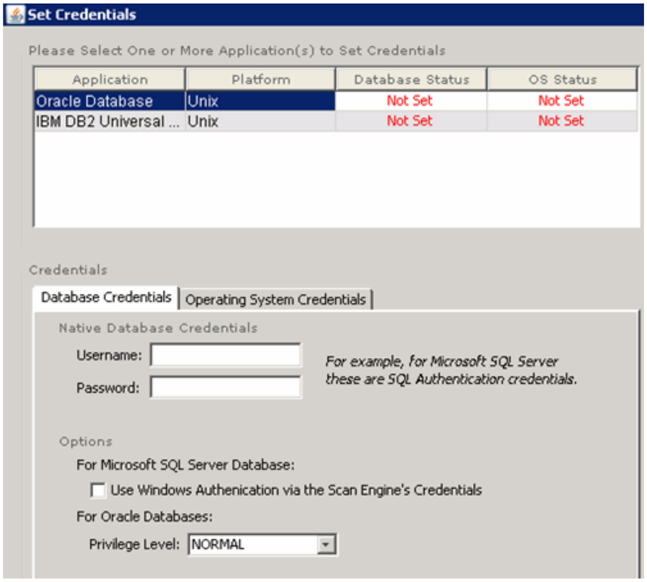
- set credentials manually, see Step 7
- apply a Credential Profile, see Step 8
- import credentials from a properly-formatted User Credentials File, see Step 9.

For more information on Credential Profiles and User Credentials Files, see *Working with Credential Profiles and User Credential Files.*

7. Set credentials manually for this Audit Job.

You can set credentials only for this Audit Job, without applying a Credential Profile. Do the following:

- Click the **Edit** button under the **Credential** column in the **Audit Template Editor** dialog box to display the **Set Credentials** dialog box.



Set Credentials

Please Select One or More Application(s) to Set Credentials

Application	Platform	Database Status	OS Status
Oracle Database	Unix	Not Set	Not Set
IBM DB2 Universal ...	Unix	Not Set	Not Set

Credentials

Database Credentials | Operating System Credentials

Native Database Credentials

Username:

Password:

For example, for Microsoft SQL Server these are SQL Authentication credentials.

Options

For Microsoft SQL Server Database:

□ Use Windows Authenication via the Scan Engine's Credentials

For Oracle Databases:

Privilege Level: NORMAL

FIGURE: **Set Credentials** dialog box

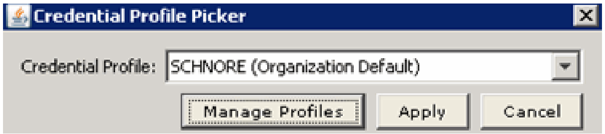
- Select an **Application/Platform** combination in the **Please Select One or More Application(s) to Set Credentials** portion of the **Set Credentials** dialog box, e.g., **Oracle Database** running on **Windows**.

  The corresponding **Database Credentials** and **Operating System Credentials** tabbed fields display in the **Credentials** portion the **Set Credentials** dialog box.
- Set your credentials, according to your selected **Application/Platform** combination. For more information, see *Setting and testing your database and operating system credentials*.

8. Apply an existing Credential Profile to this Audit Job.

You can apply an existing Credential Profile to this Audit Job. Do the following:

- Click the **Apply Credential Profile...** button in the **Audit Template Editor** dialog box to display the **Credential Profile Picker**.

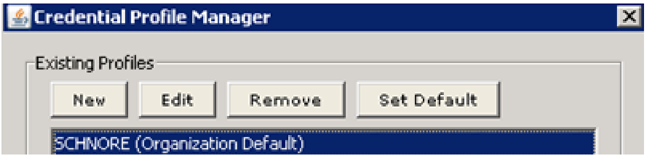


Credential Profile: SCHNORE (Organization Default)

FIGURE: Credential Profile Picker

- Use the **Credential Profile:** drop-down to select an existing Credential Profile, then click the **Apply** button.

  DbProtect Vulnerability Management applies the selected, existing Credential Profile to this Audit Job.
- Alternately, from the **Credential Profile Picker** you can click the **Manage Profiles** button to display the **Credential Profile Manager**.



SCHNORE (Organization Default)

FIGURE: Credential Profile Manager

The **Credential Profile Manager** allows you to click the:

- **New** button to create a new Credential Profile; for more information, see *Creating a Credential Profile*
- **Edit** button to edit a Credential Profile; for more information, see *Editing a Credential Profile*
- **Remove** button to remove a Credential Profile; for more information, see *Removing a Credential Profile*

- **Set Default** button to set the Credential Profile selected with the **Credential Profile:** drop-down as your Organizational default; for more information see *Setting a Credential Profile as an Organizational default*.

9. Import credentials.

All Users (except View Users) can import User Credentials from an `.xml` file. This file must be properly-formatted or the import will fail, and the credentials will remain unchanged. For more information on:

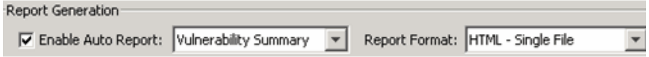
- the proper format of a User Credentials File, see *Appendix A: Creating a User Credentials File*
- importing a User Credentials File, see *Importing a User Credentials File*.

10. Export credentials (Super Users only).

Super Users can export User Credentials to an `.xml` file. For more information, see *Exporting a User Credentials File*.

11. Auto-generate a Report upon completion of your Audit Job.

The **Report Generation** portion of the **Audit Template Editor** dialog box allows you to automatically generate a **Vulnerability Details** or **Vulnerability Summary** Report upon completion of your Audit Job. For more information on Report types, see *Report types*.



Report Generation

☑ Enable Auto Report: Vulnerability Summary

Report Format: HTML - Single File

FIGURE: **Report Generation** section of the **Audit Template Editor** dialog box

If you want to use the Report auto-generation feature, do the following:

- Check the **Enable Auto Report** checkbox in the **Report Generation** portion of the **Audit Template Editor** dialog box. Check the **Enable Auto Report** checkbox in the **Report Generation** portion of the **Audit Template Editor** dialog box. The **Job History** portion of the pane displays the status of your auto Report Job after your Audit Job completes. The format that displays is: `"for JOB_TYPE JOB_NAME [ran at 11/29/2007 12:23:20]"`
- Use the Report type drop-down to select whether you want to auto-generate a **Vulnerability Details** or **Vulnerability Summary** Report upon completion of your Audit Job; for more information on Report types, see *Report types*.
- Use the **Report Format** drop-down to select whether you want to auto-generate your Report in any of the following formats:

  -HTML - Single File

  -Text

  -XML

  -PDF.

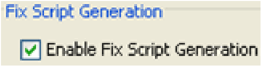
For more information on Report formats, see *Report formats*.

If you use the Report auto-generation feature to generate a Report for an Audit Job, you can:

- view the completed Report (when the Job is complete) in whatever format you specified in this step; for more information, see *Viewing a completed Report*
- save the completed Report (when the Job is complete) in whatever format you specified in this step; for more information, see *Saving a completed Report*.

12. Auto-generate Fix Scripts upon completion of your Audit Job.

The **Fix Script Generation** section of the **Audit Template Editor** dialog box allows you to check the **Enable Fix Script Generation** checkbox (unchecked by default) to automatically generate a Fix Script for all vulnerabilities detected upon completion of your Audit Job. For more information on Fix Scripts, see *Automatically running a Fix Script*.



Fix Script Generation

☑ Enable Fix Script Generation

FIGURE: **Fix Script Generation** section of the **Audit Template Editor** dialog box

13. Click the **Save** button to save your Audit Job.

14. You can:

- run the Audit Job now; for more information, see *"Run Job Now"*
- schedule the Audit Job to run later; for more information, see *Scheduling a Job*.

15. After your Audit Job completes, you can:

- view the completed Job details; for more information, see *Viewing Job details*
- view the completed Job properties; for more information, see *Viewing the properties of a completed Job*
- view individual vulnerabilities detected during an Audit of a Discovered database; for more information, see *Viewing individual vulnerabilities detected during an Audit*.

Report Jobs

This topic consists of the following sub-topics:

- *What is a Report?*
- *Understanding legacy Reports*
- *Report types*
- *Report formats*
- *Creating a Report Job*.

WHAT IS A REPORT?

DbProtect Vulnerability Management allows you to generate **Reports** designed to communicate vulnerabilities detected by DbProtect Vulnerability Management to all levels of your Organization.

Note: You can schedule a Report Job to run in the *future* (explained in this topic), or you can create a Report Job and run a Report *now*; for more information, see *"Run Job Now"*.

UNDERSTANDING LEGACY REPORTS

DbProtect allows you to run Vulnerability Management Reports as **legacy Reports** (if you selected the Legacy Vulnerability Assessment Reporting option during the installation of the DbProtect suite). A legacy Report is a Vulnerability Management Report that displays in a pre-DbProtect 2009.1R4 (i.e., legacy) format.

As explained in the *DbProtect Installation Guide*, when you first install the DbProtect suite, you have the option of adding support for Legacy VA (Vulnerability Assessment) Reporting.

If you did **not** select legacy Vulnerability Assessment reporting when you installed the DbProtect suite, then legacy Vulnerability Assessment reports are **not** available. Specifically, the **Enable Legacy Reports** checkbox will **not** display on the **New Report Template** dialog box when you create a Report Job; for more information, see *Creating a Report Job*.

On the other hand, if you selected legacy Vulnerability Assessment reporting when you installed the DbProtect suite, then legacy Vulnerability Assessment reports are available. Specifically, the **Enable Legacy Reports** checkbox displays on the **New Report Template** dialog box when you create a Report Job; for more information, see *Creating a Report Job*.

REPORT TYPES

DbProtect Vulnerability Management supports the following **Report types**:

- **Application Banners.** This type of Report displays information found within the **Details** tab of the main window.
- **Application Inventory.** Use this Report to generate a snapshot of your applications. This Report is useful in summarizing the state of your network applications.

- **Check Status.** Creates a Report of all security checks run on an application and their results. The following table explains possible **Status** field messages.

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

- **Policy Detail.** Generates a Report based on the Policy you choose.
- **Summary Report.** Displays a high-level summary of all the applications and vulnerabilities Discovered on the network or in a particular folder.
- **User Information.** Creates a Report containing a list of User logins and related information.
- **Vulnerability Differences.** Generates a Report showing the differences in vulnerabilities between two Penetration Tests or Audits of a specific application.
- **Vulnerability Details.** Creates a Report containing the *specific* vulnerability details found for each Audit and Penetration Test performed.
- **Vulnerability Summary.** Creates a Report which contains *high-level summary information* for vulnerabilities found for each Audit and Penetration Test.
- **STIG Findings by Database Overview.** This report shows a summary of STIG compliance broken down by results that pass, fail, and are not applicable (N/A) for automated verification.
- **STIG Findings by Database Mapping.** This report shows the findings summary mapped to STIG compliance.
- **STIG Findings by Database Detail.** This report shows the detailed findings mapped to STIG compliance.

Note: To run DISA-STIG compliance pack reports, you must import a compliance content pack; for more information see *Importing a Compliance Content Pack*.

You can also display generated DISA-STIG compliance pack reports (i.e., **STIG Findings by Database Overview**, **STIG Findings by Database Mapping**, and **STIG Findings by Database Detail**) -- as well as generated DISA-STIG compliance Dashboards -- on the **Compliance Packs** page; for more information, see *Interpreting Your Generated Compliance Pack Dashboards, and Displaying/Interpreting Your Generated Compliance Pack Reports*.

REPORT FORMATS

DbProtect Vulnerability Management generates Reports in the following **Report formats**:

- **HTML - Single File.** You can view an HTML Report in a web browser. DbProtect Vulnerability Management stores the Report in a directory.
- **Text.** You can view a text Report with any text or word processing program, such as Notepad or Word.
- **XML.** The "bare" XML skeleton used to generate custom Reports.
- **PDF.** You can view a PDF Report, using Acrobat Reader.

Note: You can download Acrobat Reader for free from `www.adobe.com`.

Important: In the current version of DbProtect Vulnerability Management, you can view a Report in HTML, but if you want to **save** a Report to your computer or network, then you **must** save your Report as an `.mht` file instead of `.html` or `.xml`.

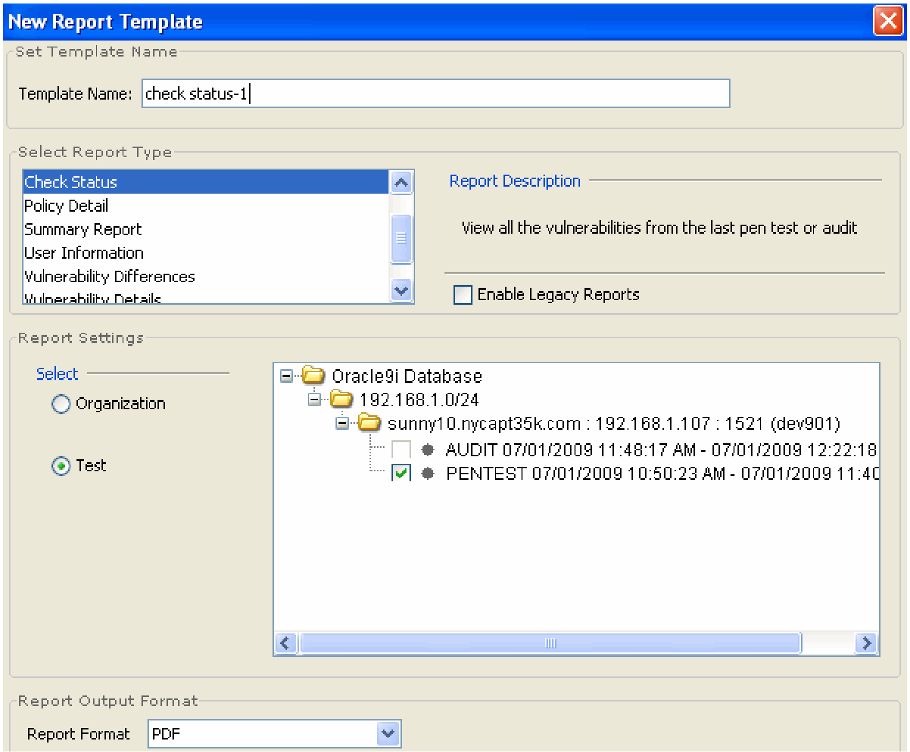
Note: You can only generate legacy Reports in XML or PDF formats; for more information, see *Report types*.

CREATING A REPORT JOB

To create a Report Job:

1. Do one of the following to display the **New Report Template** dialog box:

   - Choose **Jobs > Templates > New Report** from the menu.
   - Click the **Manage Jobs** tab, and choose **New Job > New Report** in the **Job Setup Options** Toolbar on the **Manage Jobs** page; for more information, see *Toolbars*.



New Report Template

Set Template Name

Template Name: check status-1

Select Report Type

Check Status
Policy Detail
Summary Report
User Information
Vulnerability Differences
Vulnerability Details

Report Description

View all the vulnerabilities from the last pen test or audit

□ Enable Legacy Reports

Report Settings

Select

○ Organization

● Test

Oracle9i Database
192.168.1.0/24
sunny10.nycapt35k.com : 192.168.1.107 : 1521 (dev901)
□ AUDIT 07/01/2009 11:48:17 AM - 07/01/2009 12:22:18
☑ PENTEST 07/01/2009 10:50:23 AM - 07/01/2009 11:40

Report Output Format

Report Format PDF

FIGURE: **New Report Template** dialog box

2. In the **Template:** portion of the **New Report Template** dialog box, enter the name of your new Report Job in the **Template Name:** field.
3. In the **Select Report Type** portion of the **New Report Template** dialog box, highlight the Report you want to associate with this Job.
4. A **Report description** displays to the right, and corresponding setting options display in the **Report Settings** portion of the dialog box (see Step 5). For more information, see *Report types*.

Note: As explained in *Understanding legacy Reports*, DbProtect allows you to run Vulnerability Management Reports as legacy Reports (if you selected the Legacy Vulnerability Assessment Reporting option during the installation of the DbProtect suite). A legacy Report is a Vulnerability Management Report that displays in a pre-DbProtect 2009.1R4 (i.e., legacy) format.

When you first install the DbProtect suite, you have the option of adding support for Legacy VA (Vulnerability Assessment) Reporting. If you did **not** select legacy Vulnerability Assessment reporting when you installed the DbProtect suite, then legacy Vulnerability Assessment reports are **not** available. Specifically, the **Enable Legacy Reports** checkbox will **not** display on the **New Report Template** dialog box. On the other hand, if you selected legacy Vulnerability Assessment reporting when you installed the DbProtect suite, then legacy Vulnerability Assessment reports are available. Specifically, the **Enable Legacy Reports** checkbox displays on the **New Report Template** dialog box.

5. The **Report Settings** portion of the dialog box allows you specify your Report-specific criteria, i.e., a Policy name for a **Policy Report**, a Penetration Test for a **Vulnerability Report**, etc. This portion of the dialog box is different for each Report.
6. In the **Report Output Format** portion of the **New Report Template** dialog box, use the **Report Format** drop-down to choose whether you want to generate your Report as:
   - **HTML - Single File**
   - **Text**
   - **XML**
   - **PDF**.

Important: In the current version of DbProtect, you can view a Report in HTML, but if you want to **save** a Report to your computer or network, then you **must** save your Report as an `.mht` file instead of `.html` or `.xml`.

For more information, see *Report formats*.

7. Click the **Save** button to save your Report Job.

8. You can:

   - run the Report Job now; for more information, see *"Run Job Now"*
   - schedule the Report Job to run later; for more information, see *Scheduling a Job*.

9. After your Report Job completes, you can:

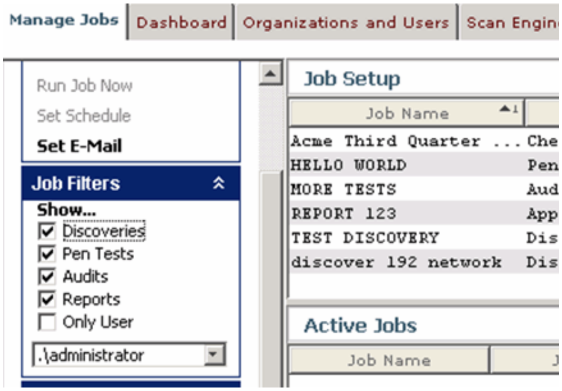
   - view the completed Report Job (in whatever format you specified in Step 5); for more information, see *Viewing a completed Report*
   - save the completed Report Job (in whatever format you specified in Step 5); for more information, see *Saving a completed Report*
   - view the completed Job details; for more information, see *Viewing Job details*
   - view the completed Job properties; for more information, see *Viewing the properties of a completed Job*.

Editing a Job

To edit a Job:

1. Do one of the following to display the **Manage Jobs** page:

   - Choose **Jobs** > **Manage** from the menu.
   - Click the **Manage Jobs** tab.



☑ Discoveries
☑ Pen Tests
☑ Audits
☑ Reports
☐ Only User
.\administrator

Job Name	
Acme Third Quarter ...	Che
HELLO WORLD	Pen
MORE TESTS	Aud
REPORT 123	App
TEST DISCOVERY	Dis
discover 192 network	Dis

FIGURE: **Manage Jobs** page

2. Do one of the following:

- Right click the Job in the pane of the **Manage Jobs** page (**Job Setup** portion) and choose **Edit**.
- Double click the Job in the pane of the **Manage Jobs** page (**Job Setup** portion).

Depending what type of Job you select (i.e., Discovery, Penetration Test, Audit, or Report), the appropriate template dialog box displays. For example, if you select a Discovery Job to edit, then the **Discovery Job Template** dialog box displays. If you choose an Audit Job, the **Audit Template Editor** dialog box displays. And so on.

For more information, see:

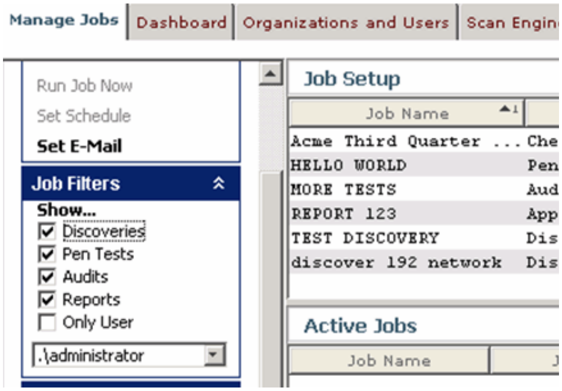
- *Discovery Jobs*
- *Penetration Test Jobs*
- *Audit Jobs*
- *Report Jobs.*

"Run Job Now"

To run a Job now:

1. Do one of the following to display the **Manage Jobs** page:

- Choose **Jobs** > **Manage** from the menu.
- Click the **Manage Jobs** tab.



Show...
☑ Discoveries
☑ Pen Tests
☑ Audits
☑ Reports
□ Only User
.\administrator

Job Setup

Job Name	
Acme Third Quarter ...	Che
HELLO WORLD	Pen
MORE TESTS	Aud
REPORT 123	App
TEST DISCOVERY	Dis
discover 192 network	Dis

Active Jobs

Job Name	J

FIGURE: **Manage Jobs** page

2. Highlight one more Jobs in the pane of the **Manage Jobs** page (**Job Setup** portion).

Hint: Click <CTRL> to highlight non-sequential Jobs.

3. Do one of the following:

- Click **Run Job Now** in the **Job Setup Options** Toolbar
- Right click the Job in the pane of the **Manage Jobs** page (**Job Setup** portion) and choose **Run Job Now**.

The Job runs, and displays in the pane of the **Manage Jobs** page (**Active Jobs** portion).

Even as the Job is running, you can:

- view the active Job details; for more information, see *Viewing Job details*
- cancel the active Job; for more information, see *Cancelling an active Job*.

Scheduling a Job

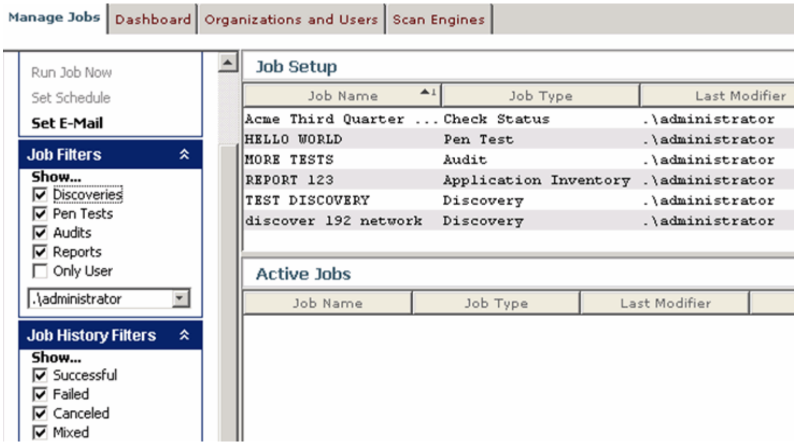
When you schedule a Job, you specify the following:

- **Job Frequency**, i.e., how often the Job should run (i.e., **Daily**, **Weekly**, **Monthly**, **Yearly**, or **Once**)
- **Date Settings**, i.e., when the Job should run (i.e., on specific date, day of the week, time, etc.).

To schedule a Job:

1. Do one of the following to display the **Manage Jobs** page:

- Choose **Jobs > Manage** from the menu.
- Click the **Manage Jobs** tab.



Job Setup

Job Name	Job Type	Last Modifier
Acme Third Quarter ...	Check Status	.\administrator
HELLO WORLD	Pen Test	.\administrator
MORE TESTS	Audit	.\administrator
REPORT 123	Application Inventory	.\administrator
TEST DISCOVERY	Discovery	.\administrator
discover 192 network	Discovery	.\administrator

Active Jobs

Job Name	Job Type	Last Modifier

Job Filters
Show...
☑ Discoveries
☑ Pen Tests
☑ Audits
☑ Reports
☐ Only User
.\administrator

Job History Filters
Show...
☑ Successful
☑ Failed
☑ Canceled
☑ Mixed

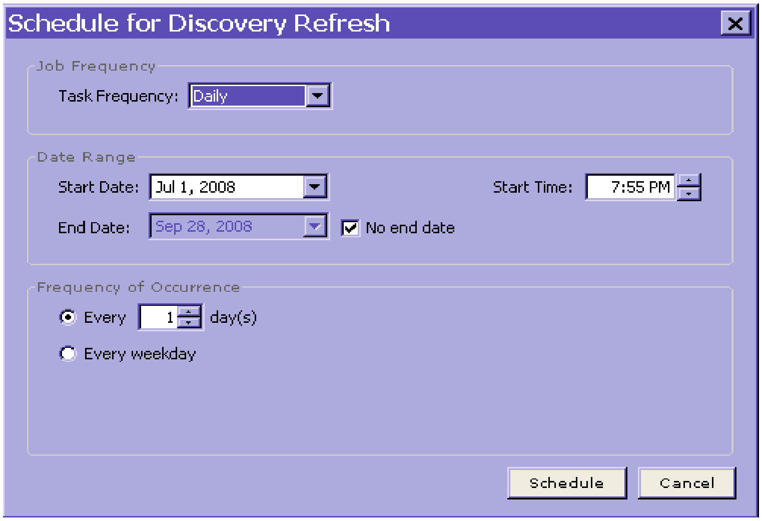
FIGURE: **Manage Jobs** page

2. Highlight one more Jobs in the pane of the **Manage Jobs** page (**Job Setup** portion).

Hint: Click <CTRL> to highlight non-sequential Jobs.

3. Do one of the following to display the **Schedule Job** dialog box:

- Click **Set Schedule** in the **Job Setup Options** Toolbar
- Right click the Job and choose **Set Schedule**.



Task Frequency: Daily

Start Date: Jul 1, 2008

Start Time: 7:55 PM

End Date: Sep 28, 2008

☑ No end date

● Every 1 day(s)

○ Every weekday

FIGURE: **Schedule Job** dialog box

Note: If you are re-scheduling a previously-scheduled Job, the Schedule Job dialog box displays the existing schedule information (which you can modify).

4. Select Job frequency.

In the **Job Frequency** portion of the **Schedule Jobs** dialog box, use the **Task Frequency:** drop-down to select how often you want the Job to run.

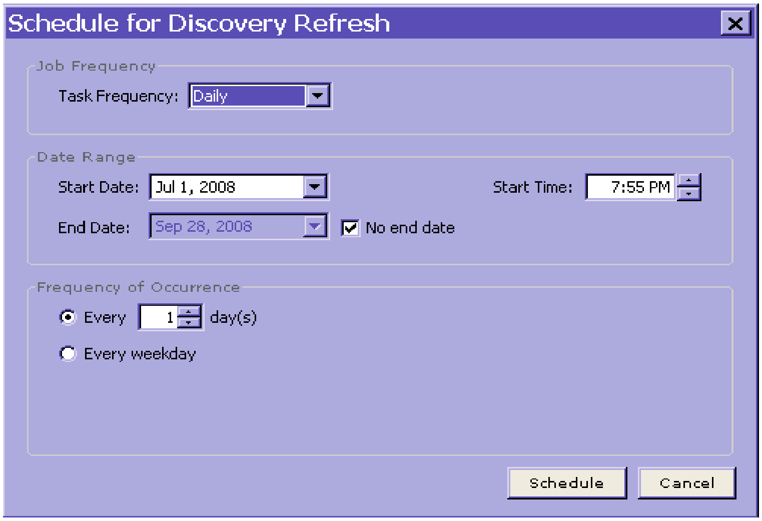
Note: The fields that display in the **Date Settings** portion of the **Schedule Jobs** dialog box vary depending on your selection.

If you select:

- **Daily**, then go to Step 5
- **Weekly**, then go to Step 6
- **Monthly**, then go to Step 7
- **Yearly**, then go to Step 8
- **Once**, then go to Step 9.

5. Scheduling a daily Job.

If you selected a Job frequency of **Daily** in Step 4, then the **Schedule Jobs** dialog box looks like this:



Schedule for Discovery Refresh

Job Frequency

Task Frequency: Daily

Date Range

Start Date: Jul 1, 2008

Start Time: 7:55 PM

End Date: Sep 28, 2008

☑ No end date

Frequency of Occurrence

● Every 1 day(s)

○ Every weekday

FIGURE: **Schedule Jobs** dialog box (**Daily** Job frequency selected)

In the **Date Settings** portion of the **Schedule Jobs** dialog box:

- Use the **Start Date:** and **End Date:** drop-downs to specify when the scheduled Job should begin and end.

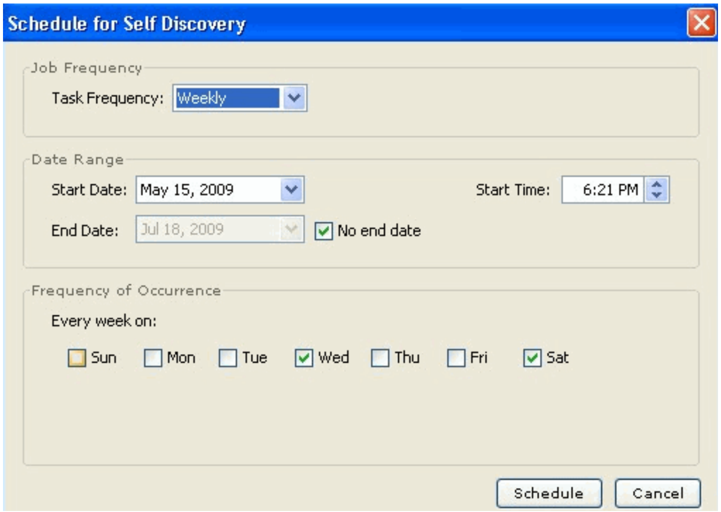
Hint: Check the **No end date** checkbox (checked by default) if you do **not** want to specify an end date for this scheduled Job. Uncheck the **No end date** checkbox if you want to specify an **End Date:** for this scheduled Job.

- Use the **Start Time:** scroll bar to specify (in **HH:MM:SS** format) when the scheduled Job should run. Use the up and down arrow keys to advance and back up the time.
- Select **Every _ Day(s)**, and use the up and down arrow keys to specify how many days a week the daily Job should run. If you select the default **1**, then DbProtect Vulnerability Management runs your daily Job every day (within the specified start and end dates). If you select **2**, then DbProtect Vulnerability Management runs your daily Job every other day (within the specified start and end dates). And so on.
- Select **Every weekday** if you want DbProtect Vulnerability Management to run your daily Job every weekday (within the specified start and end dates).

When you're done, go to Step 10.

6. Scheduling a weekly Job.

If you selected a Job frequency of **Weekly** in Step 4, then the **Schedule Jobs** dialog box looks like this:



Schedule for Self Discovery

Job Frequency

Task Frequency: Weekly

Date Range

Start Date: May 15, 2009

Start Time: 6:21 PM

End Date: Jul 18, 2009 ☑ No end date

Frequency of Occurrence

Every week on:

□ Sun □ Mon □ Tue ☑ Wed □ Thu □ Fri ☑ Sat

FIGURE: **Schedule Jobs** dialog box (**Weekly** Job frequency selected)

In the **Date Range** portion of the **Schedule Jobs** dialog box:

- Use the **Start Date:** and **End Date:** drop-downs to specify when the scheduled Job should begin and end.

Hint: Check the **No end date** checkbox if you do not want to specify an end date for this scheduled Job.

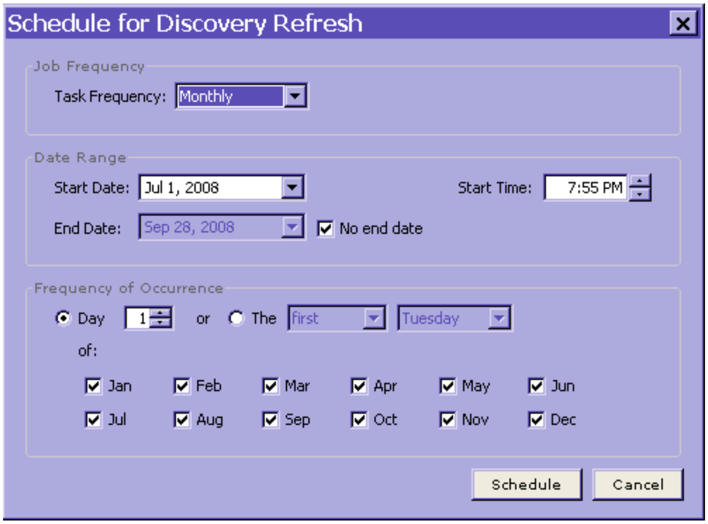
- Use the **Start Time:** scroll bar to specify (in **HH:MM:SS** format) when the scheduled Job should run. Use the up and down arrow keys to advance and back up the time.

In the **Frequency of Occurrence** portion of the **Schedule Jobs** dialog box, use the checkboxes to specify on which day(s) you want to run a weekly Job on a specific day (within the specified date range). For example, check the **Monday** checkbox to run your weekly Job every Monday (within the specified date range).

When you're done, go to Step 10.

7. Scheduling a monthly Job.

If you selected a Job frequency of **Monthly** in Step 4, then the **Schedule Jobs** dialog box looks like this:



Schedule for Discovery Refresh

Job Frequency

Task Frequency: Monthly

Date Range

Start Date: Jul 1, 2008 Start Time: 7:55 PM

End Date: Sep 28, 2008 ☑ No end date

Frequency of Occurrence

● Day 1 or ○ The first Tuesday

of:

☑ Jan ☑ Feb ☑ Mar ☑ Apr ☑ May ☑ Jun

☑ Jul ☑ Aug ☑ Sep ☑ Oct ☑ Nov ☑ Dec

FIGURE: **Schedule Jobs** dialog box (**Monthly** Job frequency selected)

In the **Date Settings** portion of the **Schedule Jobs** dialog box:

- Use the **Start Date:** and **End Date:** drop-downs to specify when the scheduled Job should begin and end.

Hint: Check the **No end date** checkbox if you do not want to specify an end date for this scheduled Job.

- Use the **Start Time:** scroll bar to specify (in **HH:MM:SS** format) when the scheduled Job should run. Use the up and down arrow keys to advance and back up the time.

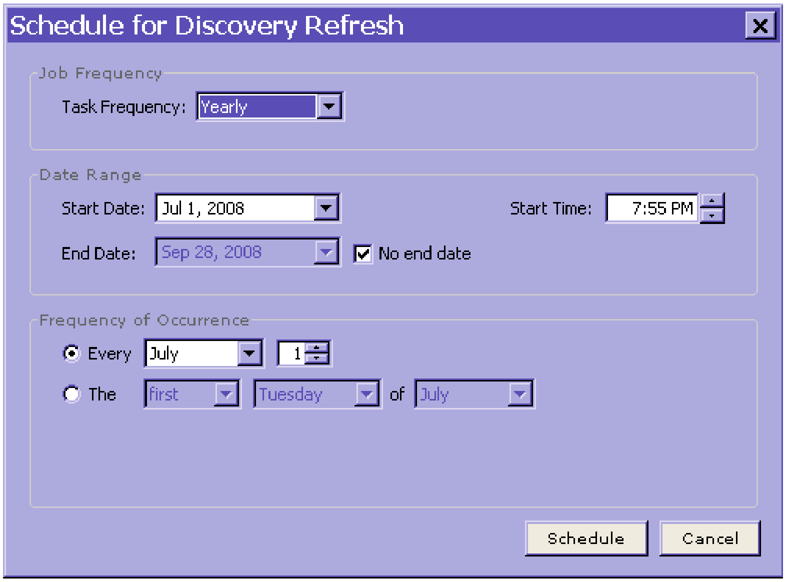
In the **Frequency of Occurrence** portion of the **Schedule Jobs** dialog box:

- Select **Day _ of every _ Month(s)** if you want to run your monthly Job on a specific date each month (within the specified date range). For example, assume You want to run a monthly Job on the 15th of every month for three months within the specified date range. Enter `15` in the date field, then use the up and down arrow keys to select **3**.
- Select **The _ _ of every _ Month(s)** if you want to run your monthly Job on a specific day of the week each month. For example, assume you want to run a monthly Job on the first Monday of every month for three months within the specified date range. Select **first**, select **Monday**, and use the up and down arrow keys to select **3**.

When you're done, go to Step 10.

8. Scheduling a yearly Job.

If you selected a Job frequency of **Yearly** in Step 4, then the **Schedule Jobs** dialog box looks like this:



Schedule for Discovery Refresh

Job Frequency

Task Frequency: Yearly

Date Range

Start Date: Jul 1, 2008

Start Time: 7:55 PM

End Date: Sep 28, 2008 ☑ No end date

Frequency of Occurrence

● Every July 1

○ The first Tuesday of July

FIGURE: **Schedule Jobs** dialog box (**Yearly** Job frequency selected)

In the **Date Settings** portion of the **Schedule Jobs** dialog box:

- Use the **Start Date:** and **End Date:** drop-downs to specify when the scheduled Job should begin and end.

Hint: Check the **No end date** checkbox if you do not want to specify an end date for this scheduled Job.

- Use the **Start Time:** scroll bar to specify (in **HH:MM:SS** format) when the scheduled Job should run. Use the up and down arrow keys to advance and back up the time.

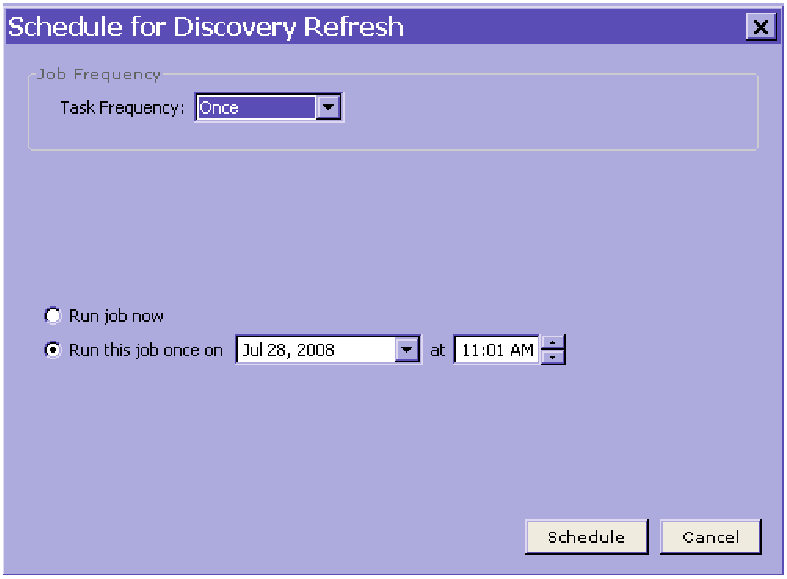
In the **Frequency of Occurrence** portion of the **Schedule Jobs** dialog box:

- Select **Every** _ if you want to run your yearly Job on a specific date each year (within the specified date range). For example, assume you want to run a yearly Job on June 16 every year within the specified date range. Select **June**, and enter `16`.
- Select **The** _ _ **of** _ if you want to run your yearly Job on a specific day of the week, during a specific month, each year. For example, assume you want to run a yearly Job on the first Monday of every June every year within the specified date range. Select **first**, select **Monday**, and select **June**.

When you're done, go to Step 10.

9. Scheduling a one-time Job.

If you selected a Job frequency of **Once** in Step 4, then the **Schedule Jobs** dialog box looks like this:



Schedule for Discovery Refresh

Job Frequency

Task Frequency: Once

○ Run job now

● Run this job once on Jul 28, 2008 at 11:01 AM

FIGURE: **Schedule Jobs** dialog box (**Once** Job frequency selected)

In the **Date Settings** portion of the **Schedule Jobs** dialog box:

- Select **Run job now** to run your Job immediately.
- Select **Run this job once on _ at _** if you want to run your Job once, on a specific date and at a specific time. For example, assume you want to run your Job once on June 16, 2008 at 4:29 P.M. Select **June 16, 2008**, then use the up and down arrow keys to select **4:29 P.M.**

When you're done, go to Step 10.

10. Click the **Schedule** button.

DbProtect Vulnerability Management schedules your Job according to the criteria specified.

Even as the Job is running, you can:

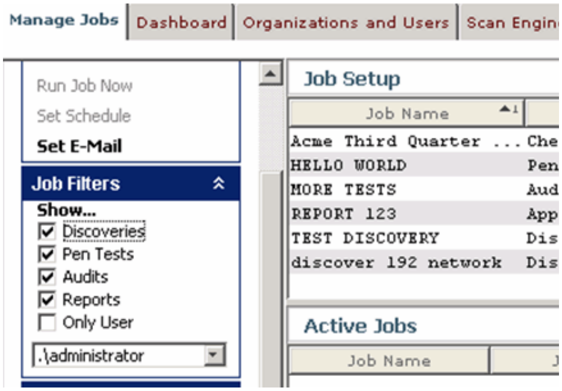
- view the active Job details; for more information, see *Viewing Job details*
- cancel the active Job; for more information, see *Cancelling an active Job*.

Unscheduling a Job

Note: Deleting an application also deletes the application from any unscheduled Job (as explained in *Deleting an application to Discover*).

To unschedule a Job:

1. Do one of the following to display the **Manage Jobs** page:
   - Choose **Jobs** > **Manage** from the menu.
   - Click the **Manage Jobs** tab.



☑ Discoveries
☑ Pen Tests
☑ Audits
☑ Reports
□ Only User

.\administrator

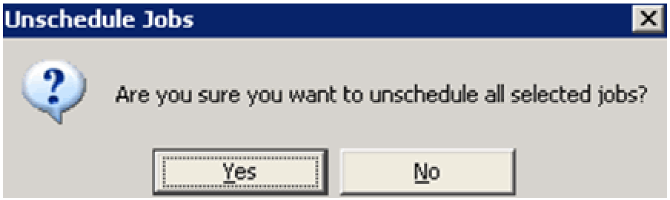
Job Name	
Acme Third Quarter ...	Che
HELLO WORLD	Pen
MORE TESTS	Aud
REPORT 123	App
TEST DISCOVERY	Dis
discover 192 network	Dis

FIGURE: **Manage Jobs** page

2. Highlight one more Jobs in the pane of the **Manage Jobs** page (**Job Setup** portion).

Hint: Click <CTRL> to highlight non-sequential Jobs.

3. Do one of the following to display the **Unschedule Jobs** pop up.
   - Click **Un-Schedule** in the **Job Setup Options** Toolbar
   - Right click the Job and choose **Un-Schedule**.



Are you sure you want to unschedule all selected jobs?

FIGURE: **Unschedule Jobs** pop up

The **Unschedule Jobs** pop up prompts you to confirm you want to unschedule the selected Jobs. Click the **Yes** button to unschedule (but not delete) the selected Jobs.

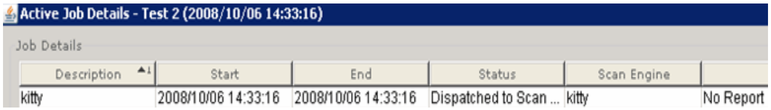
Viewing a completed Report

You can **view** a completed Report for any type of Job. For more information on using the Report auto-generation feature to generate a Report for a:

- Discovery Job, see *Discovery Jobs*
- Penetration Test Job, see *Penetration Test Jobs*
- Audit Job, see *Audit Jobs*.

To view a completed Report:

1. Locate your completed Jobs. They display in the pane of the **Manage Jobs** page (**Job History** portion).



Active Job Details - Test 2 (2008/10/06 14:33:16)

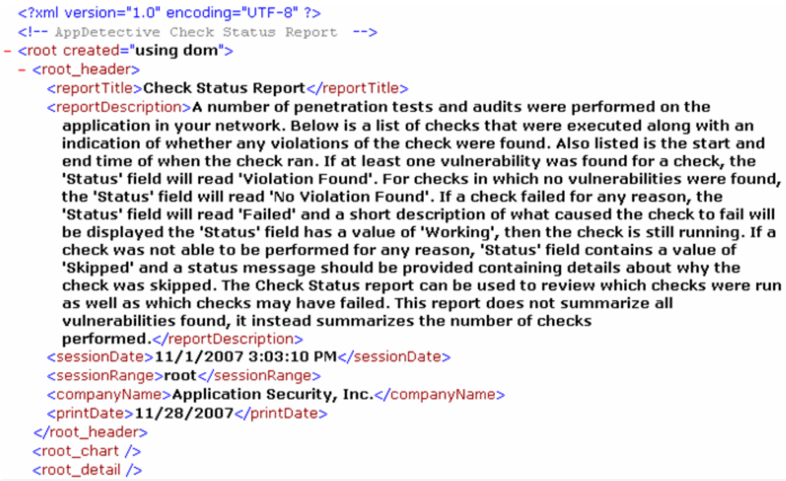
Job Details

Description	Start	End	Status	Scan Engine	
kitty	2008/10/06 14:33:16	2008/10/06 14:33:16	Dispatched to Scan ...	kitty	No Report

FIGURE: **Manage Jobs** page (**Job History** portion)

2. Right click a completed Job and choose **Show Report**.

The completed Report displays, in whatever Report format you specified (i.e., **HTML - Single File**, **Text**, **XML**, or **PDF**). A completed **Check Status** Report in XML Report format is shown below.



```
  <?xml version="1.0" encoding="UTF-8" ?>
  <!-- AppDetective Check Status Report  -->
- <root created="using dom">
  - <root_header>
      <reportTitle>Check Status Report</reportTitle>
      <reportDescription>A number of penetration tests and audits were performed on the
        application in your network. Below is a list of checks that were executed along with an
        indication of whether any violations of the check were found. Also listed is the start and
        end time of when the check ran. If at least one vulnerability was found for a check, the
        'Status' field will read 'Violation Found'. For checks in which no vulnerabilities were found,
        the 'Status' field will read 'No Violation Found'. If a check failed for any reason, the
        'Status' field will read 'Failed' and a short description of what caused the check to fail will
        be displayed the 'Status' field has a value of 'Working', then the check is still running. If a
        check was not able to be performed for any reason, 'Status' field contains a value of
        'Skipped' and a status message should be provided containing details about why the
        check was skipped. The Check Status report can be used to review which checks were run
        as well as which checks may have failed. This report does not summarize all
        vulnerabilities found, it instead summarizes the number of checks
        performed.</reportDescription>
      <sessionDate>11/1/2007 3:03:10 PM</sessionDate>
      <sessionRange>root</sessionRange>
      <companyName>Application Security, Inc.</companyName>
      <printDate>11/28/2007</printDate>
    </root_header>
    <root_chart />
    <root_detail />
```

FIGURE: Completed **Check Status** Report in XML format

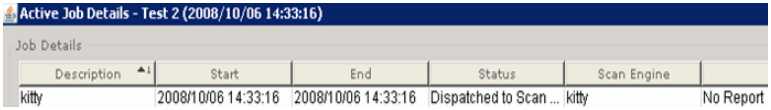
Saving a completed Report

You can **save** a completed Report for any type of Job. For more information on using the Report auto-generation feature to generate a Report for a:

- Discovery Job, see *Discovery Jobs*
- Penetration Test Job, see *Penetration Test Jobs*
- Audit Job, see *Audit Jobs*.

To save a completed Report Job:

1. Locate your completed Jobs. They display in the pane of the **Manage Jobs** page (**Job History** portion).



Active Job Details - Test 2 (2008/10/06 14:33:16)

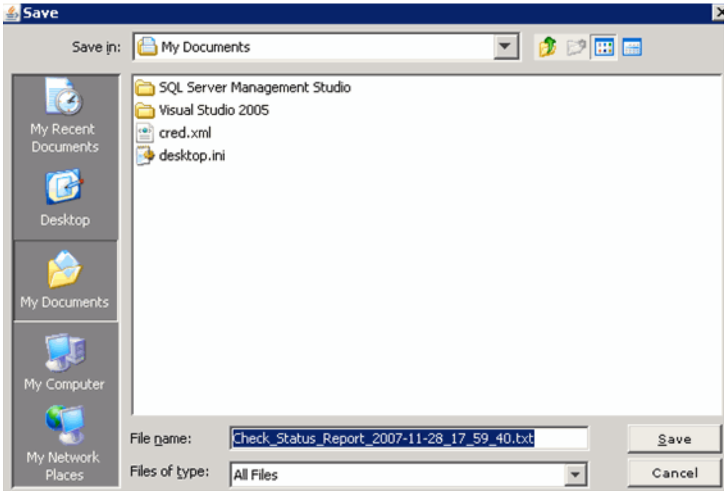
Job Details

Description	Start	End	Status	Scan Engine	
kitty	2008/10/06 14:33:16	2008/10/06 14:33:16	Dispatched to Scan ...	kitty	No Report

FIGURE: **Manage Jobs** page (**Job History** portion)

2. Right click a completed Job and choose **Save Report**.

The **Save** dialog box displays, prompting you to save a copy of your Report in whatever Report format you specified (i.e., **HTML - Single File**, **Text**, **XML**, or **PDF**).



Save

Save in: My Documents

SQL Server Management Studio
Visual Studio 2005
cred.xml
desktop.ini

File name: Check_Status_Report_2007-11-28_17_59_40.txt

Files of type: All Files

FIGURE: **Save** dialog box

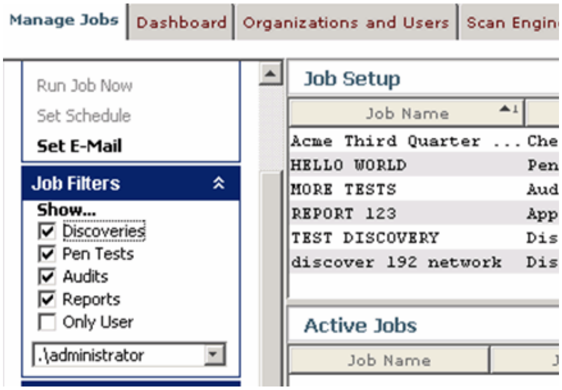
Filtering Jobs

DbProtect Vulnerability Management allows you to filter the Jobs you want to view. For example, you can filter just Penetration Test and Audit Jobs, and hide Discovery and Report Jobs.

Note: A filter reduces what information is displayed, so you won't have to scroll through a lengthy list of applications.

To filter Jobs:

1. Do one of the following to display the **Manage Jobs** page:
   - Choose **Jobs > Manage** from the menu.
   - Click the **Manage Jobs** tab.



Show...
☑ Discoveries
☑ Pen Tests
☑ Audits
☑ Reports
□ Only User
.\administrator

Acme Third Quarter ... Che
HELLO WORLD Pen
MORE TESTS Aud
REPORT 123 App
TEST DISCOVERY Dis
discover 192 network Dis

FIGURE: **Manage Jobs** page

2. Locate the **Job Filters** Toolbar on the **Manage Jobs** page; for more information, see *Toolbars*.
3. Check/uncheck:
   - **Discoveries** to filter your Discovery Jobs
   - **Pen Tests** to filter your Penetration Test Jobs
   - **Audits** to filter your Audit Jobs
   - **Reports** to filter your Report Jobs
   - **Only User**, and use the drop-down, to filter/hide Jobs by a specific User

Your filtered Jobs display in the pane of the **Manage Jobs** page (**Job Setup** portion).

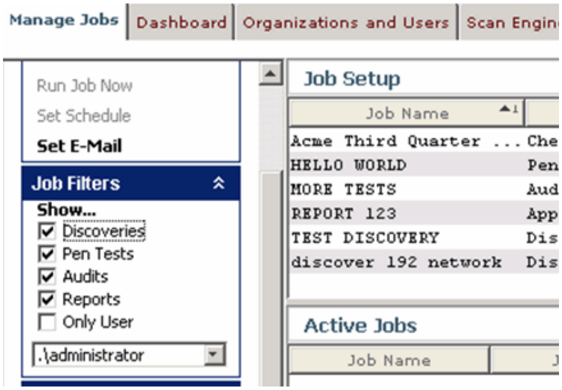
Filtering Job history

DbProtect Vulnerability Management allows you to filter Job history. For example, you can filter only *successful* Jobs that ran in the past 24 hours.

Note: A filter reduces what information is displayed, so you won't have to scroll through a lengthy list of applications.

To filter Job history:

1. Do one of the following to display the **Manage Jobs** page:
   - Choose **Jobs > Manage** from the menu.
   - Click the **Manage Jobs** tab.



Show...
☑ Discoveries
☑ Pen Tests
☑ Audits
☑ Reports
☐ Only User
.\administrator

Job Name	
Acme Third Quarter ...	Che
HELLO WORLD	Pen
MORE TESTS	Aud
REPORT 123	App
TEST DISCOVERY	Dis
discover 192 network	Dis

Job Name	J

FIGURE: **Manage Jobs** page

2. Locate the **Job History Filters** Toolbar on the **Manage Jobs** page; for more information, see *Toolbars*.
3. In the:
   - **Show...** part of the **Job History Filters** section, check/uncheck:

     -**Successful** to filter Jobs that ran successfully

     -**Failed** to filter your Jobs that failed

     -**Canceled** to filter your Jobs that you intentionally canceled

     -**Terminated** to filter your Jobs that were terminated (not through cancellation)

     -Mixed to display a mix of all completed Jobs by Job History Filter status (i.e., **Successful**, **Failed**, **Canceled**, and **Terminated**).

Important: **Include Jobs Within...** part of the **Job History Filters** section, select:

-**Last 24 Hours** to filter Jobs that ran within the last 24 hours

-**Last 7 Days** to filter Jobs that ran within the last 7 days

-**Last 30 Days** to filter Jobs that ran within the last 30 days

-**Any Time** (default) if you don't want to filter Jobs by time range.

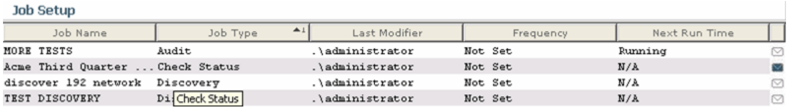
Your filtered Jobs display in the pane of the **Manage Jobs** page (**Job Setup** portion).

Deleting a set up Job

You can **delete** any Job template that you have set up in the pane of the **Manage Jobs** page (**Job Setup** portion). However, **active** Jobs must be **cancelled** (for more information, see *Cancelling an active Job*) and **completed** Jobs must be **purged** (for more information, see *Purging a completed Job*).

To delete a set up Job:

1. Locate your set up Jobs. They display in the pane of the **Manage Jobs** page (**Job Setup** portion).



Job Setup

Job Name	Job Type	Last Modifier	Frequency	Next Run Time	
MORE TESTS	Audit	.\administrator	Not Set	Running	✉
Acme Third Quarter ...	Check Status	.\administrator	Not Set	N/A	✉
discover 192 network	Discovery	.\administrator	Not Set	N/A	✉
TEST DISCOVERY	Di Check Status	.\administrator	Not Set	N/A	✉

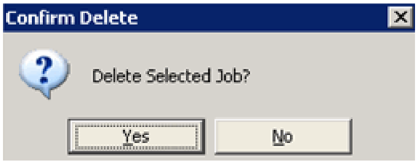
FIGURE: **Manage Jobs** page (**Job Setup** portion)

2. Do the following:

- Highlight one more set up Jobs.

Hint: Click <CTRL> to highlight non-sequential Jobs.

- Right click the set up Job(s) and select Delete.
- A **Confirm Delete** pop up prompts you to confirm the deletion.



Confirm Delete

Delete Selected Job?

FIGURE: **Confirm Delete** pop up

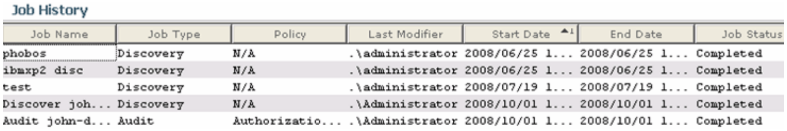
- Click the **Yes** button to delete the set up Jobs.
- The set up Jobs disappear from the pane of the **Manage Jobs** page (**Job Setup** portion).

Purging a completed Job

You can **purge** any completed Job, of any Job type, that you no longer need. Completed Jobs display in the **Manage Jobs** page (**Completed Jobs** portion).

To purge a completed Job:

1. Locate your completed Jobs. They display in the pane of the **Manage Jobs** page (**Job History** portion).



Job History

Job Name	Job Type	Policy	Last Modifier	Start Date	End Date	Job Status
phobos	Discovery	N/A	.\administrator	2008/06/25 1...	2008/06/25 1...	Completed
ibmxp2 disc	Discovery	N/A	.\administrator	2008/06/25 1...	2008/06/25 1...	Completed
test	Discovery	N/A	.\administrator	2008/07/19 1...	2008/07/19 1...	Completed
Discover joh...	Discovery	N/A	.\Administrator	2008/10/01 1...	2008/10/01 1...	Completed
Audit john-d...	Audit	Authorizatio...	.\Administrator	2008/10/01 1...	2008/10/01 1...	Completed

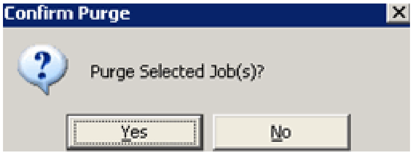
FIGURE: **Manage Jobs** page (**Job History** portion)

2. Highlight one more completed Jobs.

Hint: Click <CTRL> to highlight non-sequential Jobs.

3. Right click the completed Jobs and choose **Purge**.

A **Confirm Purge** pop up prompts you to confirm the purge.



Confirm Purge

Purge Selected Job(s)?

FIGURE: **Confirm Purge** pop up

Click the **Yes** button to purge the completed Jobs.

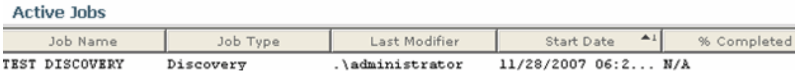
The completed Jobs disappear from the pane of the **Manage Jobs** page (**Job History** portion).

Cancelling an active Job

If your Jobs are active it means they are currently running. You can cancel any active Job in the **Manage Jobs** page (**Active Jobs** portion).

To cancel an active Job:

1. Locate your active Jobs. They display in the pane of the **Manage Jobs** page (**Active Jobs** portion).



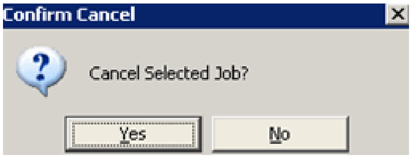
Active Jobs

Job Name	Job Type	Last Modifier	Start Date	% Completed
TEST DISCOVERY	Discovery	.\administrator	11/28/2007 06:2...	N/A

FIGURE: **Manage Jobs** page (**Active Jobs** portion)

2. Right click an active Job and choose **Cancel**.

A **Confirm Cancel** pop up prompts you to confirm the cancellation.



Cancel Selected Job?

FIGURE: **Confirm Cancel** pop up

Click the **Yes** button to cancel the active Job.

The color of the active Job turns red on the **Manage Jobs** page (**Active Jobs** portion) until DbProtect Vulnerability Management cancels the Job -- at which point it disappears.

Deleting an application to Discover

If you manually added an application for DbProtect to Discover (explained in *Adding an application to Discover*), but now you want to **delete** the application, you must **unschedule** any scheduled Jobs associated with the application (for more information, see *Unscheduling a Job*). Deleting an application deletes the application from any unscheduled Job.

Viewing Job details

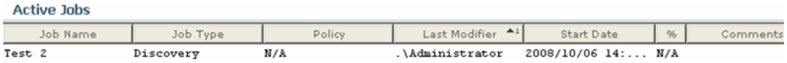
You can view the **Job details** for any Job type when the Job is in:

- an active state; for more information, see *Viewing the Job details of an active Job*
- a completed state; for more information, see *Viewing the Job details of a completed Job*.

VIEWING THE JOB DETAILS OF AN ACTIVE JOB

To view the Job details of an active Job:

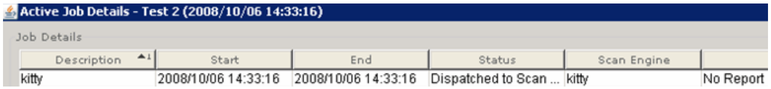
1. Locate your active Jobs. They display in the pane of the **Manage Jobs** page (**Active Jobs** portion).



Job Name	Job Type	Policy	Last Modifier	Start Date	%	Comments
Test 2	Discovery	N/A	.\Administrator	2008/10/06 14:...	N/A	

FIGURE: **Manage Jobs** page (**Active Jobs** portion)

2. Right click an active Job and choose **Show Job Details** to display the **Active Job Details** dialog box.



Active Job Details - Test 2 (2008/10/06 14:33:16)

Job Details

Description	Start	End	Status	Scan Engine	
kitty	2008/10/06 14:33:16	2008/10/06 14:33:16	Dispatched to Scan ...	kitty	No Report

FIGURE: **Active Job Details** dialog box

The **Active Job Details** dialog box displays the active Job details, including:

- **Description**
- **Start** time
- **End** time
- **Status** (e.g., **Dispatched to Scan Engine**)
- The **Scan Engine** where the Job is running.

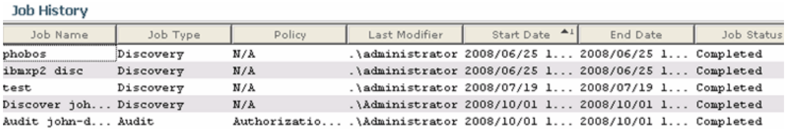
Note: You **cannot** display a Report for an active Job.

Click the **Close** button to close the **Active Job Details** dialog box.

VIEWING THE JOB DETAILS OF A COMPLETED JOB

To view the Job details of a completed Job:

1. Locate your completed Jobs. They display in the pane of the **Manage Jobs** page (**Completed Jobs** portion).



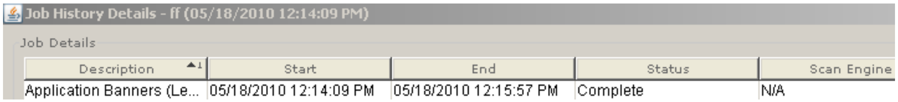
Job History

Job Name	Job Type	Policy	Last Modifier	Start Date	End Date	Job Status
phobos	Discovery	N/A	.\administrator	2008/06/25 1...	2008/06/25 1...	Completed
ibmxp2 disc	Discovery	N/A	.\administrator	2008/06/25 1...	2008/06/25 1...	Completed
test	Discovery	N/A	.\administrator	2008/07/19 1...	2008/07/19 1...	Completed
Discover joh...	Discovery	N/A	.\Administrator	2008/10/01 1...	2008/10/01 1...	Completed
Audit john-d...	Audit	Authorizatio...	.\Administrator	2008/10/01 1...	2008/10/01 1...	Completed

FIGURE: **Manage Jobs** page (**Job History** portion)

2. Do one of the following to display the **Job History Details** dialog box:
   - Double click a completed Job.
   - Right click a completed Job and choose **Show Details**.

The **Job History Details** dialog box is shown below.



Job History Details - ff (05/18/2010 12:14:09 PM)

Job Details

Description	Start	End	Status	Scan Engine
Application Banners (Le...	05/18/2010 12:14:09 PM	05/18/2010 12:15:57 PM	Complete	N/A

FIGURE: **Job History Details** dialog box

The **Job Details** portion of the **Job History Details** dialog box displays the Job's historical details, including:

- **Description**
- **Start** time
- **End** time
- **Status** (e.g., **Complete**)
- The **Scan Engine** where the Job ran.

Hint: You can click the report icon on the right side of the **Job History Details** dialog box to display the **Run Report** pop up and run a Report for a completed Job. For more information, see ***Report Jobs***.

For Audit Jobs only, the **Fix Scripts** portion of the **Job History Details** dialog box displays information about any Fix Scripts that have been run, including:

- **Name**
- **Generation Date**
- **Status**.

For more information on Fix Scripts, see *Working with Fix Scripts*.

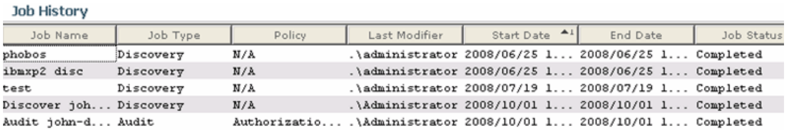
You can click the **Close** button to close the **Job History Details** dialog box.

Viewing individual vulnerabilities detected during an Audit

After you complete an Audit Job, you can view **individual vulnerabilities** detected during an Audit of a Discovered database. You can then run an "on demand" Fix Script to repair individual vulnerabilities detected on an individual Audited database instance.

To view **individual vulnerabilities** detected during an Audit of a Discovered database:

1. Audit a Discovered database application; for more information, see ***Creating an Audit Job***.
2. Locate your completed Jobs. They display in the pane of the **Manage Jobs** page (**Completed Jobs** portion).

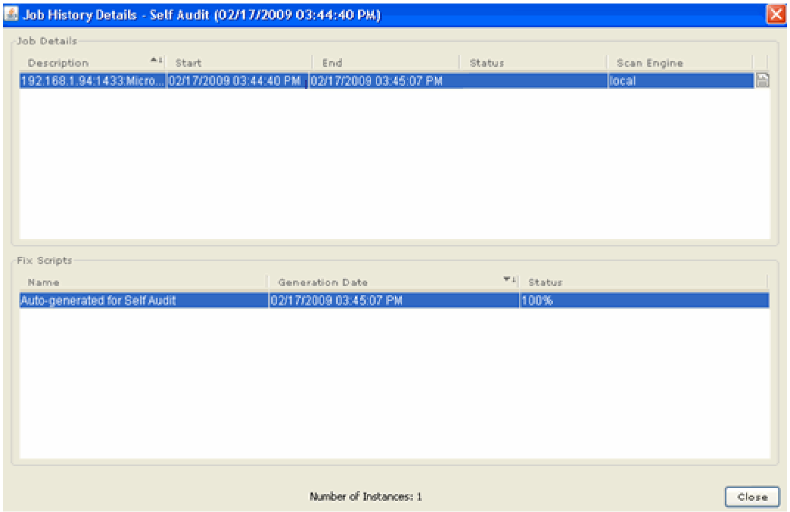


Job History

Job Name	Job Type	Policy	Last Modifier	Start Date	End Date	Job Status
phobos	Discovery	N/A	.\administrator	2008/06/25 1...	2008/06/25 1...	Completed
ibmxp2 disc	Discovery	N/A	.\administrator	2008/06/25 1...	2008/06/25 1...	Completed
test	Discovery	N/A	.\administrator	2008/07/19 1...	2008/07/19 1...	Completed
Discover joh...	Discovery	N/A	.\Administrator	2008/10/01 1...	2008/10/01 1...	Completed
Audit john-d...	Audit	Authorizatio...	.\Administrator	2008/10/01 1...	2008/10/01 1...	Completed

FIGURE: **Manage Jobs** page (**Job History** portion)

3. Right click a completed Audit Job and choose **Show Details** to display the **Job History Details** dialog box.



Job History Details - Self Audit (02/17/2009 03:44:40 PM)

Job Details

Description	Start	End	Status	Scan Engine
192.168.1.94:1433:Micro...	02/17/2009 03:44:40 PM	02/17/2009 03:45:07 PM		local

Fix Scripts

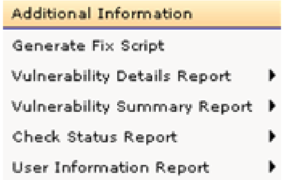
Name	Generation Date	Status
Auto-generated for Self Audit	02/17/2009 03:45:07 PM	100%

Number of Instances: 1

FIGURE: **Job History Details** dialog box

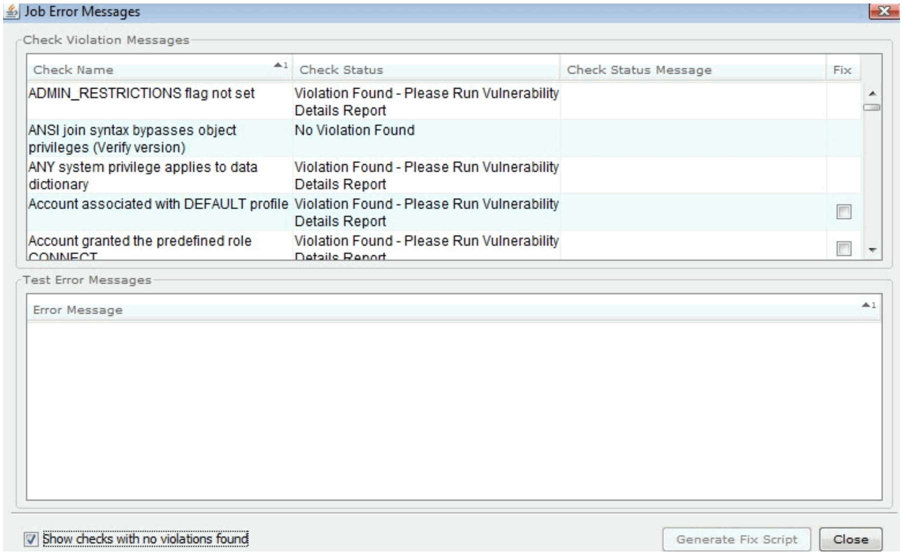
4. Do one of the following to display the **Job Error Messages** dialog box:

   - Right click any completed Audit Job in the upper **Job Details** portion of the **Job History Details** dialog box, and select **Additional Information**.



   - Double click any completed Audit Job in the upper **Job Details** portion of the **Job History Details** dialog box.

The **Job Error Messages** dialog box (shown below) lists **individual vulnerabilities** detected during an Audit of a Discovered database.



Job Error Messages

Check Violation Messages

Check Name	Check Status	Check Status Message	Fix
ADMIN_RESTRICTIONS flag not set	Violation Found - Please Run Vulnerability Details Report		
ANSI join syntax bypasses object privileges (Verify version)	No Violation Found		
ANY system privilege applies to data dictionary	Violation Found - Please Run Vulnerability Details Report		
Account associated with DEFAULT profile	Violation Found - Please Run Vulnerability Details Report		□
Account granted the predefined role CONNECT	Violation Found - Please Run Vulnerability Details Report		□

Test Error Messages

Error Message

☑ Show checks with no violations found

FIGURE: **Job Error Messages** dialog box

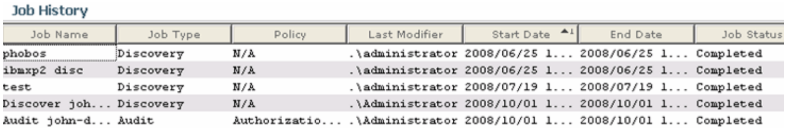
Hint: You can check the **Show checks with no violation found** to display checks that did not detect any vulnerabilities during your Audit.

Hint: In the **Check Violation Messages** portion of the **Job Error Messages** dialog box, you can generate an "on demand" Fix Script to repair **individual vulnerabilities** for a selected Audited database instance; for more information, see ***Running an "on demand" Fix Script to repair individual vulnerabilities detected on an individual Audited database instance***.

Viewing the properties of a completed Job

To view the properties of a completed Job:

1. Locate your completed Jobs. They display in the pane of the **Manage Jobs** page (**Job History** portion).



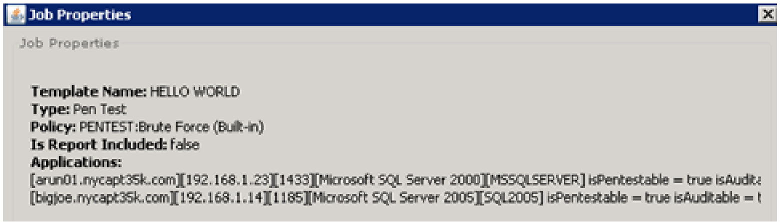
Job History

Job Name	Job Type	Policy	Last Modifier	Start Date	End Date	Job Status
phobos	Discovery	N/A	.\administrator	2008/06/25 1...	2008/06/25 1...	Completed
ibmxp2 disc	Discovery	N/A	.\administrator	2008/06/25 1...	2008/06/25 1...	Completed
test	Discovery	N/A	.\administrator	2008/07/19 1...	2008/07/19 1...	Completed
Discover joh...	Discovery	N/A	.\Administrator	2008/10/01 1...	2008/10/01 1...	Completed
Audit john-d...	Audit	Authorizatio...	.\Administrator	2008/10/01 1...	2008/10/01 1...	Completed

FIGURE: **Manage Jobs** page (**Job History** portion)

2. Right click a completed Job and choose **Show Properties**.

The **Job Properties** dialog box displays the Job's properties, including: **Template Name**, **Type** of Job (e.g., **Pen Test**), **Policy** applied, whether an auto-generated Report is included, and all Applications that you Discovered, Penetration Tested, Audited, or Reported on.



Template Name: HELLO WORLD
Type: Pen Test
Policy: PENTEST:Brute Force (Built-in)
Is Report Included: false
Applications:
[arun01.nycapt35k.com][192.168.1.23][1433][Microsoft SQL Server 2000][MSSQLSERVER] isPentestable = true isAudit
[bigjoe.nycapt35k.com][192.168.1.14][1185][Microsoft SQL Server 2005][SQL2005] isPentestable = true isAuditable = t

FIGURE: **Job Properties** dialog box

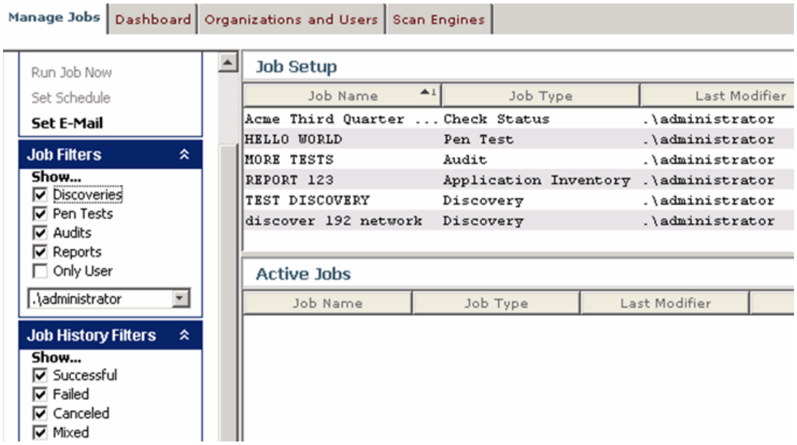
Click the **Close** button to close the **Job Properties** dialog box.

Setting the refresh rate of data on the Manage Jobs page

Job data refreshes automatically according to whatever time interval (in seconds) you set on the **Manage Jobs** page.

To set the refresh rate of Job data on the **Manage Jobs** page:

1. Do one of the following to display the **Manage Jobs** page:
   - Choose **Jobs > Manage** from the menu.
   - Click the **Manage Jobs** tab.



Job Filters
Show...
☑ Discoveries
☑ Pen Tests
☑ Audits
☑ Reports
□ Only User
.\administrator

Job History Filters
Show...
☑ Successful
☑ Failed
☑ Canceled
☑ Mixed

Job Setup

Job Name	Job Type	Last Modifier
Acme Third Quarter ...	Check Status	.\administrator
HELLO WORLD	Pen Test	.\administrator
MORE TESTS	Audit	.\administrator
REPORT 123	Application Inventory	.\administrator
TEST DISCOVERY	Discovery	.\administrator
discover 192 network	Discovery	.\administrator

Active Jobs

Job Name	Job Type	Last Modifier

FIGURE: **Manage Jobs** page

2. Locate the **Refresh** Toolbar on the **Manage Jobs** page.

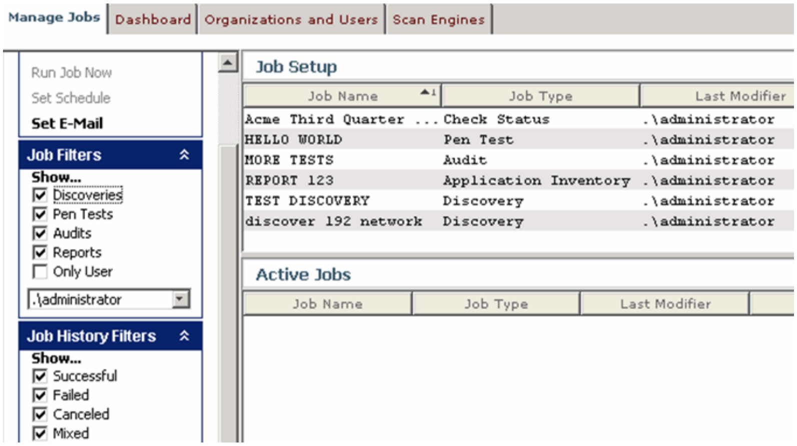
3. Edit the Job data refresh rate of the **Manage Jobs** page in the **seconds** field, then click the **Set** button.

DbProtect Vulnerability Management changes the Job data refresh rate of the **Manage Jobs** page.

Manually refreshing data on the Manage Jobs Page

To manually refresh Job data on the **Manage Jobs** page:

1. Do one of the following to display the **Manage Jobs** page:
   - Choose **Jobs** > **Manage** from the menu.
   - Click the **Manage Jobs** tab.



Job Filters
Show...
☑ Discoveries
☑ Pen Tests
☑ Audits
☑ Reports
☐ Only User
.\administrator

Job History Filters
Show...
☑ Successful
☑ Failed
☑ Canceled
☑ Mixed

Job Setup

Job Name	Job Type	Last Modifier
Acme Third Quarter ...	Check Status	.\administrator
HELLO WORLD	Pen Test	.\administrator
MORE TESTS	Audit	.\administrator
REPORT 123	Application Inventory	.\administrator
TEST DISCOVERY	Discovery	.\administrator
discover 192 network	Discovery	.\administrator

Active Jobs

Job Name	Job Type	Last Modifier	

FIGURE: **Manage Jobs** page

2. Locate the **Refresh** Toolbar on the **Manage Jobs** page.

3. Click the **Refresh** button in the **Refresh** Toolbar.

DbProtect Vulnerability Management refreshes the Job data on the **Manage Jobs** page.

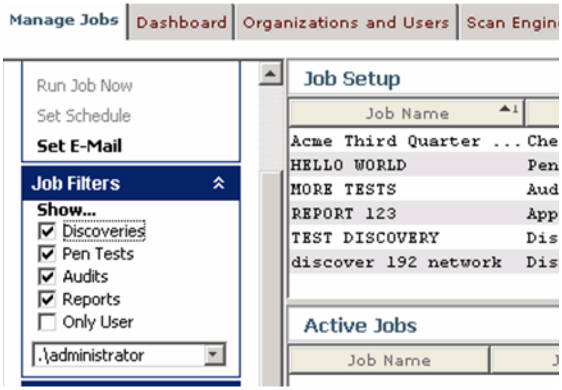
Scheduling email notification upon Job completion

DbProtect Vulnerability Management allows you to notify others via email when DbProtect Vulnerability Management completes a Job. This feature works for all types of Jobs, i.e., Discovery, Penetration Test, Audit, and Report Jobs.

Note: In order to notify others via email when DbProtect Vulnerability Management completes a Job, DbProtect Super Admin, DbProtect Admin, or Vulnerability Management Admin **must** first properly configure your Organization's SMTP mail server information. Otherwise, the email notification of Job completion feature will **not** work. For more information, see *Configuring SMTP Mail Server Information for Your Organization*.

To schedule email notification upon Job completion:

1. Do one of the following to display the **Manage Jobs** page:
   - Choose **Jobs** > **Manage** from the menu.
   - Click the **Manage Jobs** tab.



Show...
☑ Discoveries
☑ Pen Tests
☑ Audits
☑ Reports
□ Only User
.\administrator

Job Name	
Acme Third Quarter ...	Che
HELLO WORLD	Pen
MORE TESTS	Aud
REPORT 123	App
TEST DISCOVERY	Dis
discover 192 network	Dis

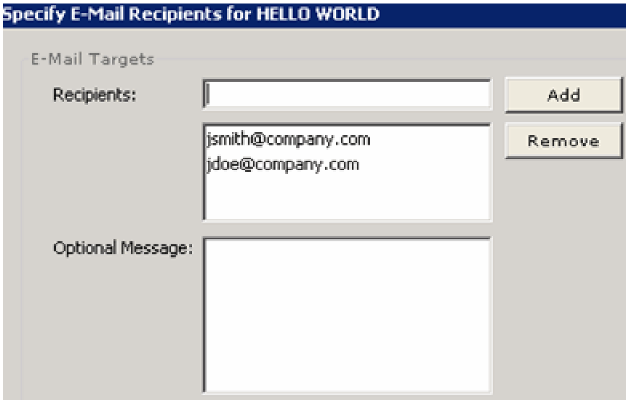
FIGURE: **Manage Jobs** page

Highlight one Job in the pane of the **Manage Jobs** page (**Job Setup** portion).

Note: You can only send email for one Job at a time. Do not select multiple Jobs.

2. Do one of the following to display the **Specify E-Mail Recipients for <JOB NAME>** dialog box:
   - Click **Set E-Mail** in the **Job Setup Options** Toolbar
   - Right click the Job and choose **Set E-Mail Recipients**.

Note: The same dialog box displays for all Job Types.



Recipients:

jsmith@company.com
jdoe@company.com

Optional Message:

FIGURE: **Specify E-Mail Recipients for <JOB NAME>** dialog box

Do the following:

- Enter one email recipient’s email address (e.g., `jsmith@company.com`) in the **Recipients:** field.

Caution! You can only enter one email recipient’s email address at a time.

- Click the **Add** button to add the email address to the field below the **Recipients:** field.
- Repeat to add as many email recipients’ email addresses as you want.

Hint: If you want to remove an email address, highlight the email address in the field below the **Recipients:** field, and click the **Remove** button.

Optionally, you can enter a message to your email recipients in the **Optional Message:** field.

Click the **Save** button.

3. The **Specify E-Mail Recipients for <JOB NAME>** dialog box closes. The **Manage Jobs** page (**Job Setup** portion) displays email icons. A blue icon indicates the corresponding Job is configured to email *at least one* email recipient when the Job completes. A white icon indicates you have **not** configured the corresponding Job to email *any* email recipients when the Job completes.

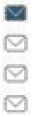


FIGURE: Email notification icons

Remember: in order to notify others via email when DbProtect Vulnerability Management completes a Job, an Admin or Super Admin **must** first properly configure your Organization’s SMTP mail server information. Otherwise, the email notification of Job completion feature will not work. For more information, see *Configuring SMTP Mail Server Information for Your Organization*.

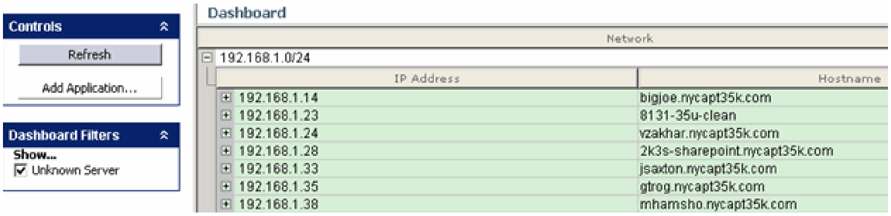
Working with the Dashboard

This chapter consists of the following topics:

- *Understanding the Dashboard*
- *Refreshing the Dashboard*
- *Adding an application to Discover*
- *Filtering "unknown" Discovered servers*
- *Detecting Oracle SIDs with a listener password.*

Understanding the Dashboard

The **Dashboard** displays detailed data about applications Discovered on your network, recent Penetration Tests and Audits performed, and the number of vulnerabilities detected.



Show...
☑ Unknown Server

⊟ 192.168.1.0/24

IP Address	Hostname
⊞ 192.168.1.14	bigjoe.nycapt35k.com
⊞ 192.168.1.23	8131-35u-clean
⊞ 192.168.1.24	vzakhar.nycapt35k.com
⊞ 192.168.1.28	2k3s-sharepoint.nycapt35k.com
⊞ 192.168.1.33	jsaxton.nycapt35k.com
⊞ 192.168.1.35	gtrog.nycapt35k.com
⊞ 192.168.1.38	mhamsho.nycapt35k.com

FIGURE: Dashboard

The columns in the pane of the **Dashboard** display the following information:

- **IP address.** The IP addresses of your Discovered applications.
- **Hostname.** The server hostnames of your Discovered applications.

Note: For more information on the pane and other DbProtect Vulnerability Management UI components, see *Understanding the DbProtect Vulnerability Management Portal User Interface (UI).*

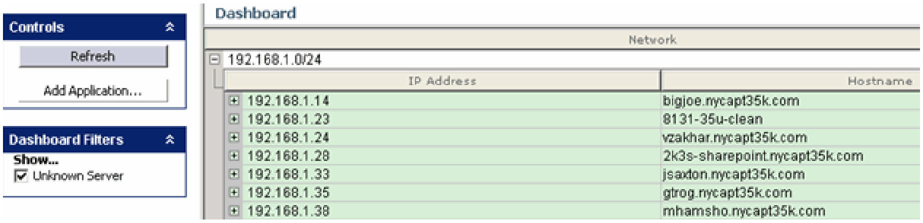
You can click the **+** icons under the **IP Address** column to display the Discovered applications. The **Dashboard** displays the following detailed information:

- **IP addresses** and **hostnames** of the applications Discovered on your network; for more information, see *Discovery Jobs*
- **ports** where your Discovered applications are installed
- **status** of your Discovered application (e.g., **Active**, **Inactive**, etc.)
- date/time of the last **Pen Test** or **Audit** performed on each application, and the **number of vulnerabilities** that were detected; for more information, see *Penetration Test Jobs* and *Audit Jobs.*

Refreshing the Dashboard

To refresh the data on the **Dashboard**:

1. Do one of the following to display the **Dashboard**:
    - Choose **Admin** > **Dashboard** from the menu.
    - Click the **Dashboard** button on the toolbar.



IP Address	Hostname
⊞ 192.168.1.14	bigjoe.nycapt35k.com
⊞ 192.168.1.23	8131-35u-clean
⊞ 192.168.1.24	vzakhar.nycapt35k.com
⊞ 192.168.1.28	2k3s-sharepoint.nycapt35k.com
⊞ 192.168.1.33	jsaxton.nycapt35k.com
⊞ 192.168.1.35	gtrog.nycapt35k.com
⊞ 192.168.1.38	mhamsho.nycapt35k.com

FIGURE: Dashboard

Do the following:

- Locate the **Controls** Toolbar on the **Dashboard**.
- Click the **Refresh** button in the **Controls** Toolbar on the **Dashboard**.

The **Dashboard** refreshes the detailed data about applications Discovered on your network, recent Penetration Tests and Audits performed, and the number of vulnerabilities detected.

Adding an application to Discover

The **Dashboard** allows you to add new applications (typically an Oracle SID or a DB2 database) for DbProtect to Discover.

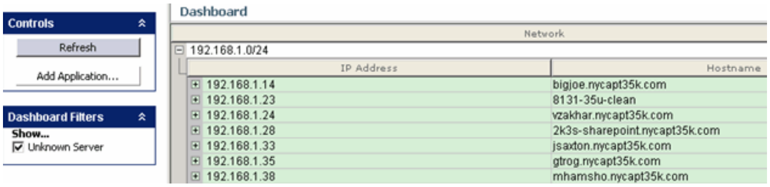
The reason this feature exists is because when you run an **Oracle** Discovery, DbProtect only detects the Oracle Listener (unless you specified a listener password during Scan Engine installation; for more information, see the *DbProtect Installation Guide*). In order to run an Audit or Pen Test on a Discovered Oracle database, the Oracle SID **must** display in the **Dashboard**. Therefore, in most cases, you must manually add the Oracle SID to the **Dashboard** by following the steps in this topic.

The same is true for running Audit and Pen Test Jobs on **DB2**. When you run a **DB2** Discovery, DbProtect only detects the DB2 instance. In order to run an Audit or Pen Test on a Discovered DB2 database, the DB2 database **must** display in the **Dashboard**. Therefore, in most cases, you must manually add the DB2 database to the **Dashboard** by following the steps in this topic.

Note: If you want to **delete an application to Discover** from DbProtect, you must unschedule any scheduled Jobs associated with the application. For more information, see *Unscheduling a Job*.

To add an application to Discover:

1. Do one of the following to display the **Dashboard**:
   - Choose **Admin** > **Dashboard** from the menu.
   - Click the **Dashboard** button on the toolbar.

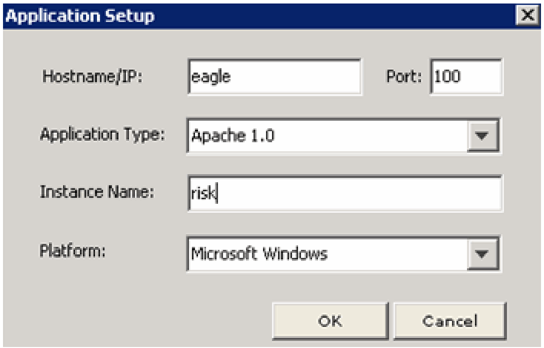


⊟ 192.168.1.0/24

IP Address	Hostname
⊞ 192.168.1.14	bigjoe.nycapt35k.com
⊞ 192.168.1.23	8131-35u-clean
⊞ 192.168.1.24	vzakhar.nycapt35k.com
⊞ 192.168.1.28	2k3s-sharepoint.nycapt35k.com
⊞ 192.168.1.33	jsaxton.nycapt35k.com
⊞ 192.168.1.35	gtrog.nycapt35k.com
⊞ 192.168.1.38	mhamsho.nycapt35k.com

FIGURE: Dashboard

2. Do the following:
   - Click an Organization in the pane of the **Dashboard**.
   - Locate the **Controls** Toolbar on the **Dashboard**.
   - Click the **Add Application** button in the **Controls** Toolbar on the **Dashboard** to display the **Application Setup** dialog box.



Hostname/IP: eagle Port: 100

Application Type: Apache 1.0

Instance Name: risk

Platform: Microsoft Windows

FIGURE: **Add Application to Organization** dialog box

3. Do the following:
   - Enter the **Hostname/IP:** address of the new application.
   - Enter the **Port:** number of the new application.
   - Use the **Application Type:** drop-down to select an application type (e.g., **DB2 6.1**, **Lotus Notes/Domino**, **Oracle 10g Database**, **Sybase 12.5 Database**, etc.).
   - Enter the database **Instance Name:** where the application database is installed.
   - Use the **Platform:** drop-down to select the application's platform.

4. Click the **OK** button.

The added application displays on the **Dashboard**, under the selected Organization, and it will now be available when you create Penetration Test and Audit Jobs.

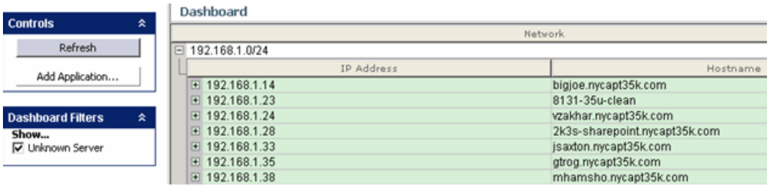
Filtering "unknown" Discovered servers

Sometimes a Discovery can't figure out a server type. You can filter Discovered servers listed as an "Unknown" server type.

To refresh the data on the **Dashboard**:

1. Do one of the following to display the **Dashboard**:

- Choose **Admin > Dashboard** from the menu.
- Click the **Dashboard** button on the toolbar.



IP Address	Hostname
192.168.1.14	bigjoe.nycapt35k.com
192.168.1.23	8131-35u-clean
192.168.1.24	vzakhar.nycapt35k.com
192.168.1.28	2k3s-sharepoint.nycapt35k.com
192.168.1.33	jsaxton.nycapt35k.com
192.168.1.35	gtrog.nycapt35k.com
192.168.1.38	mhamsho.nycapt35k.com

FIGURE: Dashboard

Locate the **Dashboard Filters** Toolbar on the **Dashboard**.

You can:

- check the **Show... Unknown Server** checkbox in the **Dashboard Filters** Toolbar to display "unknown" Discovered server types on the **Dashboard**, in addition to Discovered servers of identifiable server types
- uncheck the **Show... Unknown Server** checkbox in the **Dashboard Filters** Toolbar to display **only** Discovered servers of identifiable server types on the **Dashboard** (and hide "unknown" Discovered server types).

The **Dashboard** refreshes the results about Discovered servers on your network (i.e., filtered by "unknown" server types only, or all server types) according to whether you check or uncheck the **Show... Unknown Server** checkbox.

Detecting Oracle SIDs with a listener password

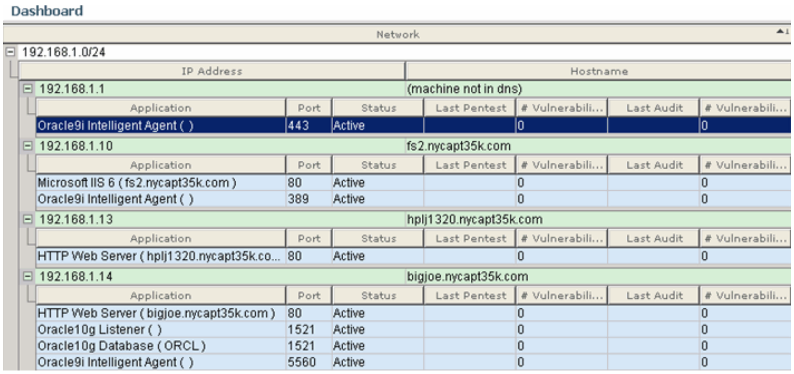
When DbProtect Vulnerability Management Discovers an Oracle listener, it might not be able to find all the Oracle SIDs because the listener may require a password. DbProtect Vulnerability Management allows you to specify the listener password so the Scan Engine can find the missing Oracle SIDs.

Caution! You **cannot** manually detect Oracle SIDs if the target Oracle listener is not using the default listener name, and the version of Oracle is 10g or 11g.

To detect Oracle SIDs with a listener password:

1. Do one of the following to display the **Dashboard**:
   - Choose **Admin** > **Dashboard** from the menu.
   - Click the **Dashboard** button on the toolbar.

In the network tree view, right click a listener.



IP Address	Hostname
192.168.1.1	(machine not in dns)

Application	Port	Status	Last Pentest	# Vulnerabili...	Last Audit	# Vulnerabili...
Oracle9i Intelligent Agent ( )	443	Active		0		0

IP Address	Hostname
192.168.1.10	fs2.nycapt35k.com

Application	Port	Status	Last Pentest	# Vulnerabili...	Last Audit	# Vulnerabili...
Microsoft IIS 6 (fs2.nycapt35k.com)	80	Active		0		0
Oracle9i Intelligent Agent ( )	389	Active		0		0

IP Address	Hostname
192.168.1.13	hplj1320.nycapt35k.com

Application	Port	Status	Last Pentest	# Vulnerabili...	Last Audit	# Vulnerabili...
HTTP Web Server (hplj1320.nycapt35k.co...	80	Active		0		0

IP Address	Hostname
192.168.1.14	bigjoe.nycapt35k.com

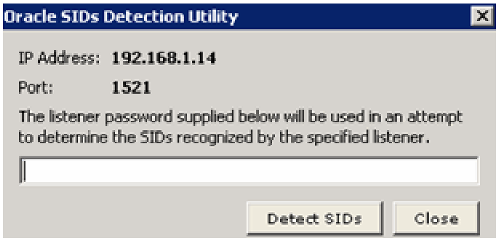
Application	Port	Status	Last Pentest	# Vulnerabili...	Last Audit	# Vulnerabili...
HTTP Web Server (bigjoe.nycapt35k.com)	80	Active		0		0
Oracle10g Listener ( )	1521	Active		0		0
Oracle10g Database (ORCL)	1521	Active		0		0
Oracle9i Intelligent Agent ( )	5560	Active		0		0

FIGURE: Dashboard

2. Click the + icons under the **IP Address** column to display the Discovered applications. For more information, see *Understanding the Dashboard*.

3. Right click a Discovered Oracle listener, and choose **Detect SIDS with Listener Password**.

The **Oracle SIDs Detection Utility** pop up displays.



Oracle SIDs Detection Utility

IP Address: 192.168.1.14

Port: 1521

The listener password supplied below will be used in an attempt to determine the SIDs recognized by the specified listener.

FIGURE: **Oracle SIDs Detection Utility** pop up

4. Enter the password for the specified listener.
5. Click the **Detect SIDs** button.
6. Refresh the **Dashboard** to see the updated applications list.

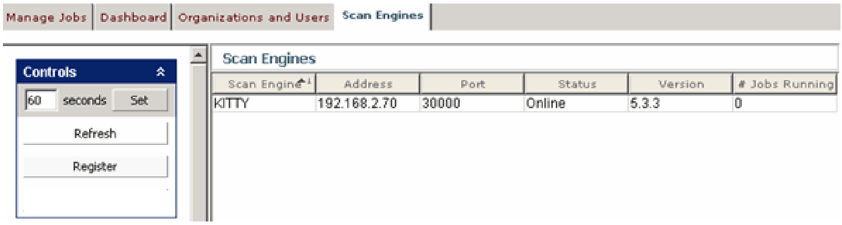
Working with Scan Engines

This chapter consists of the following topics:

- *Understanding the Scan Engines page*
- *Registering and unregistering a Scan Engine*
- *Monitoring the health of your Scan Engines*
- *Editing a Scan Engine*
- *Configuring the properties of a Scan Engine*
- *Setting the Scan Engine refresh rate*
- *Manually refreshing the Scan Engine.*

Understanding the Scan Engines page

The **Scan Engines** page (shown below) allows you to manage your installed and configured Scan Engines. Specifically, the **Scan Engines** page allows you to register your installed/configured Scan Engines, set the Scan Engine refresh rate, manually refresh the Scan Engine, monitor the "health" of your installed/configured/registered Scan Engines, or run an ASAP Update to obtain the latest Scan Engine software.



Scan Engines

Scan Engine	Address	Port	Status	Version	# Jobs Running
KITTY	192.168.2.70	30000	Online	5.3.3	0

FIGURE: **Scan Engines** page

The columns in the pane of the **Scan Engines** page display the following information:

- **Scan Engine.** The names of your installed and registered Scan Engines.
- **Address.** The hostnames or IP addresses where your Scan Engines are installed and registered.
- **Port.** The ports where your installed and registered Scan Engines "listen" to incoming network traffic.
- **Status.** The status of your installed and registered Scan Engines (i.e., **Online**, **Offline**, **Unknown**, and **Updating**).
- **Version.** The versions of your installed and registered Scan Engines.
- **# Jobs Running.** How many Scan Engines are actively running.

Note: For more information on the pane and other DbProtect Vulnerability Management UI components, see *Understanding the DbProtect Vulnerability Management Portal User Interface (UI).*

Specifically, the **Scan Engines** page allows you to:

- register an installed/configured Scan Engine; for more information, see *Registering a Scan Engine*
- monitor the "health" of your Scan Engine; for more information, see *Monitoring the health of your Scan Engines*
- edit your Scan Engines; for more information, see *Editing a Scan Engine*
- configure the properties of your Scan Engines; for more information, see *Configuring the properties of a Scan Engine*
- set the Scan Engine refresh rate (from the **Scan Engines** page); for more information, see *Setting the Scan Engine refresh rate*
- manually refresh the Scan Engine (from the **Scan Engines** page); for more information, see *Manually refreshing the Scan Engine*.

Registering and unregistering a Scan Engine

The **Scan Engines** page allows you to **register** each installed/configured Scan Engine on your network. The **Scan Engines** page also allows you to **unregister** a registered Scan Engine.

Registration involves the specification of:

- a hostname or IP address where the Scan Engine is installed
- the port where the Scan Engine "listens" to incoming network traffic
- an IP address range (or the name of a host machine) which define the extent to which the Scan Engine can scan/test applications on your network.

This topic consists of the following sub-topics:

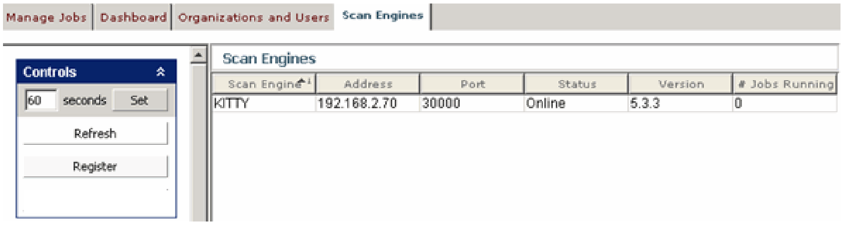
- *Registering a Scan Engine*
- *Unregistering a Scan Engine*.

REGISTERING A SCAN ENGINE

To register a Scan Engine:

1. Do one of the following to display the **Scan Engines** page:

- Choose **Admin** > **Scan Engines** from the menu
- Click the **Scan Engines** tab.

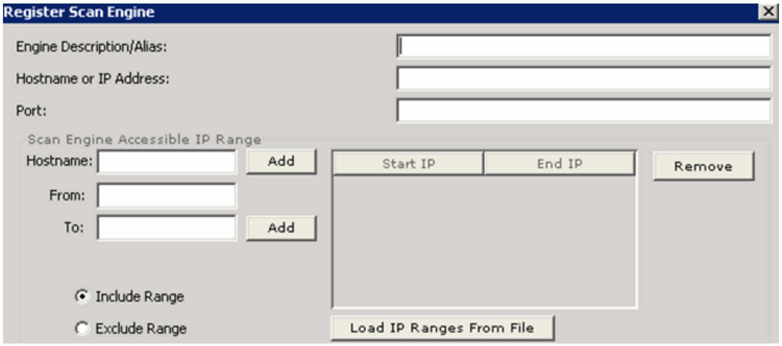


Scan Engines

Scan Engine	Address	Port	Status	Version	# Jobs Running
KITTY	192.168.2.70	30000	Online	5.3.3	0

FIGURE: **Scan Engines** page

2. Do one of the following to display the **Register Scan Engine** dialog box:
   - Choose **Scan Engines > Register** from the menu.
   - Click the **Register** button in the Controls portion.



● Include Range
○ Exclude Range

FIGURE: First **Register Scan Engine** dialog box

3. The upper portion of the dialog box allows you to enter the information you specified during Scan Engine installation and configuration. Specifically, you **must** enter the:
   - Scan Engine Description/Alias
   - **Hostname or IP Address** where the Scan Engine is installed; for more information, see the *DbProtect Installation Guide*

Caution! Do **not** register your Scan Engine with `hostname='localhost'`. You must specify either the correct hostname or a valid IP address.

   - **Port** where the Scan Engine "listens" to incoming network traffic; for more information, see the *DbProtect Installation Guide.*

4. The **Scan Engine Accessible IP Address Range** portion of the **Register Scan Engine** dialog box allows you to specify ranges of IP addresses (or enter the name of a host machine), which define the extent to which the Scan Engine can scan/test applications on your network.

Example: You can exclude the IP address range `192.168.1.1` through `192.168.1.100` when performing a Discovery using this registered Scan Engine.

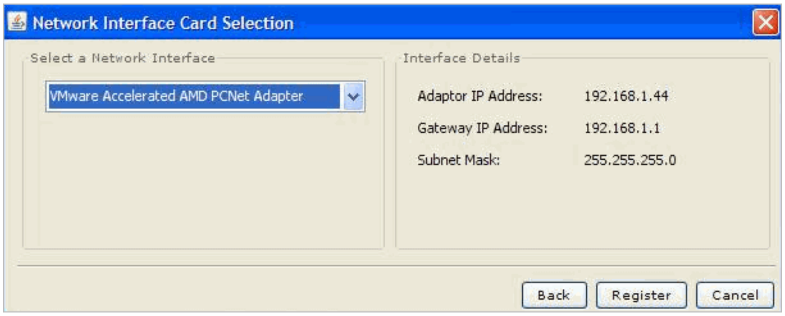
- In the **Scan Engine Accessible IP Address Range** portion of the first **Register Scan Engine** dialog box, you can do the following:
- Select whether you want to **include** or **exclude** ranges of IP addresses (or IP addresses on host machines) by selecting **Include Range** or **Exclude Range**.
- Enter a machine host name in the **Hostname** field.
- Click the **Add** button to add the IP addresses of a host machine to the include or exclude list (depending whether you chose **Include Range** or **Exclude Range**, above).

- Enter an IP address range (for example, `192.168.1.1` through `192.168.1.100`) in the **From:** and **To:** fields.
- Click the **Add** button to add the IP addresses to the include or exclude list (depending whether you chose **Include Range** or **Exclude Range**, above).

Hint: To remove an IP address range from either the include or exclude list, highlight the range, then click the **Remove** button.

- Click the **Load IP Ranges From File** button to display an **Open** dialog box and upload a standard text file (using the format `ip` or `ip-ip`).

5. Click the **Next** button to display the **Network Interface Card Selection** dialog box.



Select a Network Interface: VMware Accelerated AMD PCNet Adapter

Adaptor IP Address: 192.168.1.44

Gateway IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

FIGURE: **Network Interface Card Selection** dialog box

A **network interface card (NIC)** is used to connect your computer to an Ethernet network. The card provides an interface to DbProtect Vulnerability Management. During Scan Engine registration, DbProtect Vulnerability Management identifies all available NICs.

Use the **Select a Network Interface** drop-down to select which NIC you want the Scan Engine to use. The **Interface Details** display on the right half of the dialog box.

6. Click the **Register** button to register your Scan Engine.

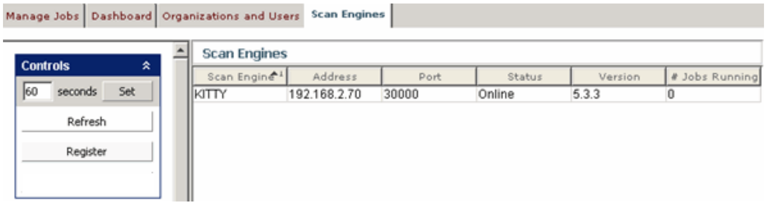
Your Scan Engine is registered.

UNREGISTERING A SCAN ENGINE

To unregister a Scan Engine:

1. Do one of the following to display the **Scan Engines** page:

   - Choose **Admin > Scan Engines** from the menu
   - Click the **Scan Engines** tab.



Scan Engine	Address	Port	Status	Version	# Jobs Running
KITTY	192.168.2.70	30000	Online	5.3.3	0

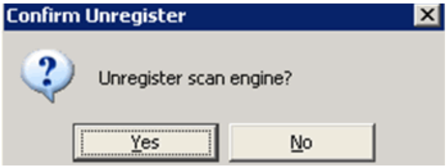
FIGURE: **Scan Engines** page

2. Do the following:

   - Highlight one more registered Scan Engines.

Hint: Click <CTRL> to highlight non-sequential registered Scan Engines.

   - Right click the registered Scan Engine(s) and select **Unregister**.
   - A **Confirm Unregister** pop up prompts you to confirm the unregistration.



Unregister scan engine?

FIGURE: **Confirm Delete** pop up

   - Click the **Yes** button to unregister the registered Scan Engines.
   - The registered Scan Engines disappear from the pane of the **Scan Engines** page.

Monitoring the health of your Scan Engines

You can monitor the "health" of your installed/configured/registered Scan Engines via the **Scan Engines** page. If DbProtect Vulnerability Management is **not** detecting vulnerabilities, it **could** be because your Scan Engine is "unhealthy".

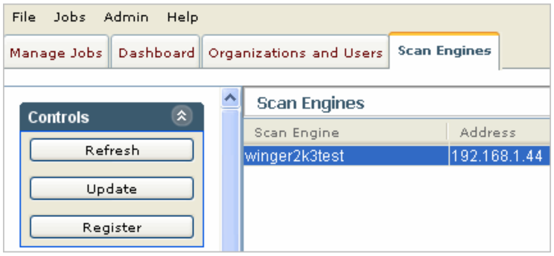
A "healthy" Scan Engine is:

- **"up and running"** on the machine where it is installed
- **actively Discovering applications** on this machine's database SIDs/instances (on which it can Penetration Tests and Audits)
- **actively collecting/interpreting data and detecting vulnerabilities**.

To monitor the "health" of your Scan Engines:

1. Do one of the following to display the **Scan Engines** page:

- Choose **Admin** > **Scan Engines** from the menu
- Click the **Scan Engines** tab.



Scan Engine	Address
winger2k3test	192.168.1.44

FIGURE: **Scan Engines** page

2. For each installed/configured Scan Engine, you can view its:

- name in the **Scan Engine** column
- IP address in the **Address** column
- installation port in the **Port** column
- status in the **Status** column

Important: If the **Status** of your Scan Engine is **Down**, this indicates your Scan Engine is "unhealthy".

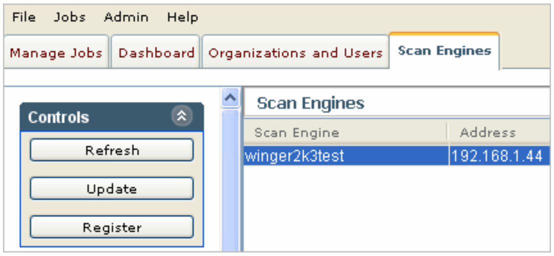
- software version in the **Version** column.

Editing a Scan Engine

DbProtect Vulnerability Management allows you to **edit** the parameters of a registered Scan Engine on your network; for more information on Scan Engine registration, see the *DbProtect Installation Guide*).

To edit a Scan Engine:

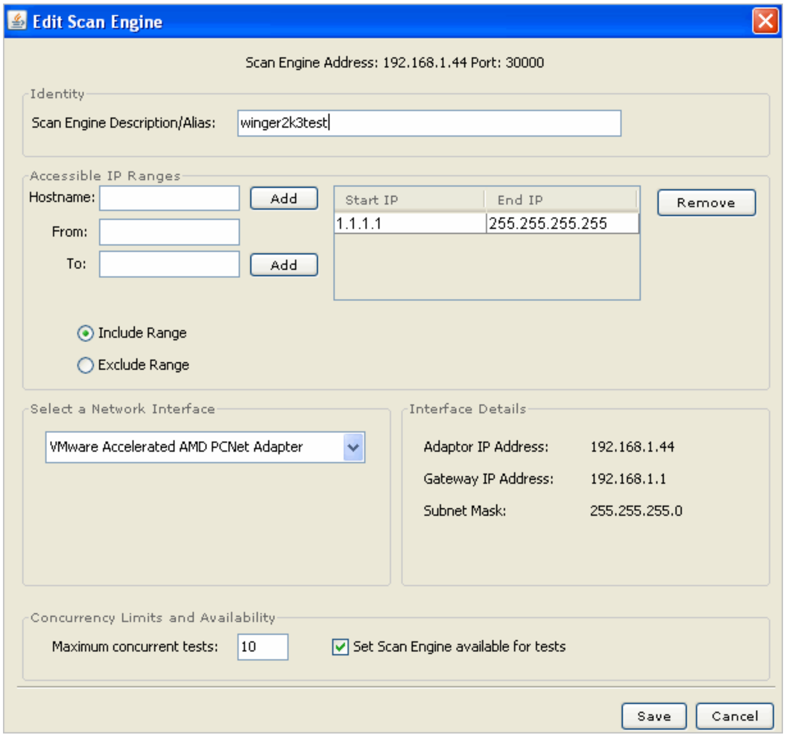
1. Do one of the following to display the **Scan Engines** page:
   - Choose **Admin** > **Scan Engines** from the menu
   - Click the **Scan Engines** tab.



Scan Engine	Address
winger2k3test	192.168.1.44

FIGURE: **Scan Engines** page

2. Do one of the following to display the **Edit Scan Engine** dialog box:
   - Choose **Scan Engines > Edit** from the menu.
   - Right click a Scan Engine (in the **Scan Engines** portion of the **Scan Engines** page) and choose **Edit**.



Scan Engine Address: 192.168.1.44 Port: 30000

Identity

Scan Engine Description/Alias: winger2k3test

Accessible IP Ranges

Hostname:

From:

To:

Start IP	End IP
1.1.1.1	255.255.255.255

● Include Range

○ Exclude Range

Select a Network Interface

VMware Accelerated AMD PCNet Adapter

Interface Details

Adaptor IP Address: 192.168.1.44

Gateway IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

Concurrency Limits and Availability

Maximum concurrent tests: 10

☑ Set Scan Engine available for tests

3. The **Identity** portion of the **Edit Scan Engine** dialog box allows you to edit the **Scan Engine Description/Alias** you specified during Scan Engine registration; for more information, see *Registering a Scan Engine*.

4. The **Accessible IP Address Range** portion of the **Edit Scan Engine** dialog box allows you to edit ranges of IP addresses (or edit the name of a host machine), which define the extent to which the Scan Engine can scan/test applications on your network.

Example: You can exclude the IP address range `192.168.1.1` through `192.168.1.100` when performing a Discovery using this registered Scan Engine.

In the **Accessible IP Address Range** portion of the **Edit Scan Engine** dialog box, you can do the following:

- Select whether you want to **include** or **exclude** ranges of IP addresses (or IP addresses on host machines) by selecting **Include Range** or **Exclude Range**.

- Edit a machine host name in the **Hostname** field.
- Click the **Add** button to add the IP addresses of a host machine to the include or exclude list (depending whether you chose **Include Range** or **Exclude Range**, above).
- Edit an IP address range (for example, `192.168.1.1` through `192.168.1.100`) in the **From:** and **To:** fields.
- Click the **Add** button to add the IP addresses to the include or exclude list (depending whether you chose **Include Range** or **Exclude Range**, above).

Hint: To remove an IP address range from either the include or exclude list, highlight the range, then click the **Remove** button.

5. The **Concurrency Limits and Availability** portion of the **Edit Scan Engine** dialog box allows you to modify the maximum concurrent tests that may be performed on the Scan Engine, and to specify whether the Scan Engine is available for Penetration Test, Audit, and Discovery Jobs.

In the **Maximum concurrent tests:** field, you can enter the maximum number of concurrent Jobs (for Discovery, Penetration Tests, and Audits only) the Scan Engine is allowed to run at the same time. The maximum value is `20` Jobs, although this great a value is **not** recommended.

Note: You can run an unlimited number of Report Jobs. Therefore, the value you enter in the Maximum concurrent tests: field only applies to Discovery, Penetration Tests, and Audits.

If you install a Scan Engine on:

- the *same* server as the DbProtect Console, the default **Maximum concurrent tests:** value is `3` (i.e., the Scan Engine can run a maximum of three Discoveries, Penetration Tests, and Audits concurrently)
- a *remote* server, the default **Maximum concurrent tests:** value is `10` (i.e., the Scan Engine can run a maximum of 10 Discoveries, Penetration Tests, and Audits concurrently).

Hint: Depending on the capacity of your local or remote Scan Engine server, you can increase or decrease the **Maximum concurrent tests:** value, accordingly.

For example, if your Scan Engine is installed on a powerful server with multiple CPUs and several gigabytes of RAM, you can probably *increase* the default **Maximum concurrent tests:** value. However, if your Scan Engine server is not especially powerful, or is installed on a virtual machine (VM), and you notice a decrease in performance, you may instead want to *decrease* the default **Maximum concurrent tests:** value.

Also, you can check **Set Scan Engine available for tests** to specify whether the Scan Engine is available for test. If unchecked, you can't use this Scan Engine for tests.

6. Click the **Save** button to save your edited, registered Scan Engine values.

Your edited, registered Scan Engine values are saved.

Configuring the properties of a Scan Engine

If you are an administrator, DbProtect Vulnerability Management allows you to configure the advanced **properties** of a registered Scan Engine, e.g., hide/display cracked User passwords, network and Discovery parameters, password parameters, etc.

This topic consists of the following sub-topics:

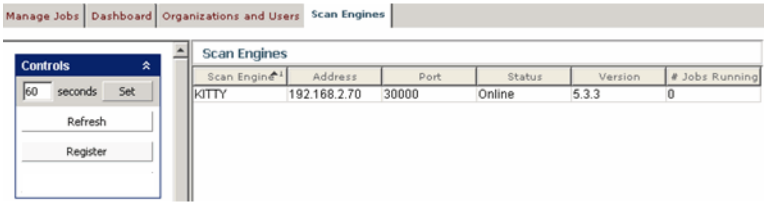
- *Displaying the Properties branches*
- *Understanding the Properties branches.*

DISPLAYING THE PROPERTIES BRANCHES

To display the **Properties** branches:

1. Do one of the following to display the **Scan Engines** page:

- Choose **Admin** > **Scan Engines** from the menu
- Click the **Scan Engines** tab.



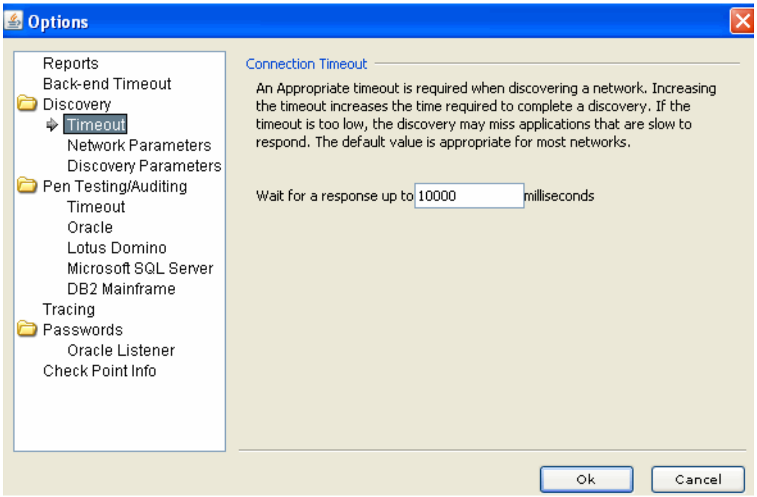
Scan Engines

Scan Engine	Address	Port	Status	Version	# Jobs Running
KITTY	192.168.2.70	30000	Online	5.3.3	0

FIGURE: **Scan Engines** page

2. Right click a Scan Engine (in the **Scan Engines** portion of the **Scan Engines** page) and choose **Properties**.

The **Options** dialog box displays the **Properties** branches.



An Appropriate timeout is required when discovering a network. Increasing the timeout increases the time required to complete a discovery. If the timeout is too low, the discovery may miss applications that are slow to respond. The default value is appropriate for most networks.

Wait for a response up to 10000 milliseconds

FIGURE: **Options** dialog box

UNDERSTANDING THE PROPERTIES BRANCHES

The following table explains the **Properties** branches:

Branch	Description
Backend Timeout	This branch allows you to enter a **Command Timeout** (in seconds), which specifies the maximum number of seconds the Scan Engine wait for a SQL command to complete. This is only for SQL commands that have been executed against its backend database. In order for this value to take effect, restart the Scan Engine. Changing this value may result in unpredictable Scan Engine behavior. Specify zero seconds for infinite timeout.
Reports	Some Audits and Penetration Tests crack passwords. This branch allows you to: • hide cracked User passwords in DbProtect Vulnerability Management Reports using *****, then check the **Hide Cracked Passwords** checkbox • display cracked User passwords in DbProtect Vulnerability Management Reports, then uncheck the **Hide Cracked Passwords** checkbox.

Branch	Description
Discovery	This branch allows you to change the Scan Engine Discovery parameters. This tab consists of three sub-branches: • **Timeout.** This sub-branch allows you to specify the amount of time the Scan Engine should wait before generating a timeout error during a Discovery. • **Network Parameters.** This sub-branch allows you to specify the delay and concurrent number of IP addresses for the Scan Engine. Delay is the amount of time the Scan Engine waits between sending packets out to the network. The concurrent number IP addresses deals with how many IP addresses to Discover against at the same time. When the limit is reached, the Scan Engine pauses until responses come back from the previously-Discovered IPs. • **Discovery Parameters.** This sub-branch allows you to select an option to **Check responsive ports even if IP address is not responsive**. If unchecked (default), DbProtect Vulnerability Management probes one port (for each IP address) to determine if the machine is responsive. If the machine is **responsive**, Discovery probes all ports for the IP address to scan applications. If the machine is **unresponsive**, Discovery ends for this IP address. DbProtect Vulnerability Management does **not** probe the rest of the ports for this IP address. If checked, DbProtect Vulnerability Management probes all ports of each IP address to scan applications.

Branch	Description
Pen Testing/Auditing	This branch allows you to set the parameters for use during a Penetration Test or Audit. This branch consists of six sub-branches. • **Timeout.** Allows the User to configure the timeout period between checks before generating a timeout error. • **Oracle.** This branch also allows you to select the **OPatch data collection method**. You can select: - **Use Java Method**. This method uses existing Java configured on the target database server to collect the OPatch data. - **Use OS** (Operating System) **Method** (default). This method detects if the Oracle CPU has been applied to your Oracle database. This method requires you to supply OS credentials, in addition to a valid database account. For more information, see *Appendix D: Oracle Critical Patch Update Detection*. • **Lotus Notes/Domino.** Reset the Lotus Notes/Domino Groupware session after a specified number of connections has been made. This will free up cached memory used by the Lotus Notes/Domino APIs. **Note:** DbProtect Vulnerability Management does **not** perform Audits on Lotus Notes/Domino applications. • **Microsoft SQL Server.** -**Attempt to use Windows Authentication when performing a Pen Test on Microsoft SQL Server.** Uncheck to force the Scan Engine to skip this step, which enhances information gathering. -**Connect to Microsoft SQL Servers via Named Pipes.** Check to force the Scan Engine to use named pipes. • **DB2 Mainframe.** Allows you to select which security option DbProtect Vulnerability Management should use to authenticate a DB2 mainframe application. You can select: -**Use authentication value in server's DBM configuration** -**Client authentication** -**Server authentication** -**Server authentication with encryption** -**DDCS authentication** -**DDCS authentication with encryption**.

Branch	Description
Tracing	This branch allows you to enable tracing, which collects details about the Scan Engine tasks for the purposes of troubleshooting with Application Security, Inc. Technical Support. You can set the tracing level to: • **Debug** • **Normal** • **Warning** • **Error** • **Critical** • **Off**. **Note:** Application Security, Inc. recommends you turn the tracing level to **Off**, unless otherwise instructed by Application Security, Inc. Technical Support.
Passwords	This branch allows you to set the following Scan Engine password parameter: • **Oracle Listener.** This tab records a default value to try as the Oracle Listener password, when DbProtect Vulnerability Management encounters an Oracle Listener with a password set on it.

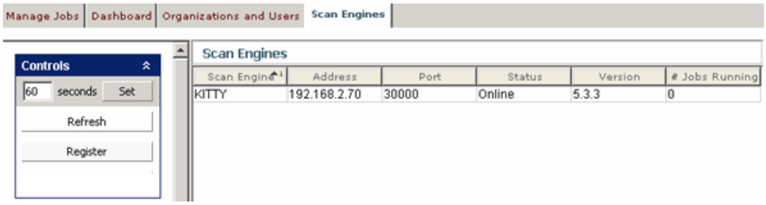
Branch	Description
Check Point Info	The Scan Engine allows you to forward Penetration Test and Audit results from an Scan Engine to a Check Point Event Logging Server (Check Point SmartView Tracker). This branch allows you to send a log entry for every vulnerability a Check Point Event Logging Server. This branch consists of the following fields: • **Enable Check Point SmartCenter Server logging.** Check to enable logging capability. • **Authentication Type.** Allows you to specify an authentication method. Check Point provides several methods. Application Security, Inc. recommends SSLCA for log sending. • **Target Server IP Address.** Allows you to specify the server machine where Check Point SmartCenter Server is installed. • **Target Server Port.** Allows you to specify the port on the server machine where the Check Point ELA Server is enabled. • **Target SIC Name.** This field allows you enter the Secure Internal Communication (SIC) name of your Check Point SmartCenter Server. SIC is Check Point's proprietary internal communication method for the components within a Next Generation (NG) Check Point System. In order for the Scan Engine to communicate with a Check Point SmartCenter server in SSLCA mode, the SIC name of the Check Point SmartCenter Server is required. • **Client SIC Name.** For SSLCA authentication, Check Point requires each client to be registered on Check Point SmartCenter Console. This field allows you to add the computer where the Scan Engine is installed. • **P12 Key File.** Allows you to enter the location of the `.p12` file generated after you execute the `opsec_pull_certificate.exe` command. You can click the **Browse** button to search for the `.p12` file on your computer.

Setting the Scan Engine refresh rate

Scan Engines refresh automatically according to whatever time interval (in seconds) you set on the **Scan Engines** page (explained in this topic). Or you can manually refresh the Scan Engines from the **Scan Engines** page; for more information, see *Manually refreshing data on the Manage Jobs Page*.

To set the Scan Engine refresh rate:

1. Do one of the following to display the **Scan Engines** page:
   - Choose **Admin > Scan Engines** from the menu
   - Click the **Scan Engines** tab.



60 seconds

Scan Engines

Scan Engine	Address	Port	Status	Version	# Jobs Running
KITTY	192.168.2.70	30000	Online	5.3.3	0

FIGURE: **Scan Engines** page

2. Edit the Scan Engine refresh rate in the **seconds** field and click the **Set** button.

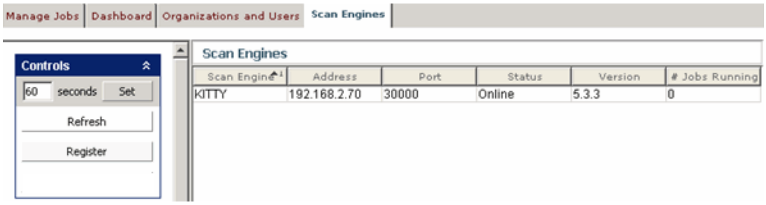
DbProtect Vulnerability Management changes your Scan Engine refresh rate.

Manually refreshing the Scan Engine

You can manually refresh the Scan Engines from the **Scan Engines** page (explained in this topic). Normally, Scan Engines refresh automatically according to the time interval (in seconds) specified on the **Scan Engines** page; for more information, see *Setting the Scan Engine refresh rate*.

To manually refresh the Scan Engine:

1. Do one of the following to display the **Scan Engines** page:
   - Choose **Admin > Scan Engines** from the menu
   - Click the **Scan Engines** tab.



Scan Engines

Scan Engine	Address	Port	Status	Version	# Jobs Running
KITTY	192.168.2.70	30000	Online	5.3.3	0

FIGURE: **Scan Engines** page

2. Click the **Refresh** button in the **Controls** portion.

DbProtect Vulnerability Management refreshes the status of your Scan Engines.

Working with Policies

This chapter consists of the following topics:

What are Policies?

Policies are sets of security checks used by DbProtect Vulnerability Management to perform Penetration Tests and Audits. DbProtect Vulnerability Management includes built-in Policies which you can use "out of the box". For more information, see *Built-In Audit Policies* and *Built-In Penetration Test Policies*.

Built-In Audit Policies

DbProtect Vulnerability Management includes the following built-in Audit Policies.

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

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

- **Download.** A default Policy that allows an evaluator the chance to test specific checks.
- **MITS.** This Policy is structured following CoBIT, ISO, and NIST standards and is recommended for use in a MITS compliance assessment.
- **Passwords.** This Policy is used to Audit password strength and settings.
- **DISA-STIG Database Security Configuration.** This policy has been created with guidance of the configuration parameters outlined by the DISA-STIG for SQL Server and Oracle only.
- **Authorization.** This Policy is used to Audit permissions and access controls.
- **PCI Data Security Standard.** This Policy is structured following the PCI Data Security Standard and is recommended for use in a compliance assessment.
- **Sarbanes-Oxley.** This policy is structured following CoBIT and ISO 17799 standards and is recommended for use in a Sarbanes-Oxley compliance assessment.
- **Strict.** Provides a maximum level of security with a significant impact on functionality. This Policy is much more restrictive than required by most applications. Usually used by only the most top secret applications.
- **Massachusetts 201 CMR.** TBA
- **MiFID.** This Policy is structured for use in a Markets in Financial Instruments Directive (MiFID) compliance assessment.
- **EU Data Protection Directive.** This Policy is structured following EU 95/46/EC standards and is recommened for use in a EU Data Protection Directive compliance assessment.
- **Gramm-Leach-Bliley Act.** This Policy is structured following Gramm-Leach-Bliley Act (GLBA) standards and is recommened for use in a GLBA compliance assessment.
- **HIPAA.** This Policy is structured following NIST standards and best practices for database security and is recommended for use in a HIPAA compliance assessment.

Built-In Penetration Test Policies

DbProtect Vulnerability Management includes the following built-in Penetration Test Policies.

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

- **HIPAA.** This Policy is structured following NIST standards and best practices for database security and is recommended for use in a HIPAA compliance assessment.
- **PCI Data Security Standard.** This Policy is structured following the PCI Data Security Standard and is recommended for use in a compliance assessment.

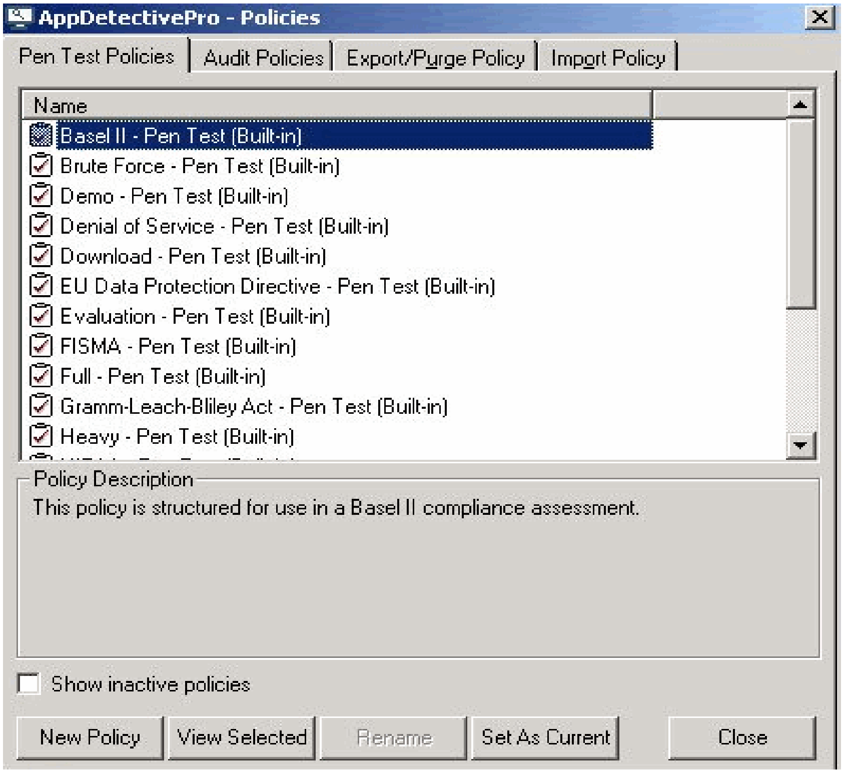
- **Gramm-Leach-Bliley Act.** This Policy is structured following Gramm-Leach-Bliley Act (GLBA) standards and is recommened for use in a GLBA compliance assessment.
- **Demo.** Runs a demonstration of DbProtect Vulnerability Management features. This demo runs quickly, returning a maximum number of vulnerabilities in a short period of time.
- **Sarbanes-Oxley.** This Policy is structured following CoBIT and ISO 17799 standards and is recommended for use in a Sarbanes-Oxley compliance assessment.
- **Evaluation.** Performs a Penetration Test using basic checks, allowing you to evaluate DbProtect Vulnerability Management.
- **FISMA.** This Policy is structured following NIST standards and is recommended for use in a FISMA compliance assessment.
- **Safe.** Runs safe checks only. This Policy does not perform Brute Force or Denial of Service checks that cannot be run safely.
- **Basel II.** This Policy is structured for use in a Basel II compliance assessment.
- **Full.** Performs a complete Penetration Test of your application using all available checks.
- **EU Data Protection Directive.** This Policy is structured following EU 95/46/EC standards and is recommened for use in a EU Data Protection Directive compliance assessment.
- **Brute Force.** Performs a Penetration Test designed to test the strength of your applications' passwords as well as other mechanisms that may be breached by brute force methods.
- **Heavy.** Performs a detail-level Penetration Test on your applications. Adds a heavy amount of usage. May take more than one hour to run.
- **Download.** A default Policy that allows you to test specific checks.
- **MiFID.** This Policy is structured for use in a Markets in Financial Instruments Directive (MiFID) compliance assessment.
- **Light.** Performs a first-level Penetration Test on your application. Adds a minimal amount of usage. Should take less than one minute to run.
- **Medium.** Performs a second level Penetration Test on an application. Adds a moderate amount of usage on the application. Should take less than 15 minutes to run.
- **Denial of Service.** This Policy checks if your applications are vulnerable to any Denial of Service (DoS) attacks by looking at the version and platform of the database or listener.

Viewing a Policy

DbProtect Vulnerability Management allows you to view a Policy (for either a Penetration Test or an Audit), including what security checks it contains.

To view a Policy:

1. Choose **Start > Programs > AppSecInc > DbProtect > Policy Editor** to display the **Policies** dialog box.



- ☑ Basel II - Pen Test (Built-in)
- ☑ Brute Force - Pen Test (Built-in)
- ☑ Demo - Pen Test (Built-in)
- ☑ Denial of Service - Pen Test (Built-in)
- ☑ Download - Pen Test (Built-in)
- ☑ EU Data Protection Directive - Pen Test (Built-in)
- ☑ Evaluation - Pen Test (Built-in)
- ☑ FISMA - Pen Test (Built-in)
- ☑ Full - Pen Test (Built-in)
- ☑ Gramm-Leach-Bliley Act - Pen Test (Built-in)
- ☑ Heavy - Pen Test (Built-in)

Policy Description

This policy is structured for use in a Basel II compliance assessment.

□ Show inactive policies

FIGURE: **Policies** dialog box

2. Click the **Pen Test Policies** or **Audit Policies** tab.
3. Select a Policy.
4. Click the **View Selected** button to display the **Policy Editor**.
5. View which security checks are active within the chosen Policy. (Security checks with check marks next to them are **active**.)
6. Click an individual security check to display its detailed description.

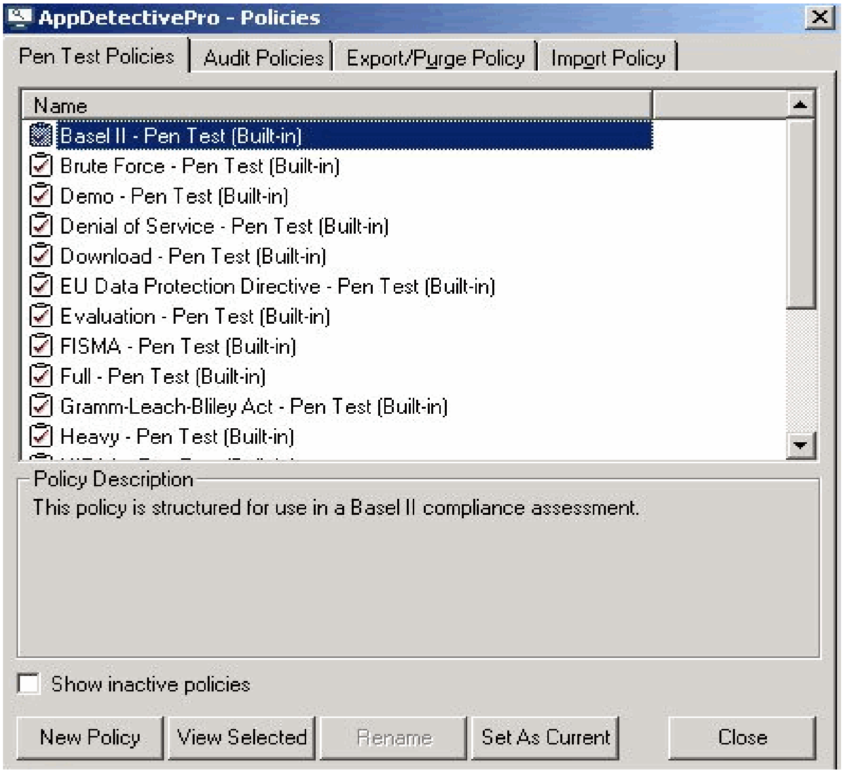
Creating a Policy

DbProtect Vulnerability Management allows you to create a Policy (for either a Penetration Test or an Audit), including what security checks it contains. This is known as a **User-defined Policy**.

Note: Some security checks allow you to customize your Policies by excluding individual checks (known as Exceptions). You can only add Exceptions to/ delete Exceptions from User-defined Policies. A check must be enabled in order to add/delete an Exception. For more information, see *Adding and deleting Exceptions*.

To create a Policy:

1. Choose **Start > Programs > AppSecInc > DbProtect > Policy Editor** to display the **Policies** dialog box.



☒ Basel II - Pen Test (Built-in)
☑ Brute Force - Pen Test (Built-in)
☑ Demo - Pen Test (Built-in)
☑ Denial of Service - Pen Test (Built-in)
☑ Download - Pen Test (Built-in)
☑ EU Data Protection Directive - Pen Test (Built-in)
☑ Evaluation - Pen Test (Built-in)
☑ FISMA - Pen Test (Built-in)
☑ Full - Pen Test (Built-in)
☑ Gramm-Leach-Bliley Act - Pen Test (Built-in)
☑ Heavy - Pen Test (Built-in)

Policy Description
This policy is structured for use in a Basel II compliance assessment.

□ Show inactive policies

FIGURE: **Policies** dialog box

2. Click the **Pen Test Policies** or **Audit Policies** tab.
3. Click the **New Policy** button to display the **Policy Editor**.
4. Activate security checks by checking the corresponding checkboxes.

Note: Optionally, some checks allow you to customize your Policies by excluding individual checks (known as **Exceptions**). You can only add Exceptions to/ delete Exceptions from User-defined Policies, **not** built-in Policies. A check **must** be enabled in order to add/delete an Exception. For more information, see *Adding and deleting Exceptions*.

5. Click the **Save** button on the toolbar to display the **Save New Policy** pop up.
6. Enter the new Policy name in the **Policy Name** field (required).
7. Enter the new Policy description in the **Policy Description** field (optional).
8. Click the **OK** button.

DbProtect Vulnerability Management saves your new Policy.

9. You **must** edit the permissions for each individual Organization and each individual User who is allowed to use this new Policy; for more information, see *Editing an Organization* and *Editing a User*, respectively.

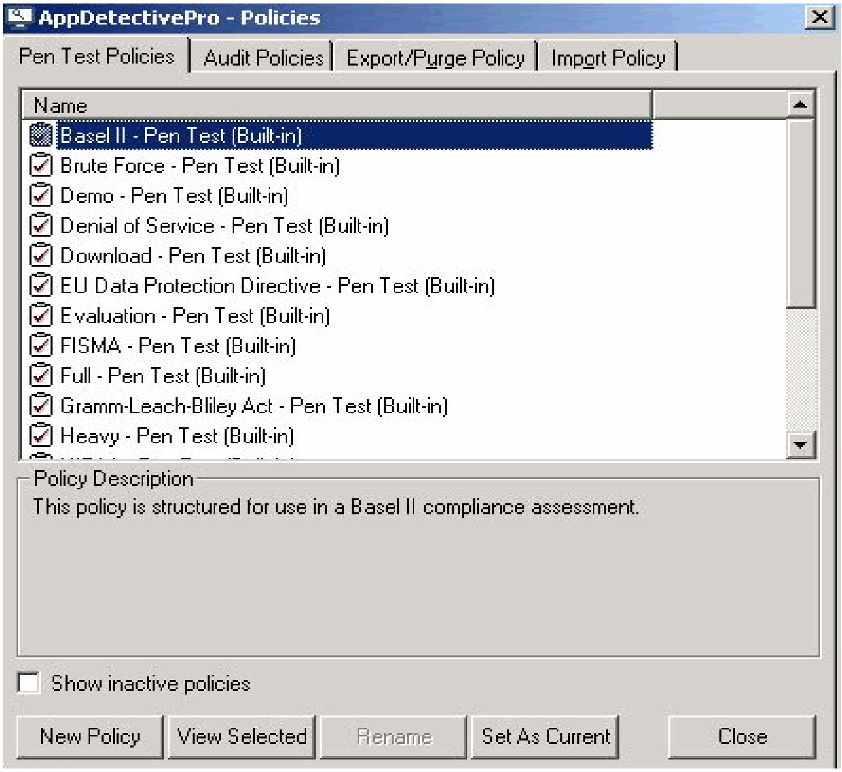
Editing a Policy

DbProtect Vulnerability Management allows you to edit a Policy.

Note: You **cannot** modify built-in Policies. However, you **can** edit a built-in Policy and perform a "save as" to save the edited Policy under a different name.

To edit a Policy:

1. Choose **Start > Programs > AppSecInc > DbProtect > Policy Editor** to display the **Policies** dialog box.



- Basel II - Pen Test (Built-in)
- Brute Force - Pen Test (Built-in)
- Demo - Pen Test (Built-in)
- Denial of Service - Pen Test (Built-in)
- Download - Pen Test (Built-in)
- EU Data Protection Directive - Pen Test (Built-in)
- Evaluation - Pen Test (Built-in)
- FISMA - Pen Test (Built-in)
- Full - Pen Test (Built-in)
- Gramm-Leach-Bliley Act - Pen Test (Built-in)
- Heavy - Pen Test (Built-in)

This policy is structured for use in a Basel II compliance assessment.

☐ Show inactive policies

FIGURE: **Policies** dialog box

2. Click the **Pen Test Policies** or **Audit Policies** tab.
3. Select a Policy.
4. Click the **View Selected** button to display the **Policy Editor**.
5. Activate/deactivate security checks within the chosen Policy by checking/unchecking the checkboxes, respectively.

6. Optionally, some checks allow you to customize your Policies by excluding individual checks (known as **Exceptions**). You can only add Exceptions to/ delete Exceptions from User-defined Policies, **not** built-in Policies. A check **must** be enabled in order to add/delete an Exception. For more information, see *Adding and deleting Exceptions*.

7. Save the edited Policy. If the Policy is a:

   - **built-in Policy**, then click the **Save** button to save the edited Policy
   - **User-defined Policy**, then click the **Save As** button to save the edited Policy under a different name.

8. You **must** edit the permissions for each Organization and each individual User who is allowed to use the edited Policy; for more information, see *Editing an Organization* and *Editing a User*, respectively.

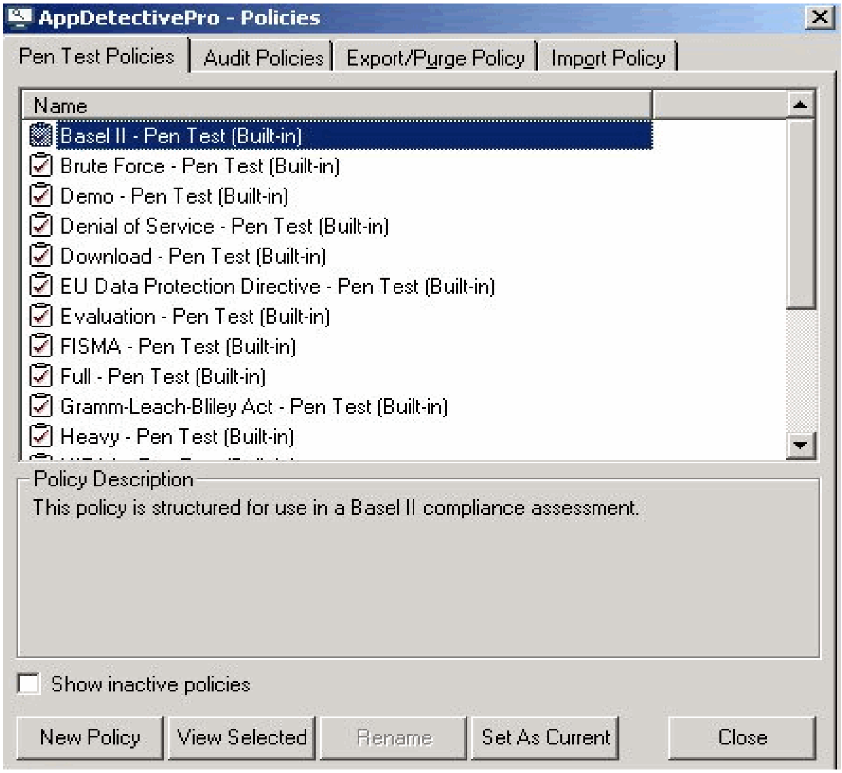
Renaming a Policy

DbProtect Vulnerability Management allows you to rename a Policy.

Note: You **cannot** modify Built-in Policies.

To rename a Policy:

1. Choose **Start > Programs > AppSecInc > DbProtect > Policy Editor** to display the **Policies** dialog box.



- ☑ Basel II - Pen Test (Built-in)
- ☑ Brute Force - Pen Test (Built-in)
- ☑ Demo - Pen Test (Built-in)
- ☑ Denial of Service - Pen Test (Built-in)
- ☑ Download - Pen Test (Built-in)
- ☑ EU Data Protection Directive - Pen Test (Built-in)
- ☑ Evaluation - Pen Test (Built-in)
- ☑ FISMA - Pen Test (Built-in)
- ☑ Full - Pen Test (Built-in)
- ☑ Gramm-Leach-Bliley Act - Pen Test (Built-in)
- ☑ Heavy - Pen Test (Built-in)

Policy Description
This policy is structured for use in a Basel II compliance assessment.

□ Show inactive policies

FIGURE: **Policies** dialog box

2. Click the **Pen Test Policies** or **Audit Policies** tab.
3. Select the Policy you want to rename.
4. Click the **Rename** button to display the **Rename Policy** pop up.
5. Enter the new Policy name.
6. Click the **OK** button.

A pop up displays and informs you if the rename was successful.

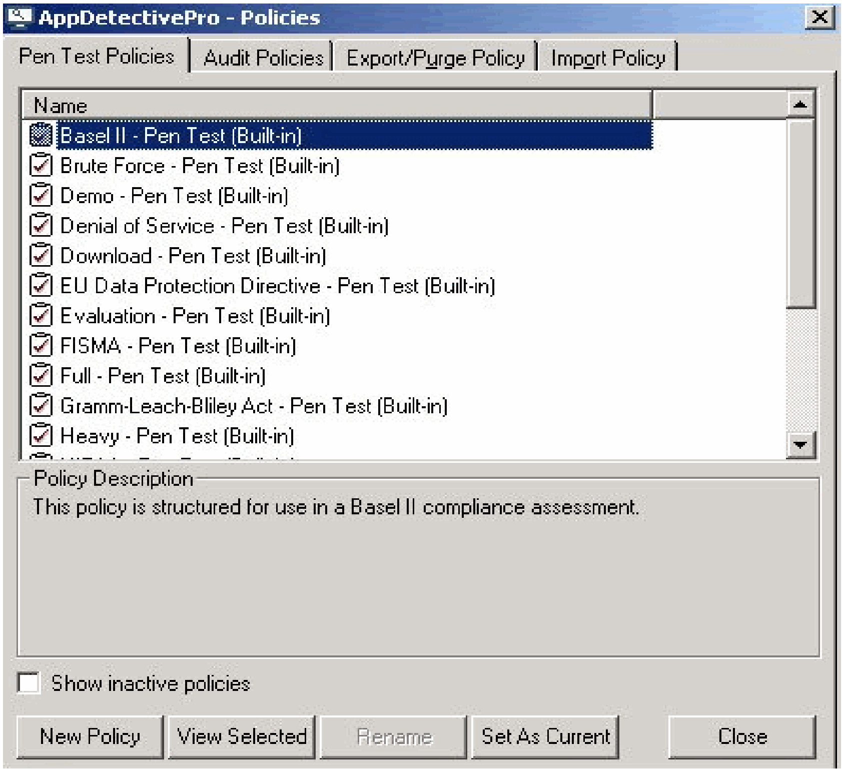
7. Click the **OK** button.

Searching Policies

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

To search Policies:

1. Choose **Start > Programs > AppSecInc > DbProtect > Policy Editor** to display the **Policies** dialog box.



Basel II - Pen Test (Built-in)
☑ Brute Force - Pen Test (Built-in)
☑ Demo - Pen Test (Built-in)
☑ Denial of Service - Pen Test (Built-in)
☑ Download - Pen Test (Built-in)
☑ EU Data Protection Directive - Pen Test (Built-in)
☑ Evaluation - Pen Test (Built-in)
☑ FISMA - Pen Test (Built-in)
☑ Full - Pen Test (Built-in)
☑ Gramm-Leach-Bliley Act - Pen Test (Built-in)
☑ Heavy - Pen Test (Built-in)

This policy is structured for use in a Basel II compliance assessment.

□ Show inactive policies

FIGURE: **Policies** dialog box

2. Click the **Pen Test Policies** or **Audit Policies** tab.
3. Select a Policy.
4. Click the **View Selected** button.
5. Enter text to search for. If you have a specific CVE number, enter it as the target string.
6. DbProtect Vulnerability Management displays your search results in the **Policy Search** portion of the **Policy Editor**.

7. Click a search result to display a description of the security check, as well as its location within the **Policy Editor**.
8. Check the checkbox to activate it.

Adding and deleting Exceptions

DbProtect Vulnerability Management allows you to customize your Policies by excluding individual checks (known as **Exceptions**). You can only add Exceptions to/delete Exceptions from User-defined Policies, **not** built-in Policies. A check **must** be enabled in order to add/delete an Exception. There are two ways to add an Exception to a user-defined Policy. You can:

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

This topic consists of the following sub-topics:

- *Exception examples*
- *Adding an Exception*
- *Deleting an Exception.*

EXCEPTION EXAMPLES

Below is an example for creating an Exception file for the Oracle check **"Easily-guessed database password"**:

- `Username=John,Password=johnspass`
- `Username=Bob,"Password=bobs,pass"`
- `Username=Jim,"Password=jims""pass"`
- `Password=12345`

As a result, DbProtect Vulnerability Management will **not** report "Easily-guessed database password" vulnerabilities if:

- John has an easily-guessed password and it is `johnspass`
- Bob has an easily-guessed password and it is `bobs,pass`
- Jim has an easily-guessed password and it is `jims""pass`
- Any of the database accounts has an easily-guessed password and it is `12345`

To follow the CSV standard and allow a correct parsing:

- The `'Password=bobs,pass'` value is enclosed in double quotes because it contains a comma.
- The `'Password=jims"pass'` value is enclosed in double quotes because it contains a double quote. The inner double quote has been duplicated.

Below is an example of creating an Exception `.txt` or `.csv` file for the MSSQL check **"Blank password"**:

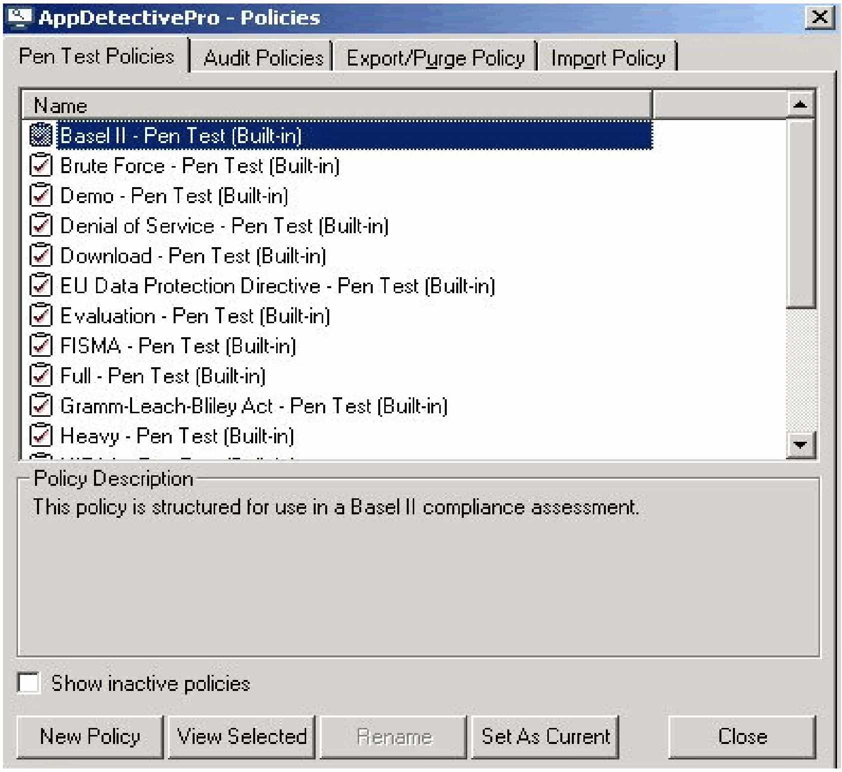
- `Login=John`
- `Login=Bob`
- `Login=Jim`

If John, Bob or Jim have blank passwords, DbProtect Vulnerability Management will **not** report "Blank password" check vulnerabilities.

ADDING AN EXCEPTION

To add an Exception:

1. Choose **Start > Programs > AppSecInc > DbProtect > Policy Editor** to display the **Policies** dialog box.



☑ Basel II - Pen Test (Built-in)
☑ Brute Force - Pen Test (Built-in)
☑ Demo - Pen Test (Built-in)
☑ Denial of Service - Pen Test (Built-in)
☑ Download - Pen Test (Built-in)
☑ EU Data Protection Directive - Pen Test (Built-in)
☑ Evaluation - Pen Test (Built-in)
☑ FISMA - Pen Test (Built-in)
☑ Full - Pen Test (Built-in)
☑ Gramm-Leach-Bliley Act - Pen Test (Built-in)
☑ Heavy - Pen Test (Built-in)

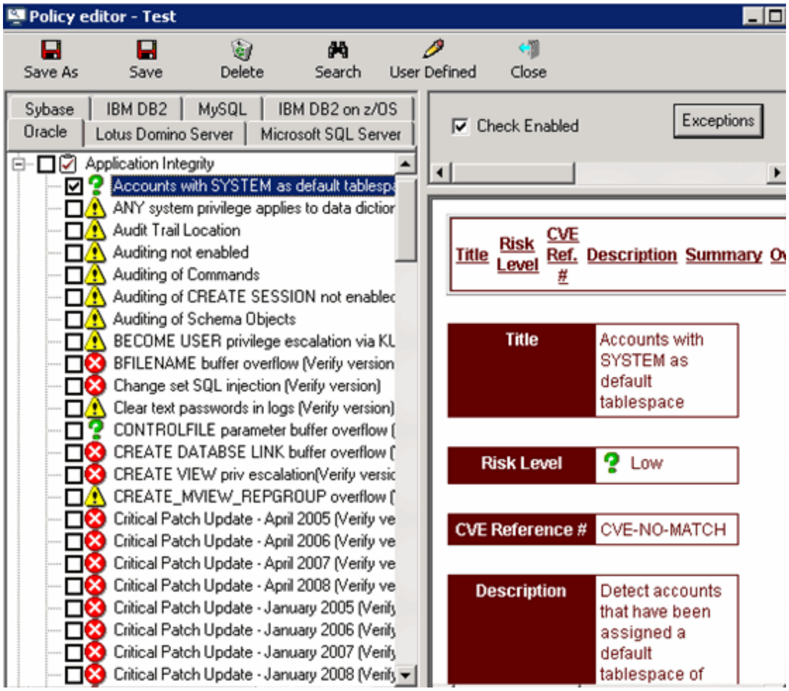
Policy Description
This policy is structured for use in a Basel II compliance assessment.

☐ Show inactive policies

FIGURE: **Policies** dialog box

2. Click the **Pen Test Policies** or **Audit Policies** tab.

3. Click the **New Policy** button or the **View Selected** button to display the **Policy Editor**.



☑ Check Enabled

□ ☑ Application Integrity

- ☑ ? Accounts with SYSTEM as default tablesp
- □ ⚠ ANY system privilege applies to data dictior
- □ ⚠ Audit Trail Location
- □ ⚠ Auditing not enabled
- □ ⚠ Auditing of Commands
- □ ⚠ Auditing of CREATE SESSION not enablec
- □ ⚠ Auditing of Schema Objects
- □ ⚠ BECOME USER privilege escalation via KL
- □ ⊗ BFILENAME buffer overflow (Verify version
- □ ⊗ Change set SQL injection (Verify version)
- □ ⚠ Clear text passwords in logs (Verify version)
- □ ? CONTROLFILE parameter buffer overflow (
- □ ⊗ CREATE DATABSE LINK buffer overflow (
- □ ⊗ CREATE VIEW priv escalation(Verify versic
- □ ⚠ CREATE_MVIEW_REPGROUP overflow (
- □ ⊗ Critical Patch Update - April 2005 (Verify ve
- □ ⊗ Critical Patch Update - April 2006 (Verify ve
- □ ⊗ Critical Patch Update - April 2007 (Verify ve
- □ ⊗ Critical Patch Update - April 2008 (Verify ve
- □ ⊗ Critical Patch Update - January 2005 (Verif
- □ ⊗ Critical Patch Update - January 2006 (Verif
- □ ⊗ Critical Patch Update - January 2007 (Verif
- □ ⊗ Critical Patch Update - January 2008 (Verif

Title	Risk Level	CVE Ref. #	Description	Summary	O

Title	Accounts with SYSTEM as default tablespace
Risk Level	? Low
CVE Reference #	CVE-NO-MATCH
Description	Detect accounts that have been assigned a default tablespace of

FIGURE: Policy Editor

4. Select a Policy.

5. View which security checks are active within the chosen Policy. (Security checks with check marks next to them are **active**.)

Some checks allow you to click an **Exceptions** button and customize your Policies by excluding individual checks (known as Exceptions). You can only add Exceptions to/ delete Exceptions from User-defined Policies, **not** built-in Policies. A check **must** be enabled in order to add/delete an Exception.

Note: You **cannot** modify built-in Policies. However, you **can** edit a built-in Policy and choose "save as" to save the edited Policy under a different name. For more information, see *Editing a Policy*.

To add an Exception, check the **Check Enabled** checkbox and click the **Exceptions** button.

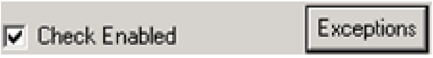
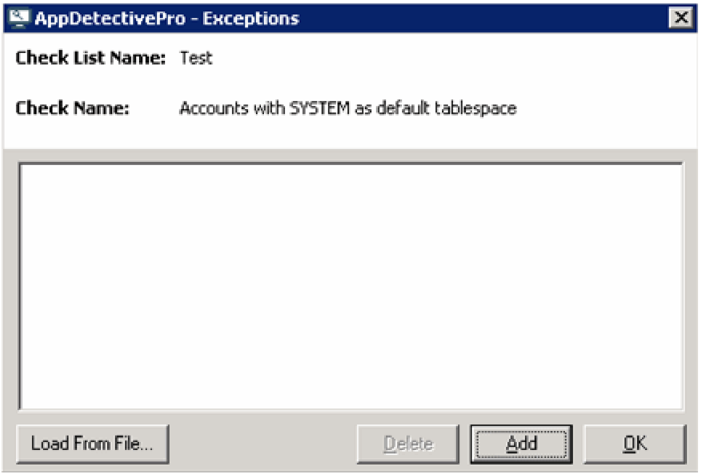


FIGURE: **Check Enabled** checkbox and **Exceptions** button

6. The **Exceptions** pop up displays.



Check List Name: Test

Check Name: Accounts with SYSTEM as default tablespace

FIGURE: **Exceptions** pop up

If you want to:

- manually create an Exception, go to Step 7
- load a file of Exceptions (from a `.txt` or `.csv` file), go to Step 8.

7. Manually create an Exception.

Click the **Add** button on the **Exceptions** dialog box to display the **Create Exception** pop up, which allows you to add:

- single Exceptions, e.g., `Login=Admin`
- Exceptions with an `AND` clause when more than one **Parameter Name** is available in the **Parameter Name** drop-down list, e.g., `Login=Admin`, `Password=admin123`, etc.
- Exceptions with an `AND/OR` clause, e.g., `Login=Admin`, `Password=admin123`, `Password=Admin`, etc.

To add an Exception with an `AND` clause:

- Use the **Parameter Name** drop-down to select a parameter and a enter a value in the **Parameter Value** field, e.g., `Login=Admin`.
- Use the **Parameter Name** drop-down to select a different parameter and enter a value in the **Parameter Value** field, e.g., `Password=admin123`.
- Click the **OK** button.

To add an Exception with an AND/OR clause:

- Add an Exception with an AND clause. Use the **Parameter Name** drop-down to select a parameter and a enter a value in the **Parameter Value** field, e.g., Login=Admin.
- Use the **Parameter Name** drop-down to select a different parameter and enter a value in the **Parameter Value** field, e.g., Password=admin123.
- Click the **OK** button.
- Immediately after adding that Exception, use the **Parameter Name** drop-down to select the parameter you want to use for the OR clause, e.g., Password=Admin.
- Click the **OK** button and go to Step 6.

8. Load a file of Exceptions (from a .txt or .csv file).

Click the **Load From File** button on the **Exceptions** dialog box to display the **Load Exceptions from file** pop up, which allows you to select a valid.txt or .csv file of Exceptions.

The content of the file, line by line, **must** adhere to the following syntax and rules:

```
PairNameValue[[,<PairNameValue>][,...]]

[PairNameValue[[,<PairNameValue>][,...]]]

[...]

<PairNameValue> ::= <ParamName>=<ParamValue>
```

<ParamName>: must be an existing parameter in the ParamaterNames table for the check.

<ParamValue>: cannot be empty.

If <ParamName> or <ParamValue> contains commas (,) or double quotes ("), you must enclose <PairNameValue> between double quotes (") and you replace the contained double quotes (if they exist) with (""), as follows:

- If <ParamName> or <ParamValue> contains commas:
  `Login=Admin,"Password=Pass,word"`
- If <ParamName> or <ParamValue> contain double quotes:
  `"Login=""Admin""",Password=mypwd`

Click the **OK** button and go to Step 9.

9. Click the **Save** button on the toolbar to display the e **Save New Policy** pop up.

10. Enter the new Policy name in the **Policy Name** field (required).

11. Enter the new Policy description in the **Policy Description** field (optional).

DELETING AN EXCEPTION

To delete an Exception:

1. Click the enabled check where you want to delete an Exception.
2. Click the **Exceptions** button.
3. Select the Exception you want to delete.
4. Click the **Delete** button.
5. Click the **Yes** button to verify the delete.

Importing a Policy

DbProtect allows you to **import** a Policy using AppDetectivePro (which is installed automatically during your installation of DbProtect).

Alternately, you can use the standalone **DbProtect Migration Tool** to migrate Session data from a **source** (an AppDetectivePro database) to a **destination** (the DbProtect Vulnerability Management database). When you do so, DbProtect Vulnerability Management automatically inherits all Policies associated with the migrated Session(s); for more information, see *Appendix E: Importing Session Data with the DbProtect Import Utility*.

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

To import a Policy using AppDetectivePro:

1. Choose **Start > Programs > AppSecInc > DbProtect > Policy Editor** to display the **Policy Editor**.

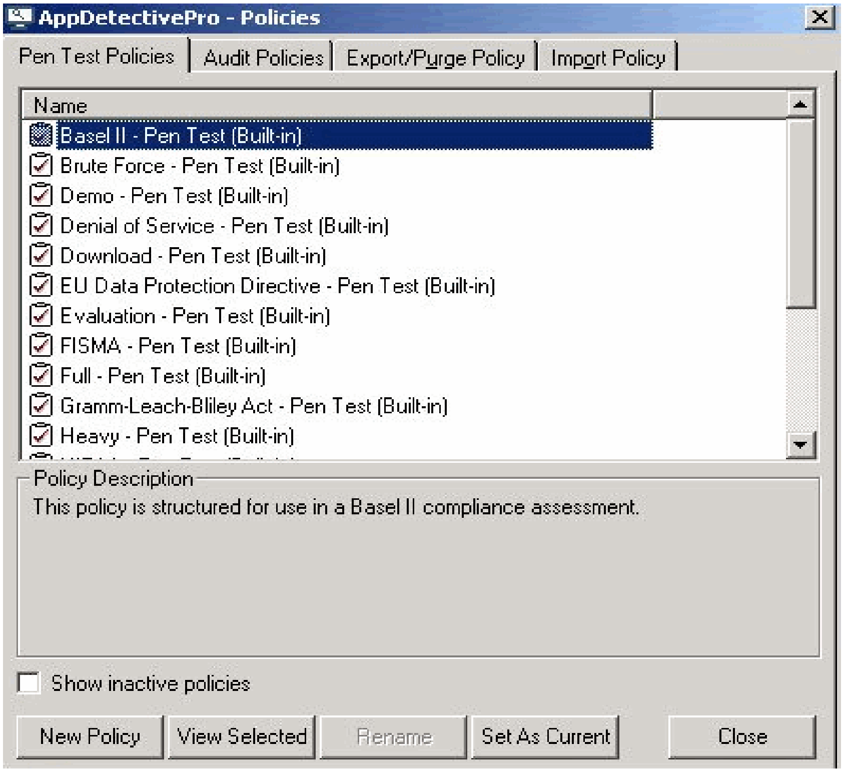

AppDetectivePro - Policies
Pen Test Policies
Audit Policies
Export/Purge Policy
Import Policy
Name
Basel II - Pen Test (Built-in)
Brute Force - Pen Test (Built-in)
Demo - Pen Test (Built-in)
Denial of Service - Pen Test (Built-in)
Download - Pen Test (Built-in)
EU Data Protection Directive - Pen Test (Built-in)
Evaluation - Pen Test (Built-in)
FISMA - Pen Test (Built-in)
Full - Pen Test (Built-in)
Gramm-Leach-Bliley Act - Pen Test (Built-in)
Heavy - Pen Test (Built-in)
Policy Description
This policy is structured for use in a Basel II compliance assessment.
□ Show inactive policies
New Policy
View Selected
Rename
Set As Current
Close

FIGURE: Policy Editor

2. Click the **Import Policy** tab.
3. Click the **Set Import File** button to display the **Set Import File** dialog box.
4. Specify the path and file name of the AppDetectivePro database file (`.adb`).
5. Click the **Import** button.

A pop up displays, notifying you AppDetectivePro has imported your Policy data as an AppDetectivePro database file (`.adb`). The imported Policy is now available.

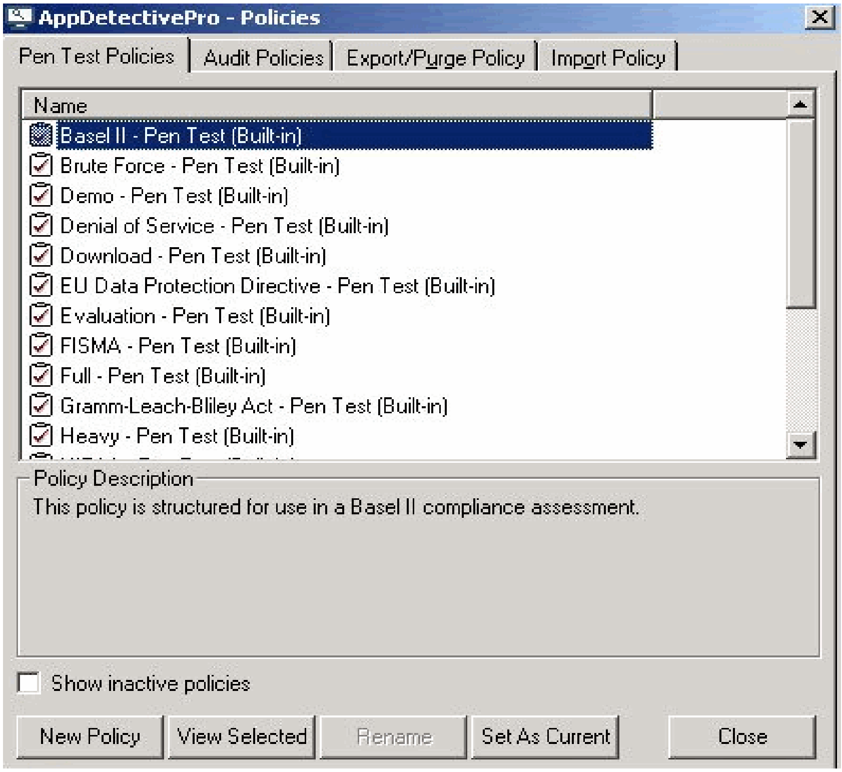
Exporting a Policy

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

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

To export a Policy:

1. Choose **Start > Programs > AppSecInc > DbProtect > Policy Editor** to display the **Policy Editor**.



- ▨ Basel II - Pen Test (Built-in)
- ☑ Brute Force - Pen Test (Built-in)
- ☑ Demo - Pen Test (Built-in)
- ☑ Denial of Service - Pen Test (Built-in)
- ☑ Download - Pen Test (Built-in)
- ☑ EU Data Protection Directive - Pen Test (Built-in)
- ☑ Evaluation - Pen Test (Built-in)
- ☑ FISMA - Pen Test (Built-in)
- ☑ Full - Pen Test (Built-in)
- ☑ Gramm-Leach-Bliley Act - Pen Test (Built-in)
- ☑ Heavy - Pen Test (Built-in)

Policy Description

This policy is structured for use in a Basel II compliance assessment.

□ Show inactive policies

FIGURE: **Policy Editor**

2. Click the **Export/Purge Policy** tab.
3. Check the Policies you want to export.
4. Click the **Export** button.

A pop up displays, notifying you AppDetectivePro has exported your Policy data as an AppDetectivePro database file (`.adb`). The exported Policy is now available.

Working with Credential Profiles and User Credential Files

This chapter consists of the following topics:

- *What is a Credential Profile?*
- *What is a User Credentials File?*
- *Understanding the Credential Profile hierarchy*
- *Credential Profiles and User role privileges*
- *Creating a Credential Profile*
- *Setting and testing your database and operating system credentials*
- *Editing a Credential Profile*
- *Removing a Credential Profile*
- *Setting a Credential Profile as an Organizational default*
- *Removing applications from a Credential Profile*
- *Deleting credentials from a Credential Profile*
- *Importing a User Credentials File*
- *Exporting a User Credentials File*.

What is a Credential Profile?

DbProtect Vulnerability Management allows you to create, view, and modify a **Credential Profile** which contains the specific authentication details DbProtect Vulnerability Management uses to authenticate to a target application or operating system for the purpose of performing an Audit; for more information, see *What is an Audit?*

You can modify Credential Profiles at any of the following hierarchical levels: **network**, **subnet**, **host**, or **application**.

Important: DbProtect Vulnerability Management displays *different Audit credential parameters* at each level, i.e., network, subnet, host, and application. For more information, see *Setting and testing your database and operating system credentials*.

What is a User Credentials File?

The **User Credentials File** includes the administration User's operating system User name, operating system password, system privileges, database username, and database password.

You **must** provide database and operation system authentication credentials in order to run an Audit Job. If you don't use a Credential Profile, you can import a properly-formatted User Credentials File. For more information, see *Appendix A: Creating a User Credentials File*.

All Users (except View Users) can import a User Credentials File. Super Admin Users can also export a User Credentials File.

For more information on:

- importing a User Credentials File, see *Importing a User Credentials File*
- exporting a User Credentials File, see *Exporting a User Credentials File*.

Understanding the Credential Profile hierarchy

As shown below, Credential Profiles are hierarchical.

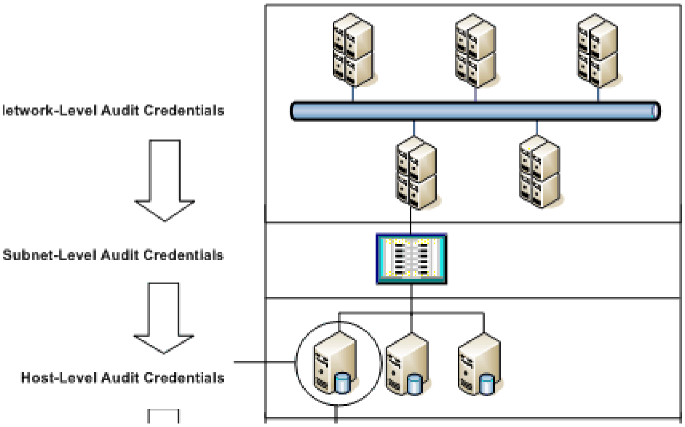

letwork-Level Audit Credentials
Subnet-Level Audit Credentials
Host-Level Audit Credentials

FIGURE: Credential profile hierarchy (conceptual diagram)

Specifically, when you set a Credential Profile for:

- **a network**, then all underlying **subnets**, **hosts**, and **applications** inherit the network's credentials
- **a subnet**, then all underlying **hosts** and **applications** inherit the subnet's credentials
- **a host**, then all underlying **applications** inherit the host's credentials
- **an application**, then the credential settings apply *only* to the application.

The applications specified in your Credential Profile must *exactly* match the applications specified in your Audit Job, at the application type level. For example, if you specify subnet `192.168.1.x` in your Credential Profile, and attempt to apply this Credential Profile to an Audit Job that does **not** include subnet `192.168.1.x` in its list of applications to Audit, then the Audit Job will fail. However, if the Audit Job includes the entire **network** in its list of applications to Audit, then this Credential Profile will work, because in the credential file, as well as the Audit Job, the subnet `192.168.1.x` is hierarchically below the network level.

Credential Profiles and User role privileges

As explained in the *DbProtect Administrator's Guide*, Credential Profile privileges are restricted to certain User types. The following table explains which User roles can (and cannot):

- **export** credentials to file via a Job template or Credential Profile; for more information, see *Exporting a User Credentials File*
- **import** credentials from file via a Job template or Credential Profile; for more information, see *Importing a User Credentials File*
- **create/modify** a Credential Profile; for more information, see *Creating a Credential Profile* and *Editing a Credential Profile*, respectively. ,

Privileges	User role			
	Super Admin	Admin	Basic User	View User
Create or modify a Credential Profile	✓	✓	✓	X
Export credentials to file via a Job template or Credential Profile	✓	X	X	X
Import credentials from file via a Job template or Credential Profile	✓	✓	✓	X

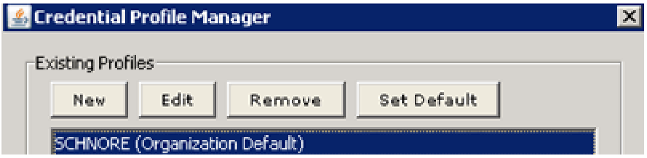
Access	✓	**No Access**	X

Creating a Credential Profile

Super Admins, Admins, and Basic Users can create a Credential Profile; for more information, see *What is a Credential Profile?*

To create a Credential Profile:

1. Do one of the following to display the **Credential Profile Manager**:
   - Choose **File** > **Credential Profile Manager** from the menu.
   - Display the **Audit Template Editor** dialog box (for more information, see *Creating an Audit Job*), then click the **Apply Credential Profile** button to display the **Credential Profile Picker** pop up, then click the **Manage Profiles** button.



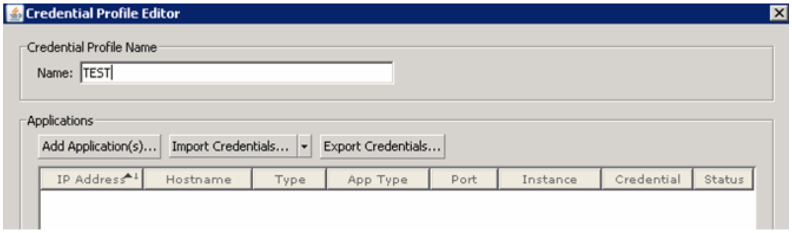
SCHNORE (Organization Default)

FIGURE: Credential Profile Manager

You can click the:

- New button to create a Credential Profile (see Step 2)
- **Edit** button to edit a Credential Profile; for more information, see *Editing a Credential Profile*
- **Remove** button to remove a Credential Profile; for more information, see *Removing a Credential Profile*
- **Set Default** button to set a Credential Profile as an **Organizational default**, for more information, see *Setting a Credential Profile as an Organizational default*.

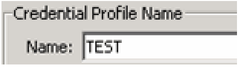
2. Click the **New** button on the **Credential Profile Manager** to display the **Credential Profile Editor** dialog box.



Name: TEST

FIGURE: **Credential Profile Editor** dialog box

3. In the **Credential Profile Name** portion of the **Credential Profile Editor** dialog box, enter the name of your new Credential Profile in the **Name:** field.

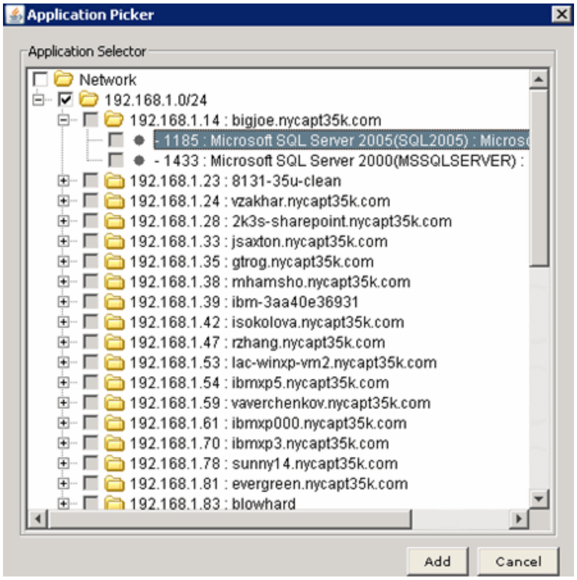


Credential Profile Name

Name: TEST

FIGURE: **Credential Profile Name** portion of the **Credential Profile Editor** dialog box

4. Click the **Add Application(s)...** button to display the **Application Picker**.



Application Picker

Application Selector

- □ Network
- ☑ 192.168.1.0/24
  - □ 192.168.1.14 : bigjoe.nycapt35k.com
    - □ ● - 1185 : Microsoft SQL Server 2005(SQL2005) : Micros
    - □ ● - 1433 : Microsoft SQL Server 2000(MSSQLSERVER) :
  - □ 192.168.1.23 : 8131-35u-clean
  - □ 192.168.1.24 : vzakhar.nycapt35k.com
  - □ 192.168.1.28 : 2k3s-sharepoint.nycapt35k.com
  - □ 192.168.1.33 : jsaxton.nycapt35k.com
  - □ 192.168.1.35 : gtrog.nycapt35k.com
  - □ 192.168.1.38 : mhamsho.nycapt35k.com
  - □ 192.168.1.39 : ibm-3aa40e36931
  - □ 192.168.1.42 : isokolova.nycapt35k.com
  - □ 192.168.1.47 : rzhang.nycapt35k.com
  - □ 192.168.1.53 : lac-winxp-vm2.nycapt35k.com
  - □ 192.168.1.54 : ibmxp5.nycapt35k.com
  - □ 192.168.1.59 : vaverchenkov.nycapt35k.com
  - □ 192.168.1.61 : ibmxp000.nycapt35k.com
  - □ 192.168.1.70 : ibmxp3.nycapt35k.com
  - □ 192.168.1.78 : sunny14.nycapt35k.com
  - □ 192.168.1.81 : evergreen.nycapt35k.com
  - □ 192.168.1.83 : blowhard

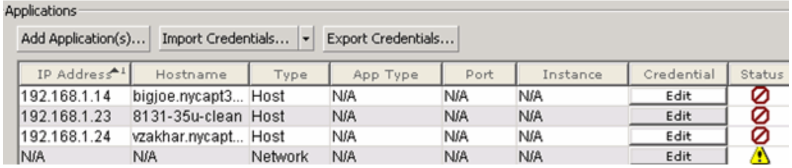
FIGURE: **Credential Profile Editor** dialog box

The **Application Picker** allows you to establish which applications are allowed to use the credentials specified in this Credential Profile when you apply the Credential Profile to an Audit Job. You can add a(n):

- **network**, and all subordinate **subnets**, **hosts**, and **application**s on the network
- **subnet**, and all subordinate **hosts** and **applications** on the subnet
- **host**, and all subordinate **applications** on the host
- individual **application**.

Important: The applications specified in your Credential Profile must *exactly* match the applications specified in your Audit Job, at the application type level. For example, if you specify subnet `192.168.1.x` in your Credential Profile, and attempt to apply this Credential Profile to an Audit Job that does not include subnet `192.168.1.x` in its list of applications to Audit, then the Audit Job will fail. However, if the Audit Job includes the entire network in its list of applications to Audit, then this Credential Profile will work, because in the credential file, as well as the Audit Job, the subnet `192.168.1.x` is hierarchically below the network level.For more information, see *Understanding the Credential Profile hierarchy*.

5. When you are done picking which applications are allowed to use the credentials specified in this Credential Profile, click the **Add** button to close the **Application Picker**. Your selected applications display in the **Credential Profile Editor** dialog box.



IP Address	Hostname	Type	App Type	Port	Instance	Credential	Status
192.168.1.14	bigjoe.nycapt3...	Host	N/A	N/A	N/A	Edit	⊘
192.168.1.23	8131-35u-clean	Host	N/A	N/A	N/A	Edit	⊘
192.168.1.24	vzakhar.nycapt...	Host	N/A	N/A	N/A	Edit	⊘
N/A	N/A	Network	N/A	N/A	N/A	Edit	⚠

FIGURE: Selected networks, subnets, hosts, and applications in the **Credential Profile Editor** dialog box

For each application you selected with the **Application Picker**, the following fields display:

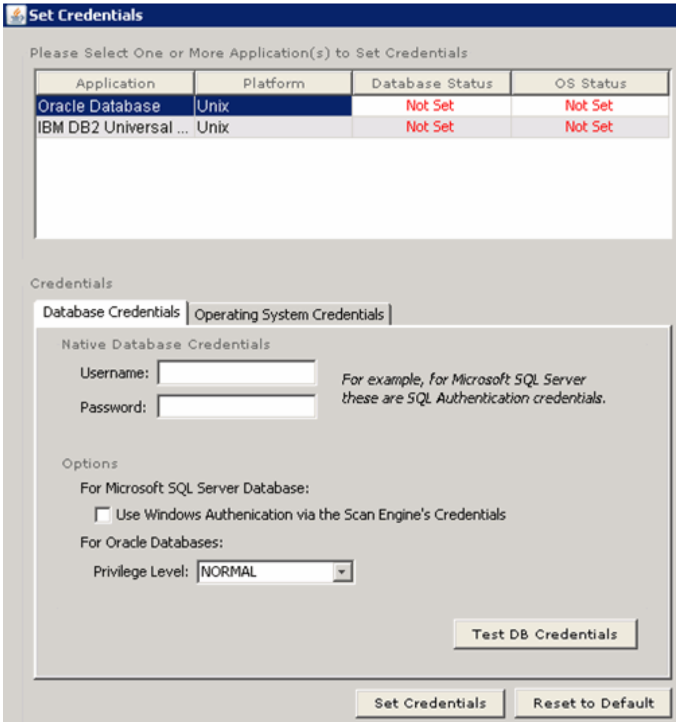
- The **IP Address** of your selected application (if applicable).
- The **Hostname** of your selected application (if applicable).
- The **Type** of application you selected with the **Application Picker**, i.e., **App**, **Subnet**, **Host**, **Network**.
- The **App Type** of the database application selected (e.g., **Oracle Database**), if you selected an application with the **Application Picker** in Step 4.
- The **Port** number of your selected application (if applicable).
- The **Instance** name of your selected application (if applicable).
- An **Edit** button under the **Credential** column, which you can click to set credentials for this Credential Profile (see Step 6).
- The icon under the **Status** column indicates whether your credentials are **incomplete** ⊘, **partial** ⚠, or **complete** ✓. If your credentials are incomplete or partial, click the **Edit** button under the **Credential** column, and set credentials for this Credential Profile (see Step 6).

6. You can set credentials for this Credential Profile. Do the following:

- Click the **Edit** button under the **Credential** column in the **Credential Profile Editor** dialog box.

The **Set Credentials** dialog box displays. The **Please Select One or More Application(s) to Set Credentials** portion displays each available **Application** and **Platform** combination (for which you can set credentials); for example, **Oracle Database** on **Unix**.

Note: The **Database Status** and **OS Status** columns display the status of your database and operating system credentials, respectively (i.e., **Set** or **Not Set**).



Please Select One or More Application(s) to Set Credentials

Application	Platform	Database Status	OS Status
Oracle Database	Unix	Not Set	Not Set
IBM DB2 Universal ...	Unix	Not Set	Not Set

Username:

Password:

For example, for Microsoft SQL Server these are SQL Authentication credentials.

For Microsoft SQL Server Database:

□ Use Windows Authentication via the Scan Engine's Credentials

For Oracle Databases:

Privilege Level: NORMAL

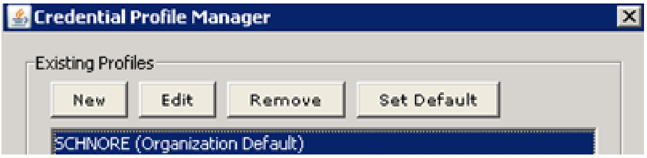
FIGURE: **Set Credentials** dialog box

- Select an **Application/Platform** combination in the **Please Select One or More Application(s) to Set Credentials** portion of the **Set Credentials** dialog box.

  The corresponding **Database Credentials** and **Operating System Credentials** tabbed fields display in the **Credentials** portion of the dialog box.
- Set your database and OS credentials, according to your selected Application/ Platform combination; for more information, see *Setting and testing your database and operating system credentials*.

7. Click the **Save** button to save your Credential Profile.

The **Credential Profile Manager** displays with your new Credential Profile added.



SCHNORE (Organization Default)

FIGURE: Credential Profile Manager

You can click the:

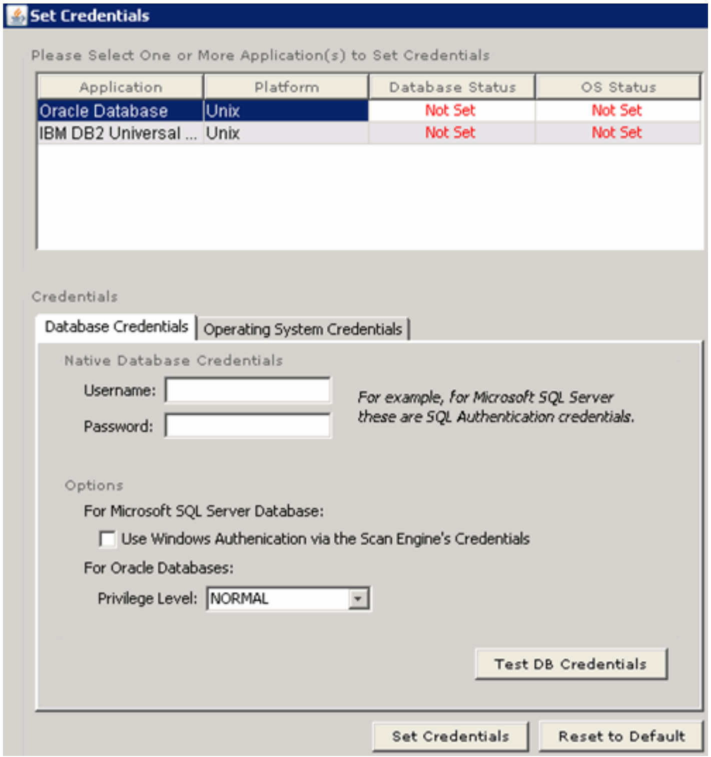
- New button to create another Credential Profile (go back to Step 2)
- **Edit** button to edit a Credential Profile, see *Editing a Credential Profile*
- **Remove** button to remove a Credential Profile, see *Removing a Credential Profile*
- **Set Default** button to set a Credential Profile as an **Organizational default**, see *Setting a Credential Profile as an Organizational default.*

Setting and testing your database and operating system credentials

As the diagram in *Understanding the Credential Profile hierarchy* illustrates, when you set credentials for **a network**, then all underlying **subnets**, **hosts**, and **applications** inherit the network's credentials. When you run an Audit Job, you must authenticate to the host database at both the application and OS levels. This topic explains how to set your application and platform credentials in various, supported application/platform combinations.

When you set the credentials (for a Credential Profile or an individual Audit Job), certain fields will display in the **Database Credentials** and **Operating System Credentials** tabs of the **Set Credentials** dialog box. The fields that display depend on which network **Application** and **Platform** you select in the **Please Select One or More Application(s) to Set Credentials** portion of the **Set Credentials** dialog box (shown below).

Note: To display the **Set Credentials** dialog box, click **Edit** button under the **Credential** column in the **Audit Template Editor** dialog box; for more information, see Step 7 of *Creating an Audit Job*.



Set Credentials

Please Select One or More Application(s) to Set Credentials

Application	Platform	Database Status	OS Status
Oracle Database	Unix	Not Set	Not Set
IBM DB2 Universal ...	Unix	Not Set	Not Set

Credentials

Database Credentials | Operating System Credentials

Native Database Credentials

Username:

Password:

For example, for Microsoft SQL Server these are SQL Authentication credentials.

Options

For Microsoft SQL Server Database:

☐ Use Windows Authenication via the Scan Engine's Credentials

For Oracle Databases:

Privilege Level: NORMAL

FIGURE: **Set Credentials** dialog box

In the **Please Select One or More Application(s) to Set Credentials** portion of the **Set Credentials** dialog box, you can set the credentials that allow you to authenticate to a database and an operating system.

What you will find in this help topic:

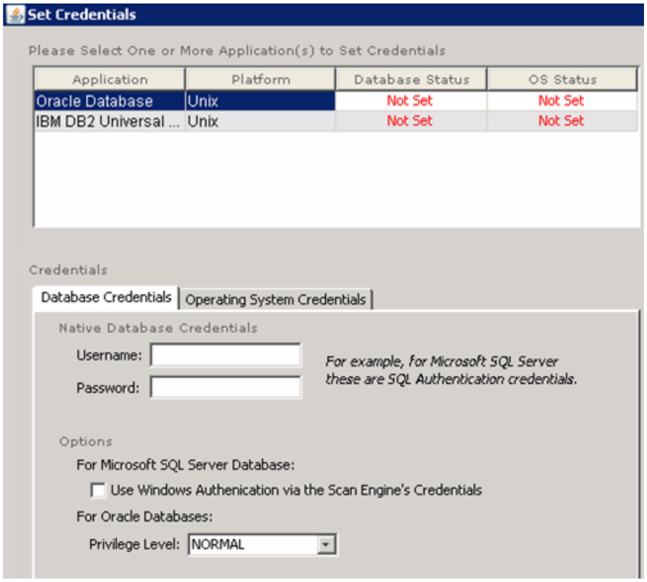
- *Setting your database credentials*
- *Testing your database credentials*
- *Setting your operating system credentials (for Unix-based operating systems)*
- *Setting your operating system credentials (for Windows)*
- *Setting your operating system credentials (for an "Unknown" operating system)*
- *Testing your operating system credentials (for Unix-based operating systems).*

SETTING YOUR DATABASE CREDENTIALS

To set your database credentials (for database authentication on any operating system):

1. To display the **Set Credentials** dialog box, you must click the **Edit** button under the **Credential** column in the **Audit Template Editor** dialog box; for more information, see Step 7 of ***Creating an Audit Job***.

In the **Please Select One or More Application(s) to Set Credentials** portion of the **Set Credentials** dialog box, select an application/platform combination.



Set Credentials

Please Select One or More Application(s) to Set Credentials

Application	Platform	Database Status	OS Status
Oracle Database	Unix	Not Set	Not Set
IBM DB2 Universal ...	Unix	Not Set	Not Set

Credentials

Database Credentials | Operating System Credentials

Native Database Credentials

Username:

Password:

For example, for Microsoft SQL Server these are SQL Authentication credentials.

Options

For Microsoft SQL Server Database:

☐ Use Windows Authenication via the Scan Engine's Credentials

For Oracle Databases:

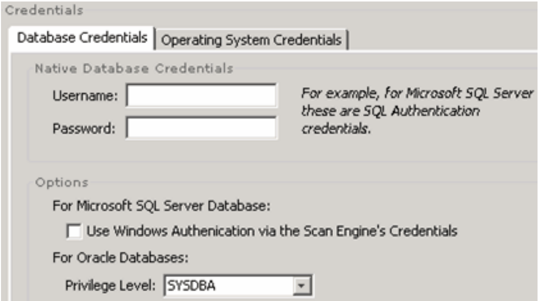
Privilege Level: NORMAL

FIGURE: **Set Credentials** dialog box

2. Do the following:

- Click the **Database Credentials** tab.

The **Database Credentials** portion of the **Set Credentials** dialog box displays. The available fields are the same for **Oracle** and **SQL Server**.



Credentials

Native Database Credentials

Username:

Password:

For example, for Microsoft SQL Server these are SQL Authentication credentials.

Options

For Microsoft SQL Server Database:

☐ Use Windows Authenication via the Scan Engine's Credentials

For Oracle Databases:

Privilege Level: SYSDBA

FIGURE: **Database Credentials** portion of the **Set Credentials** dialog box

- Under **Native Database Credentials**, enter your native database **Username:** and **Password:**
- Under **Options**, do the following:

  -**For a SQL Server native database.** Check the **Use Windows Authentication via the Scan Engine's Credentials** checkbox to authenticate to Windows using the privileges associated with your registered Scan Engine; for more information, see *Working with Scan Engines*

  -**For an Oracle native database.** Use the **Privilege Level:** drop-down to select the associated Oracle privileges (`SYSOPER`, `SYSDBA`, or `NORMAL`).
- Optionally, you can click the **Test DB Credentials** button to test your database credentials (before you set them). For more information, see *Testing your database credentials.*

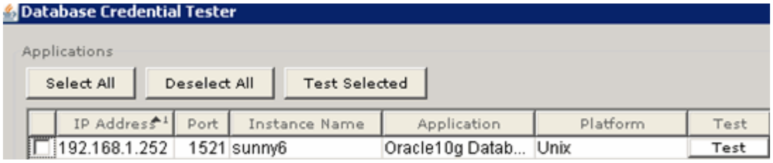
3. Click the **Set Credentials** button to set these database credentials (or click the **Reset to Default** button to restore your last saved database credential settings).

4. When you are done, click the **Save Changes** button to save the database and operating system credential changes you made to your Credential Profile (for this application/platform combination).

TESTING YOUR DATABASE CREDENTIALS

To test the database credentials you supplied in Step 2 of *Setting your database credentials*:

1. If you clicked the **Test DB Credentials** button in Step 2 of ***Setting your database credentials***, then the **Database Credential Tester** dialog box displays (like the one shown below).

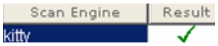


	IP Address	Port	Instance Name	Application	Platform	Test
□	192.168.1.252	1521	sunny6	Oracle10g Datab...	Unix	Test

FIGURE: **Database Credential Tester** dialog box

2. The following columns display in the **Database Credential Tester** dialog box (for each application you selected with the **Application Picker** in *Creating a Credential Profile*):
   - The **IP Address** of your selected application.
   - The **Port** number of your selected application.
   - The **Instance Name** of your selected application.
   - The **Hostname** of your selected application.
   - The **Application** selected (e.g., **Oracle Database**).
   - The **Platform** on which the database application runs (e.g., **Unix**).
3. Check one or more applications (against which you want to test your database credentials). You can click the:
   - **Select All** button to select all applications
   - **Deselect All** button to de-select all applications.
4. Test your database credentials against one or more selected applications. You can click:
   - an individual **Test** button Test next to an *individual* checked application in order to test your database credentials
   - the **Test Selected** button Test Selected at the top of the **Database Credential Tester** dialog box, which allows you to test the database credentials for *all* of your checked applications simultaneously.

DbProtect Vulnerability Management tests the database credentials for all checked applications. The test results display under the **Scan Engine** and **Result** columns of the **Database Credential Tester** dialog box.



Scan Engine	Result
kitty	✓

FIGURE: **Scan Engine** and **Result** columns

The **Scan Engine** column displays the name of the Scan Engine that is scanning applications (selected in Step 3) for vulnerabilities.

The icon under the **Result** column indicates whether your database credentials are **Set** ✓ or **Not Set** ⊘ ,.

The **Scan Engine Not Available** icon ⚠ , may also display; for more information, see *Monitoring the health of your Scan Engines*.

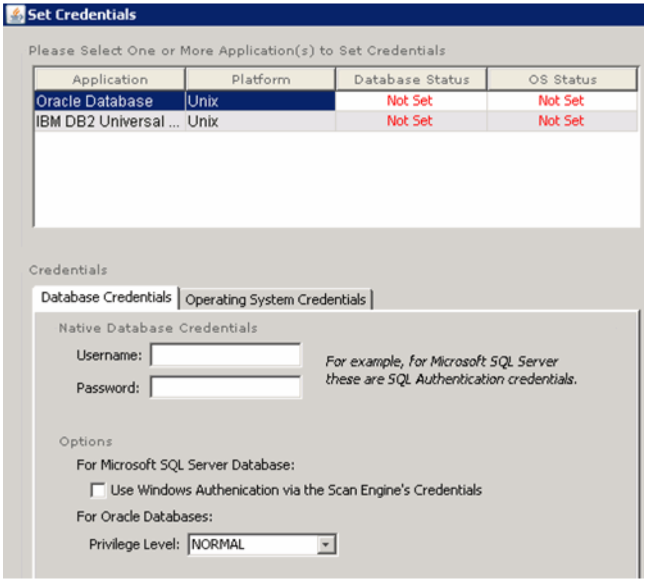
SETTING YOUR OPERATING SYSTEM CREDENTIALS (FOR UNIX-BASED OPERATING SYSTEMS)

To set your operating system credentials (for Unix-based operating systems):

1. To display the **Set Credentials** dialog box, you must click the **Edit** button under the **Credential** column in the **Audit Template Editor** dialog box; for more information, see Step 7 of ***Creating an Audit Job***.

In the **Please Select One or More Application(s) to Set Credentials** portion of the **Set Credentials** dialog box, select an **Application** on a Unix-based **Platform**.

Note: The **Database Status** and **OS Status** columns display the status of your database and operating system credentials, respectively, i.e., **Set** or **Not Set**.


Set Credentials
Please Select One or More Application(s) to Set Credentials
Credentials
Database Credentials
Operating System Credentials
Native Database Credentials
Options

Application	Platform	Database Status	OS Status
Oracle Database	Unix	Not Set	Not Set
IBM DB2 Universal ...	Unix	Not Set	Not Set

Username:

Password:

For example, for Microsoft SQL Server these are SQL Authentication credentials.

For Microsoft SQL Server Database:

□ Use Windows Authenication via the Scan Engine's Credentials

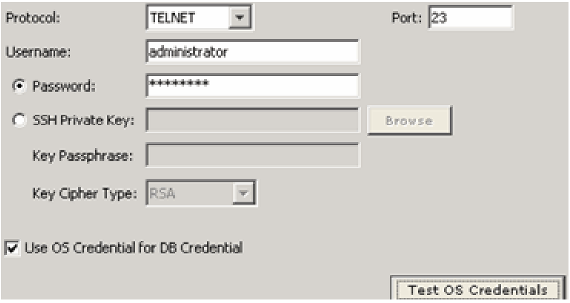
For Oracle Databases:

Privilege Level: NORMAL

FIGURE: **Set Credentials** dialog box

2. Click the **Operating System Credentials** tab to display the **Operating System Credentials** portion of the **Set Credentials** dialog box.

Note: The available fields depend on whether you want to set credentials for **Windows**, **Unix**, or another (**Unknown**) platform.



Protocol: TELNET Port: 23

Username: administrator

● Password: ********

○ SSH Private Key:

Key Passphrase:

Key Cipher Type: RSA

☑ Use OS Credential for DB Credential

FIGURE: **Operating System Credentials** portion of the **Set Credentials** dialog box

You can do the following:

- Use the **Protocol:** drop-down to select the authentication protocol (**Telnet** or **SSH**), and enter the **Port:** number.

Note: DbProtect Vulnerability Management automatically populates the **Port:** field with the default port numbers, in association with the **Protocol:** you select. The default port number for **Telnet** is **23**, and the default port number for **SSH** is **22**. You can overwrite these default values.

- Enter the operating system **Username:** associated with the username to authenticate to the operating system.
- Select either of the following:

  -**Password:** Enter the password associated with the username above, or

  -**SSH Private Key:** The SSH private key is the half of the key pair that you keep on your computer. The public key is the part that you upload to the remote server. Click the Browse button to select a your `.ppk` file. You must also enter the **Key Passphrase:** for your password-protected private key, and use the **Key Cipher Type** drop-down to select the **RSA** or **DSA** cipher type.

Hint: To **remove** a private key and passphrase, you must do the following: 1.) Delete the **SSH Private Key:** and **Key Passphrase:** 2.) Click the **Clear** button. 3.) Click the **Save Changes** button. 4.) When the **Audit Template Editor** dialog box re-displays, click the **Save** button.

Optionally, you can:

- check **Use OS Credential for DB Credential** to use your operating system credentials to authenticate to the host database
- click the **Test OS Credentials** button to test your database credentials (before you set them); for more information, see *Testing your operating system credentials (for Unix-based operating systems)*.

3. When you are done, click the **Save Changes** button to save the database and operating system credential changes you made to your Credential Profile (for this application/platform combination).

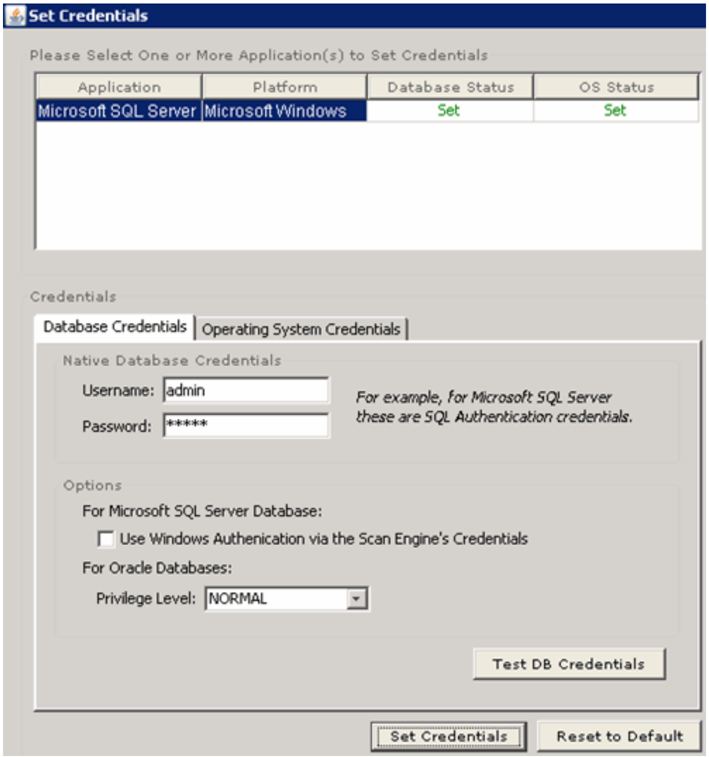
SETTING YOUR OPERATING SYSTEM CREDENTIALS (FOR WINDOWS)

To set your operating system credentials (for Windows):

1. To display the **Set Credentials** dialog box, you must click the **Edit** button under the **Credential** column in the **Audit Template Editor** dialog box; for more information, see Step 7 of ***Creating an Audit Job***.

In the **Please Select One or More Application(s) to Set Credentials** portion of the **Set Credentials** dialog box, select an **Application** on the Windows **Platform**.

Note: The **Database Status** and **OS Status** columns display the status of your database and operating system credentials, respectively, i.e., **Set** or **Not Set**.



Set Credentials
Please Select One or More Application(s) to Set Credentials

Application	Platform	Database Status	OS Status
Microsoft SQL Server	Microsoft Windows	Set	Set

Credentials
Database Credentials
Operating System Credentials
Native Database Credentials

Username: admin

Password: *****

For example, for Microsoft SQL Server these are SQL Authentication credentials.

For Microsoft SQL Server Database:

□ Use Windows Authenication via the Scan Engine's Credentials

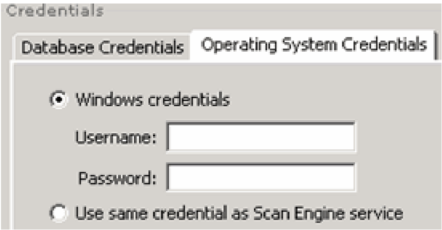
For Oracle Databases:

Privilege Level: NORMAL

Test DB Credentials
Set Credentials
Reset to Default

FIGURE: **Set Credentials** dialog box

2. Click the **Operating System Credentials** tab to display the **Operating System Credentials** portion of the **Set Credentials** dialog box.



Credentials

Database Credentials | Operating System Credentials

● Windows credentials

Username:

Password:

○ Use same credential as Scan Engine service

FIGURE: **Operating System Credentials** portion of the **Set Credentials** dialog box

You can select:

- **Windows credentials** and enter your Windows **Username:** and **Password:**
- **Use same credential as Scan Engine service** to use the same Windows credentials as used by your registered Scan Engine.

3. When you are done, click the **Save Changes** button to save the database and operating system credential changes you made to your Credential Profile (for this application/platform combination).

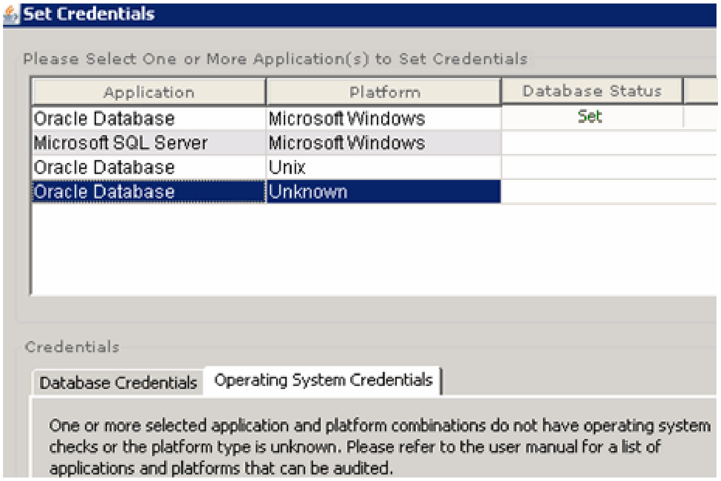
SETTING YOUR OPERATING SYSTEM CREDENTIALS (FOR AN "UNKNOWN" OPERATING SYSTEM)

To set your operating system credentials (for applications on an "unknown" operating system):

1. To display the **Set Credentials** dialog box, you must click the **Edit** button under the **Credential** column in the **Audit Template Editor** dialog box; for more information, see Step 7 of ***Creating an Audit Job***.

In the **Please Select One or More Application(s) to Set Credentials** portion of the **Set Credentials** dialog box, select an **Application** on an unknown **Platform**.

Note: The **Database Status** and **OS Status** columns display the status of your database and operating system credentials, respectively, i.e., **Set** or **Not Set**.

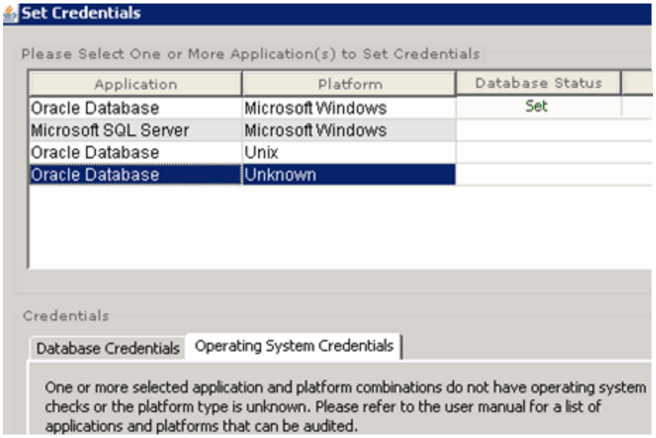

Set Credentials
Please Select One or More Application(s) to Set Credentials
Credentials
Database Credentials
Operating System Credentials

Application	Platform	Database Status
Oracle Database	Microsoft Windows	Set
Microsoft SQL Server	Microsoft Windows	
Oracle Database	Unix	
Oracle Database	Unknown	

One or more selected application and platform combinations do not have operating system checks or the platform type is unknown. Please refer to the user manual for a list of applications and platforms that can be audited.

FIGURE: **Set Credentials** dialog box

2. Click the **Operating System Credentials** tab to display the **Operating System Credentials** portion of the **Set Credentials** dialog box.


Set Credentials
Please Select One or More Application(s) to Set Credentials
Credentials
Database Credentials
Operating System Credentials

Application	Platform	Database Status
Oracle Database	Microsoft Windows	Set
Microsoft SQL Server	Microsoft Windows	
Oracle Database	Unix	
Oracle Database	Unknown	

One or more selected application and platform combinations do not have operating system checks or the platform type is unknown. Please refer to the user manual for a list of applications and platforms that can be audited.

FIGURE: **Operating System Credentials** portion of the **Set Credentials** dialog box

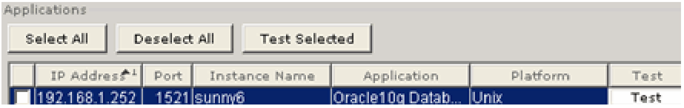
A message displays informing you that your operating system is unknown. For more information on applications and platforms that you can Audit, see *Scan Engines*.

3. When you are done, click the **Save Changes** button to save the database and operating system credential changes you made to your Credential Profile (for this application/platform combination).

TESTING YOUR OPERATING SYSTEM CREDENTIALS (FOR UNIX-BASED OPERATING SYSTEMS)

To test the database credentials you supplied in Step 2 of *Setting your operating system credentials (for Unix-based operating systems)*:

1. If you clicked the **Test OS Credentials** button in Step 2 of ***Setting your operating system credentials (for Unix-based operating systems)***, then the **Operating System Credential Tester** dialog box displays (like the one shown below).

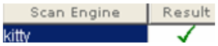


	IP Address	Port	Instance Name	Application	Platform	Test
☐	192.168.1.252	1521	sunny6	Oracle10g Datab...	Unix	Test

FIGURE: **Database Credential Tester** dialog box

2. The following columns display in the **Operating System Credential Tester** dialog box (for each application you selected with the **Application Picker** in *Creating a Credential Profile*):
   - The **IP Address** of your selected application.
   - The **Port** number of your selected application.
   - The **Instance Name** of your selected application.
   - The **Hostname** of your selected application.
   - The **Application** selected (e.g., **Oracle Database**).
   - The **Platform** on which the database application runs (e.g., **Unix**).
3. Check one or more applications (against which you want to test your database credentials). You can click the:
   - **Select All** button to select all applications
   - **Deselect All** button to de-select all applications.
4. Test your operating system credentials against one or more selected applications. You can click:
   - an individual **Test** button Test next to an *individual* checked application in order to test your operating system credentials
   - the **Test Selected** button Test Selected at the top of the **Operating System Credential Tester** dialog box, which allows you to test the operating system credentials for *all* of your checked applications simultaneously.

DbProtect Vulnerability Management tests the operating system credentials for all checked applications. The test results display under the **Scan Engine** and **Result** columns of the **Operating System Credential Tester** dialog box.



Scan Engine	Result
kitty	✓

FIGURE: **Scan Engine** and **Result** columns

The **Scan Engine** column displays the name of the Scan Engine that is scanning applications (selected in Step 3) for vulnerabilities.

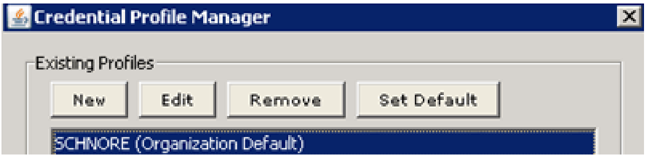
The icon under the **Result** column indicates whether your operating system credentials are **Set** ✓ or **Not Set** ⊘ ,.

The **Scan Engine Not Available** icon ⚠ , may also display; for more information, see *Monitoring the health of your Scan Engines*.

Editing a Credential Profile

To **edit** a Credential Profile:

1. Do one of the following to display the **Credential Profile Manager**:
   - Choose **File > Credential Profile Manager** from the menu.
   - Display the **Audit Template Editor** dialog box (for more information, see *Creating an Audit Job*), then click the **Apply Credential Profile** button to display the **Credential Profile Picker** pop up, then click the **Manage Profiles** button.



SCHNORE (Organization Default)

FIGURE: Credential Profile Manager

You can click the:

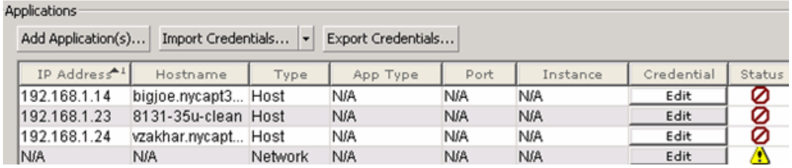
- **Edit** button to edit a Credential Profile (see Step 2)

Hint: You can also right click an application in the **Credential Profile Editor** dialog box (as shown in Step 2), and choose **Edit Credentials**.

- **New** button to create a Credential Profile; for more information, see *Creating a Credential Profile*
- **Remove** button to remove a Credential Profile; for more information, see *Removing a Credential Profile*
- **Set Default** button to set a Credential Profile as an **Organizational default**; for more information, see *Setting a Credential Profile as an Organizational default*.

2. Select a Credential Profile in the **Existing Profiles** portion of the **Credential Profile Manager** and click the **Edit** button.

The **Credential Profile Editor** dialog box displays, with the current settings shown.



IP Address	Hostname	Type	App Type	Port	Instance	Credential	Status
192.168.1.14	bigjoe.nycapt3...	Host	N/A	N/A	N/A	Edit	⊘
192.168.1.23	8131-35u-clean	Host	N/A	N/A	N/A	Edit	⊘
192.168.1.24	vzakhar.nycapt...	Host	N/A	N/A	N/A	Edit	⊘
N/A	N/A	Network	N/A	N/A	N/A	Edit	⚠

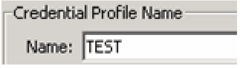
FIGURE: **Credential Profile Editor** dialog box

For each application that comprises the Credential Profile, the following fields display:

- The **IP Address** of your selected application (if applicable).
- The **Hostname** of your selected application (if applicable).
- The **Type** of application you selected with the **Application Picker**, i.e., **App**, **Subnet**, **Host**, **Network**.

- The **App Type** of the database application selected (e.g., **Oracle Database**), if you selected an application with the **Application Picker** in Step 4.
- The **Port** number of your selected application (if applicable).
- The **Instance** name of your selected application (if applicable).
- An **Edit** button under the **Credential** column, which you can click to set credentials for this Credential Profile.
- The icon under the **Status** column indicates whether your credentials are **incomplete** ⊘ , **partial** ⚠ , or **complete** ✓ . If your credentials are incomplete or partial, click the **Edit** button under the **Credential** column, and set credentials for this Credential Profile.

3. In the **Credential Profile Name** portion of the **Credential Profile Editor** dialog box, you can edit the name of the Credential Profile in the **Name:** field.

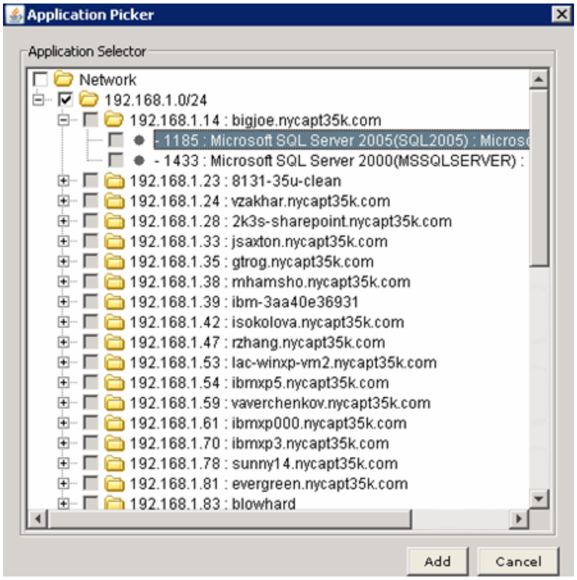


Credential Profile Name

Name: TEST

4. Credential Profile Name portion of the **Credential Profile Editor** dialog box

You can click the **Add Application(s)...** button to display the **Application Picker**.



Application Picker

Application Selector

□ Network
☑ 192.168.1.0/24
□ 192.168.1.14 : bigjoe.nycapt35k.com
□ ● - 1185 : Microsoft SQL Server 2005(SQL2005) : Micros
□ ● - 1433 : Microsoft SQL Server 2000(MSSQLSERVER) :
□ 192.168.1.23 : 8131-35u-clean
□ 192.168.1.24 : vzakhar.nycapt35k.com
□ 192.168.1.28 : 2k3s-sharepoint.nycapt35k.com
□ 192.168.1.33 : jsaxton.nycapt35k.com
□ 192.168.1.35 : gtrog.nycapt35k.com
□ 192.168.1.38 : mhamsho.nycapt35k.com
□ 192.168.1.39 : ibm-3aa40e36931
□ 192.168.1.42 : isokolova.nycapt35k.com
□ 192.168.1.47 : rzhang.nycapt35k.com
□ 192.168.1.53 : lac-winxp-vm2.nycapt35k.com
□ 192.168.1.54 : ibmxp5.nycapt35k.com
□ 192.168.1.59 : vaverchenkov.nycapt35k.com
□ 192.168.1.61 : ibmxp000.nycapt35k.com
□ 192.168.1.70 : ibmxp3.nycapt35k.com
□ 192.168.1.78 : sunny14.nycapt35k.com
□ 192.168.1.81 : evergreen.nycapt35k.com
□ 192.168.1.83 : blowhard

FIGURE: **Credential Profile Editor** dialog box

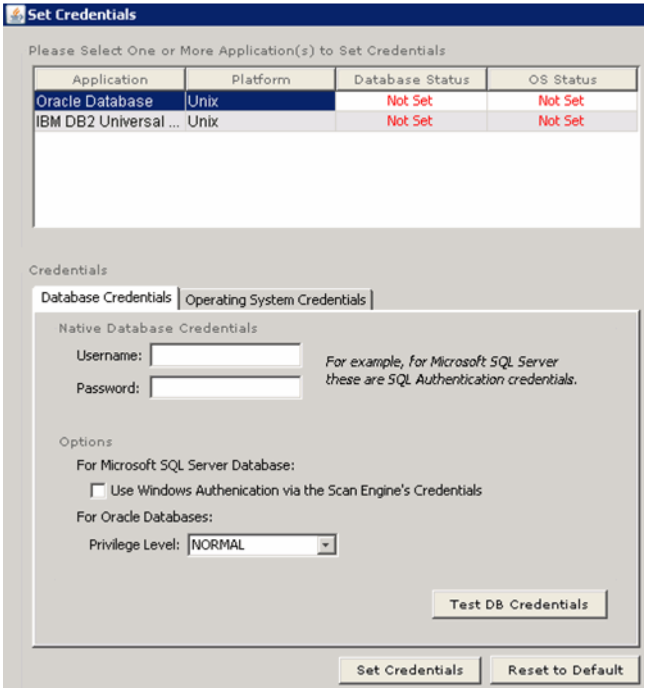
The **Application Picker** allows you to edit which applications are allowed to use the credentials specified in this Credential Profile when you apply the Credential Profile to an Audit Job. You can add a(n):

- **network**, and all subordinate **subnets**, **hosts**, and **application**s on the network
- **subnet**, and all subordinate **hosts** and **applications** on the subnet
- **host**, and all subordinate **applications** on the host
- individual **application**.

Important: The applications specified in your Credential Profile must *exactly* match the applications specified in your Audit Job, at the application type level. For example, if you specify subnet `192.168.1.x` in your Credential Profile, and attempt to apply this Credential Profile to an Audit Job that does not include subnet `192.168.1.x` in its list of applications to Audit, then the Audit Job will fail. However, if the Audit Job includes the entire network in its list of applications to Audit, then this Credential Profile will work, because in the credential file, as well as the Audit Job, the subnet `192.168.1.x` is hierarchically below the network level.For more information, see *Understanding the Credential Profile hierarchy*.

5. You can edit credentials for this Credential Profile. Do the following:

- Click the **Edit** button under the **Credential** column in the **Credential Profile Editor** dialog box to display the **Set Credentials** dialog box.



Please Select One or More Application(s) to Set Credentials

Application	Platform	Database Status	OS Status
Oracle Database	Unix	Not Set	Not Set
IBM DB2 Universal ...	Unix	Not Set	Not Set

Credentials

Native Database Credentials

Username:

Password:

For example, for Microsoft SQL Server these are SQL Authentication credentials.

Options

For Microsoft SQL Server Database:

□ Use Windows Authenication via the Scan Engine's Credentials

For Oracle Databases:

Privilege Level: NORMAL

FIGURE: **Set Credentials** dialog box

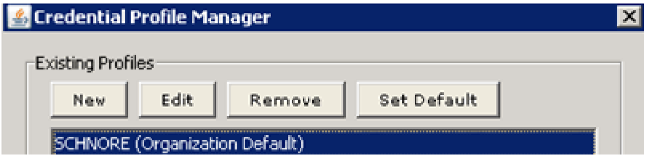
- Select an **Application/Platform** combination in the **Please Select One or More Application(s) to Set Credentials** portion of the **Set Credentials** dialog box, e.g., **Oracle Database** running on **Microsoft Windows**.

  The corresponding **Database Credentials** and **Operating System Credentials** tabbed fields display in the **Credentials** portion the **Set Credentials** dialog box.

- Set your credentials, according to your selected **Application/Platform** combination; for more information, see *Setting and testing your database and operating system credentials*.

6. Click the **Save** button to save your edited Credential Profile.

The **Credential Profile Manager** displays with your edited Credential Profile included.



SCHNORE (Organization Default)

FIGURE: Credential Profile Manager

You can click the:

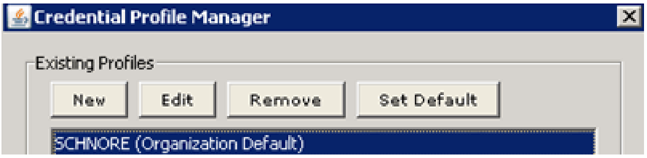
- **Edit** button to edit another Credential Profile (go back to Step 2)
- **New** button to create a Credential Profile; for more information, see *Creating a Credential Profile*
- **Remove** button to remove a Credential Profile; for more information, see *Removing a Credential Profile*
- **Set Default** button to set a Credential Profile as an **Organizational default**; for more information, see *Setting a Credential Profile as an Organizational default*.

Removing a Credential Profile

To **remove** a Credential Profile:

1. Do one of the following to display the **Credential Profile Manager**:

- Choose **File** > **Credential Profile Manager** from the menu.
- Display the **Audit Template Editor** dialog box (for more information, see *Creating an Audit Job*), then click the **Apply Credential Profile** button to display the **Credential Profile Picker** pop up, then click the **Manage Profiles** button.



SCHNORE (Organization Default)

FIGURE: Credential Profile Manager

You can click the:

- **Remove** button to remove a Credential Profile (see Step 2)
- **New** button to create a Credential Profile; for more information, see *Creating a Credential Profile*
- **Edit** button to edit a Credential Profile; for more information, see *Editing a Credential Profile*
- **Set Default** button to set a Credential Profile as an **Organizational default**; for more information, see *Setting a Credential Profile as an Organizational default*.

2. Select a Credential Profile in the **Existing Profiles** portion of the **Credential Profile Manager** and click the **Remove** button.

DbProtect Vulnerability Management removes the selected Credential Profile. The **Credential Profile Manager** displays with the Credential Profile removed.

You can click the:

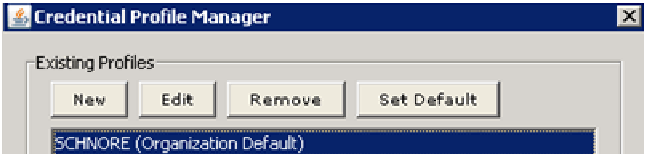
- **Remove** button to remove another Credential Profile (repeat this step)
- **New** button to create a Credential Profile; for more information, see *Creating a Credential Profile*
- **Edit** button to edit a Credential Profile; for more information, see *Editing a Credential Profile*
- **Set Default** button to set a Credential Profile as an **Organizational default**; for more information, see *Setting a Credential Profile as an Organizational default*.

Setting a Credential Profile as an Organizational default

DbProtect allows you to set a Credential Profile as your **default** Credential Profile. The default Credential Profile displays at the top of the **Credential Profile Manager**.

To set a Credential Profile as an Organizational default:

1. Do one of the following to display the **Credential Profile Manager**:
   - Choose **File** > **Credential Profile Manager** from the menu.
   - Display the **Audit Template Editor** dialog box (for more information, see *Creating an Audit Job*), then click the **Apply Credential Profile** button to display the **Credential Profile Picker** pop up, then click the **Manage Profiles** button.



SCHNORE (Organization Default)

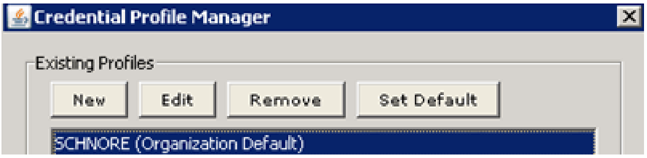
FIGURE: Credential Profile Manager

You can click the:

- **Set Default** button to set a Credential Profile as an Organizational default (see Step 2)
- **New** button to create a Credential Profile; for more information, see *Creating a Credential Profile*
- **Edit** button to edit a Credential Profile; for more information, see *Editing a Credential Profile*
- **Remove** button to remove a Credential Profile; for more information, see *Removing a Credential Profile*.

2. Select a Credential Profile in the **Existing Profiles** portion of the **Credential Profile Manager** and click the **Set Default** button.

The **Credential Profile Manager** displays the selected Credential Profile as the **Organization Default**.



SCHNORE (Organization Default)

FIGURE: Credential Profile Manager

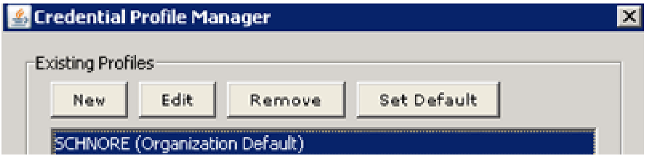
You can click the:

- **Set Default** button to set a Credential Profile as an Organizational default (repeat this step)
- **New** button to create a Credential Profile; for more information, see *Creating a Credential Profile*
- **Edit** button to edit a Credential Profile; for more information, see *Editing a Credential Profile*
- **Remove** button to remove a Credential Profile; for more information, see *Removing a Credential Profile*.

Removing applications from a Credential Profile

To remove applications from a Credential Profile:

1. Do one of the following to display the **Credential Profile Manager**:
   - Choose **File** > **Credential Profile Manager** from the menu.
   - Display the **Audit Template Editor** dialog box (for more information, see *Creating an Audit Job*), then click the **Apply Credential Profile** button to display the **Credential Profile Picker** pop up, then click the **Manage Profiles** button.

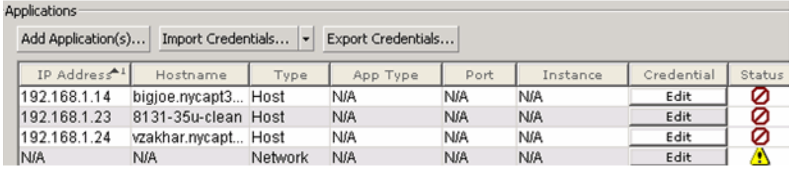


SCHNORE (Organization Default)

FIGURE: Credential Profile Manager

2. Select a Credential Profile in the **Existing Profiles** portion of the **Credential Profile Manager** and click the **Edit** button.

The **Credential Profile Editor** dialog box displays, with the current settings shown.



IP Address	Hostname	Type	App Type	Port	Instance	Credential	Status
192.168.1.14	bigjoe.nycapt3...	Host	N/A	N/A	N/A	Edit	⊘
192.168.1.23	8131-35u-clean	Host	N/A	N/A	N/A	Edit	⊘
192.168.1.24	vzakhar.nycapt...	Host	N/A	N/A	N/A	Edit	⊘
N/A	N/A	Network	N/A	N/A	N/A	Edit	⚠

FIGURE: **Credential Profile Editor** dialog box

3. Right click an application in the **Credential Profile Editor** dialog box and choose **Remove Application**.

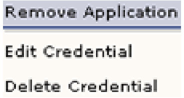


FIGURE: **Credential Profile Editor** dialog box pop up (**Remove Application** selected)

The selected application is removed from the list of Credential Profile applications in the **Credential Profile Editor** dialog box.

Deleting credentials from a Credential Profile

To delete credentials from a Credential Profile:

1. Do one of the following to display the **Credential Profile Manager**:
   - Choose **File > Credential Profile Manager** from the menu.
   - Display the **Audit Template Editor** dialog box (for more information, see *Creating an Audit Job*), then click the **Apply Credential Profile** button to display the **Credential Profile Picker** pop up, then click the **Manage Profiles** button.

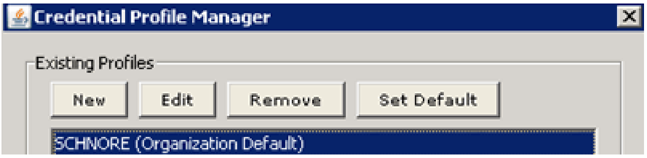
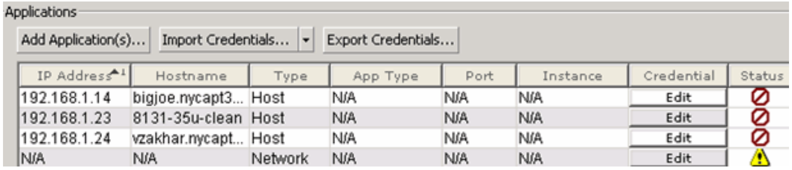


FIGURE: Credential Profile Manager

2. Select a Credential Profile in the **Existing Profiles** portion of the **Credential Profile Manager** and click the **Edit** button.

The **Credential Profile Editor** dialog box displays, with the current settings shown.



IP Address	Hostname	Type	App Type	Port	Instance	Credential	Status
192.168.1.14	bigjoe.nycapt3...	Host	N/A	N/A	N/A	Edit	⊘
192.168.1.23	8131-35u-clean	Host	N/A	N/A	N/A	Edit	⊘
192.168.1.24	vzakhar.nycapt...	Host	N/A	N/A	N/A	Edit	⊘
N/A	N/A	Network	N/A	N/A	N/A	Edit	⚠

FIGURE: **Credential Profile Editor** dialog box

3. Right click an application in the **Credential Profile Editor** dialog box and choose **Delete Credential**.

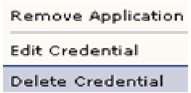


FIGURE: **Credential Profile Editor** dialog box pop up (**Delete Credential** selected)

DbProtect Vulnerability Management deletes all credentials from the selected application in this Credential Profile.

Importing a User Credentials File

To import a User Credentials File:

1. All Users (except View Users) can import User Credentials from an `.xml` file. This file **must** be properly-formatted or the import will fail, and the User Credentials will remain unchanged. For more information on the proper format of a User Credentials File, see ***Appendix A: Creating a User Credentials File***.

Do the following:

- Click the **Import Credentials** button in the **Audit Template Editor** dialog box to display the **Open** dialog box, which allows you to select a User Credentials file.

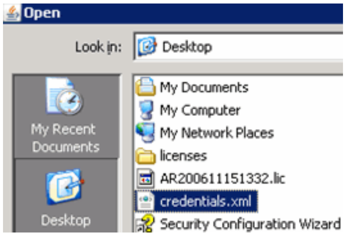


FIGURE: **Open** dialog box

- Select a properly-formatted User Credentials `.xml` file and click the **Open** button.

DbProtect Vulnerability Management imports the User Credentials.

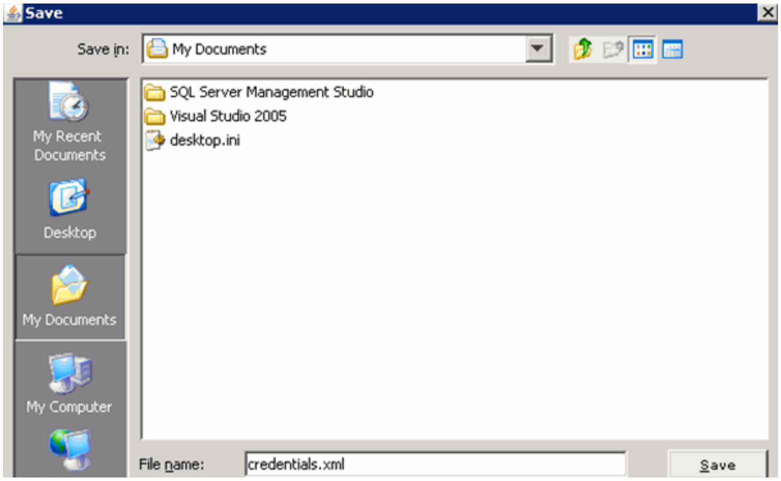
Exporting a User Credentials File

Super Users can export User Credentials to an `.xml` file.

Note: Private keys are **not** part of the User Credentials export file.

To export a User Credentials File:

1. Do the following:
   - Click the **Export Credentials** button in the **Audit Template Editor** dialog box to display the **Save** dialog box.

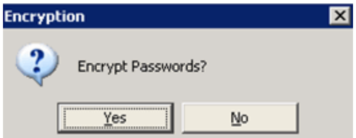


File name: credentials.xml

FIGURE: **Save** dialog box

   - Specify the location and name of the `.xml` file you want to export.
   - Click the **Save** button.

The **Encryption** pop up displays, allowing you to choose whether you want to encrypt all passwords in your Credential Profile `.xml` file.



Encrypt Passwords?

FIGURE: **Encryption** pop up

2. If you:
    - want to encrypt the passwords in your Credential Profile `.xml` file, then click the **Yes** button and see Step 3
    - do **not** want to encrypt the passwords in your Credential Profile `.xml` file, then click the **No** button and see Step 4.
3. If you click the **Yes** button in Step 2 to encrypt the passwords in your Credential Profile `.xml` file, then the **Passphrase** pop up displays, prompting you to enter a unique passphrase. Whenever you import this Credential Profile `.xml` file, you must enter this passphrase in order to load the Credential Profile.

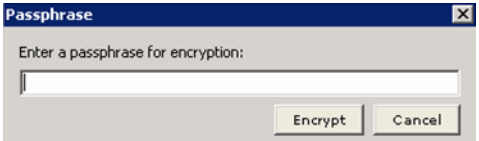


FIGURE: **Passphrase** pop up

Enter a passphrase and click the **Encrypt** button.

4. After you export your (encrypted or unencrypted) Credential Profile `.xml` file, a "success" message displays.

Working with Fix Scripts

This chapter consists of the following topics:

- *What are Fix Scripts?*
- *Fix Script parameters*
- *Running an "on-demand" Fix Script*
- *Automatically running a Fix Script*
- *Downloading and viewing the details of a Fix Script*
- *Customizing a Fix Script*
- *Deleting a Fix Script.*

What are Fix Scripts?

Fix Scripts are DbProtect-generated SQL scripts designed to correct misconfigurations and address vulnerabilities identified by DbProtect during an Audit. You can voluntarily deploy DbProtect-generated Fix Scripts to remediate your vulnerable databases.

DbProtect Vulnerability Management allows you to generate Fix Scripts in two ways:

- **"On demand"** for **all vulnerabilities** detected on an **individual Audited database instance**, or for **individual vulnerabilities** detected on an **individual Audited database instance**; for more information, see *Running an "on-demand" Fix Script* and *Automatically running a Fix Script*
- **Automatically** for **all vulnerabilities** detected for **all Audited database instances**; for more information, for more information, see *Running an "on-demand" Fix Script* and *Automatically running a Fix Script*

DbProtect Vulnerability Management also allows you to:

- download and view the details of a Fix Script; for more information, see *Downloading and viewing the details of a Fix Script*
- customize a Fix Script; for more information, see *Customizing a Fix Script*
- delete a Fix Script; for more information, see *Deleting a Fix Script*.

Important: For Fix Script details, see *Appendix J: Fix Scripts (Detail)*.

Fix Script parameters

The following table lists **Fix Script parameters**:

- `<NEW PASSWORD>`. New password to replace existing password. See database documentation for details.
- `<CURRENT PASSWORD>`. Currently active password for user.
- `<PASSWORD>`. Password to be set. See database documentation for details.
- `<NEW VERIFY FUNCTION>`. Name of a function used to verify passwords for compliance.
- `<NEW DEFAULT TABLESPACE>`. Name of a tablespace to be used as the default tablespace.
- `<NEW PROFILE NAME>`. Name of a profile to be created or assigned to a user.
- `<NEW ROLE>`. Name of a role to be created.
- `<NEW VALUE>`. Generic placeholder for parameter values. See database documentation for details.
- `<NEW METHOD>`. DB2 configuration value.
- `<LIMIT TYPE>`. Parameter value used for `sp_add_resource_limit` stored procedure. See Sybase documentation for details.
- `<ENFORCED>`. Parameter value used for `sp_add_resource_limit` stored procedure. See Sybase documentation for details.
- `<ACTION>`. Parameter value used for `sp_add_resource_limit` stored procedure. See Sybase documentation for details.
- `<SCOPE>`. Parameter value used for `sp_add_resource_limit` stored procedure. See Sybase documentation for details.
- `<CHOOSE 'on'|'off'>`. Parameter value. Possible values are `'on'` and `'off'`.
- `<CHOOSE 'on'|'fail'|'pass'>`. Parameter value. Possible values are `'on'`, `'fail'`, and `'pass'`.
- `<CURRENT AUDIT TABLE>`. Table name.
- `<YOUR SERVER NAME>`. Server host name.
- `<CORRESPONDING LOGIN>`. Login name for user.
- `<LOGIN PASSWORD>`. Password for login name.
- `<NEW SA LOGIN>`. SA login name to replace `'sa'`.

Running an “on-demand” Fix Script

You can run an **“on demand” Fix Script** to generate a Fix Script that will repair vulnerabilities detected during an Audit. As the name implies, you can run “on demand” Fix Scripts anytime you want. Specifically, you can run an **“on demand”** Fix Script to repair:

- **all vulnerabilities** detected on an **individual Audited database instance**; for more information, see *Running an “on demand” Fix Script to repair all vulnerabilities detected on an individual Audited database instance*

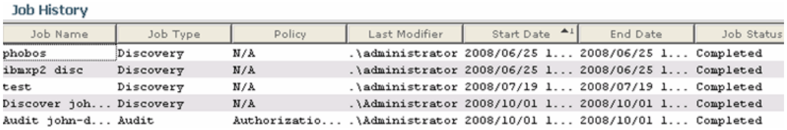
- **individual vulnerabilities** detected on an **individual Audited database instance**; for more information, see *Running an "on demand" Fix Script to repair individual vulnerabilities detected on an individual Audited database instance*.

(Alternately, you can generate a Fix Script **automatically** (i.e., as soon as your Audit Job completes). This option generates Fix Scripts to repair **all vulnerabilities** detected for **all Audited database instances**; for more information, see *Automatically running a Fix Script*.)

RUNNING AN "ON DEMAND" FIX SCRIPT TO REPAIR ALL VULNERABILITIES DETECTED ON AN INDIVIDUAL AUDITED DATABASE INSTANCE

To run an "on demand" Fix Script to repair **all vulnerabilities** detected on an **individual Audited database instance**:

1. Audit a Discovered database application; for more information, see ***Creating an Audit Job***.
2. Locate your completed Jobs. They display in the pane of the **Manage Jobs** page (**Completed Jobs** portion).

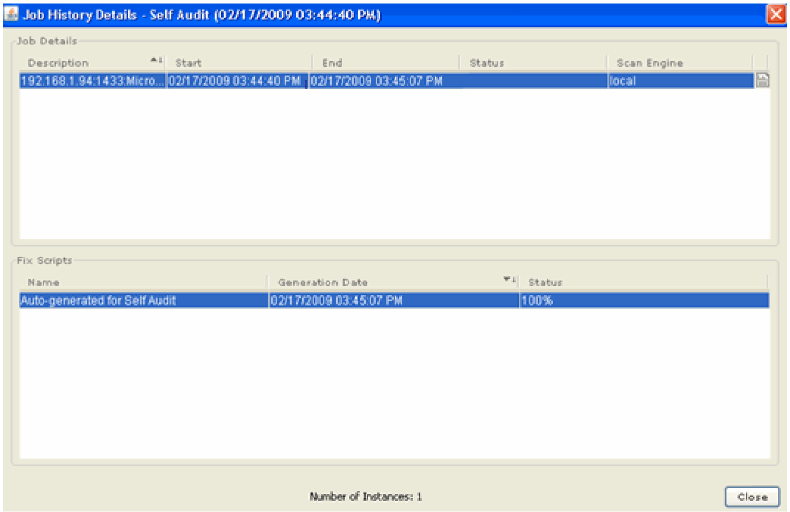


Job History

Job Name	Job Type	Policy	Last Modifier	Start Date	End Date	Job Status
phobos	Discovery	N/A	.\administrator	2008/06/25 1...	2008/06/25 1...	Completed
ibmxp2 disc	Discovery	N/A	.\administrator	2008/06/25 1...	2008/06/25 1...	Completed
test	Discovery	N/A	.\administrator	2008/07/19 1...	2008/07/19 1...	Completed
Discover joh...	Discovery	N/A	.\Administrator	2008/10/01 1...	2008/10/01 1...	Completed
Audit john-d...	Audit	Authorizatio...	.\Administrator	2008/10/01 1...	2008/10/01 1...	Completed

FIGURE: **Manage Jobs** page (**Job History** portion)

3. Right click a completed Audit Job and choose **Show Details** to display the **Job History Details** dialog box.



Description	Start	End	Status	Scan Engine
192.168.1.94:1433:Micro...	02/17/2009 03:44:40 PM	02/17/2009 03:45:07 PM		local

Name	Generation Date	Status
Auto-generated for Self Audit	02/17/2009 03:45:07 PM	100%

Number of Instances: 1

FIGURE: **Job History Details** dialog box

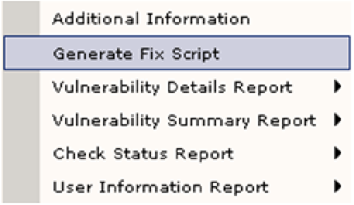
The upper **Job Details** portion of the **Job History Details** dialog box displays the Audit Job's historical details; for more information, see *Viewing the Job details of a completed Job*.

The lower **Fix Scripts** portion of the **Job History Details** dialog box displays information about any Fix Scripts that have already been run, including:

- Name
- Generation Date
- **Status**.

Note: You can right click an existing Fix Script in the **Fix Scripts** portion of the **Job History Details** dialog box to download and view the details of a Fix Script; for more information, see *Downloading and viewing the details of a Fix Script*.

4. Right click any completed Audit Job in the upper **Job Details** portion of the **Job History Details** dialog box, and select **Generate Fix Script**.



DbProtect generates an "on demand" Fix Script to repair **all vulnerabilities** detected on the selected individual Audited database instance.

The **Fix Scripts** portion of the **Job History Details** dialog box displays your "on demand" Fix Script.

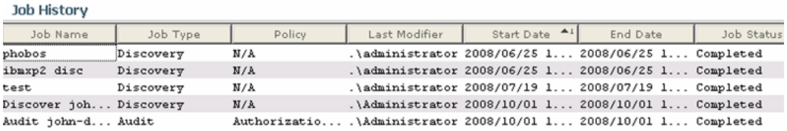
Next, you can:

- download the Fix Script and view its details; for more information, see *Downloading and viewing the details of a Fix Script*
- customize the Fix Script; for more information, see *Customizing a Fix Script*.

RUNNING AN "ON DEMAND" FIX SCRIPT TO REPAIR INDIVIDUAL VULNERABILITIES DETECTED ON AN INDIVIDUAL AUDITED DATABASE INSTANCE

To run an "on demand" Fix Script to repair **individual vulnerabilities** detected on an **individual Audited database instance**:

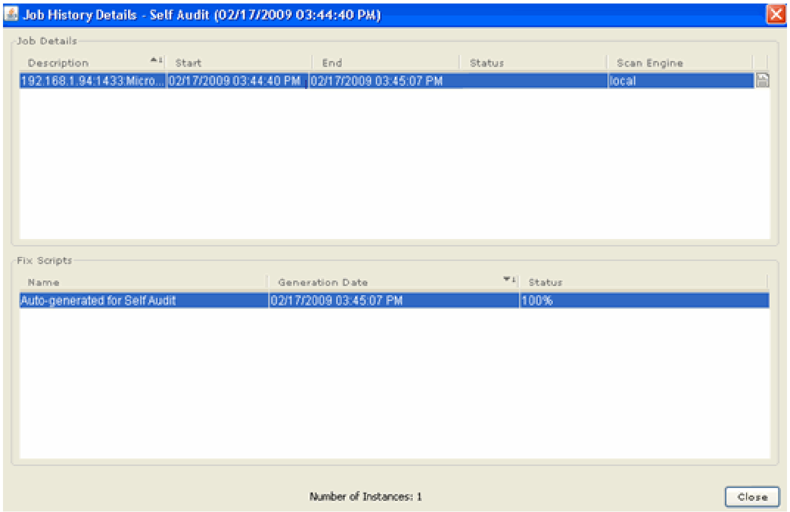
1. Audit a Discovered database application; for more information, see ***Creating an Audit Job***.
2. Locate your completed Jobs. They display in the pane of the **Manage Jobs** page (**Completed Jobs** portion).


Job History

Job Name	Job Type	Policy	Last Modifier	Start Date	End Date	Job Status
phobos	Discovery	N/A	.\administrator	2008/06/25 1...	2008/06/25 1...	Completed
ibmxp2 disc	Discovery	N/A	.\administrator	2008/06/25 1...	2008/06/25 1...	Completed
test	Discovery	N/A	.\administrator	2008/07/19 1...	2008/07/19 1...	Completed
Discover joh...	Discovery	N/A	.\Administrator	2008/10/01 1...	2008/10/01 1...	Completed
Audit john-d...	Audit	Authorizatio...	.\Administrator	2008/10/01 1...	2008/10/01 1...	Completed

FIGURE: **Manage Jobs** page (**Job History** portion)

3. Right click a completed Audit Job and choose **Show Details** to display the **Job History Details** dialog box.



Job History Details - Self Audit (02/17/2009 03:44:40 PM)

Job Details

Description	Start	End	Status	Scan Engine
192.168.1.94:1433:Micro...	02/17/2009 03:44:40 PM	02/17/2009 03:45:07 PM		local

Fix Scripts

Name	Generation Date	Status
Auto-generated for Self Audit	02/17/2009 03:45:07 PM	100%

Number of Instances: 1

FIGURE: **Job History Details** dialog box

The upper **Job Details** portion of the **Job History Details** dialog box displays the Audit Job's historical details; for more information, see *Viewing the Job details of a completed Job*.

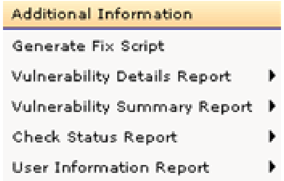
The lower **Fix Scripts** portion of the **Job History Details** dialog box displays information about any Fix Scripts that have already been run, including:

- **Name**
- **Generation Date**
- **Status**.

Note: You can right click an existing Fix Script in the **Fix Scripts** portion of the **Job History Details** dialog box to download and view the details of a Fix Script; for more information, see *Downloading and viewing the details of a Fix Script*.

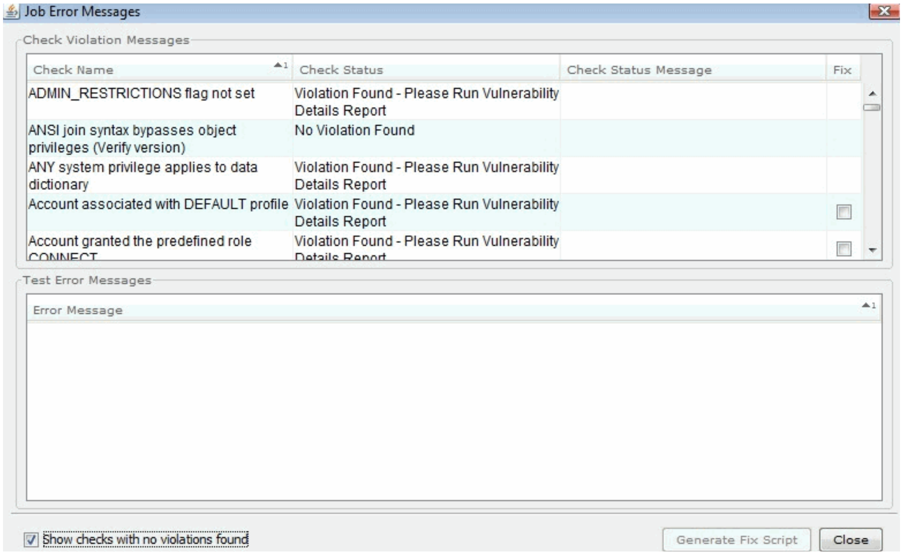
4. Do one of the following to display the **Job Error Messages** dialog box:

   - Right click any completed Audit Job in the upper **Job Details** portion of the **Job History Details** dialog box, and select **Additional Information**.



   - Double click any completed Audit Job in the upper **Job Details** portion of the **Job History Details** dialog box.

The **Job Error Messages** dialog box (shown below) lists **individual vulnerabilities** detected during an Audit of a Discovered database.



Check Name	Check Status	Check Status Message	Fix
ADMIN_RESTRICTIONS flag not set	Violation Found - Please Run Vulnerability Details Report		
ANSI join syntax bypasses object privileges (Verify version)	No Violation Found		
ANY system privilege applies to data dictionary	Violation Found - Please Run Vulnerability Details Report		
Account associated with DEFAULT profile	Violation Found - Please Run Vulnerability Details Report		□
Account granted the predefined role CONNECT	Violation Found - Please Run Vulnerability Details Report		□

Error Message

☑ Show checks with no violations found

FIGURE: **Job Error Messages** dialog box

Hint: You can check the **Show checks with no violation found** to display checks that did not detect any vulnerabilities during your Audit.

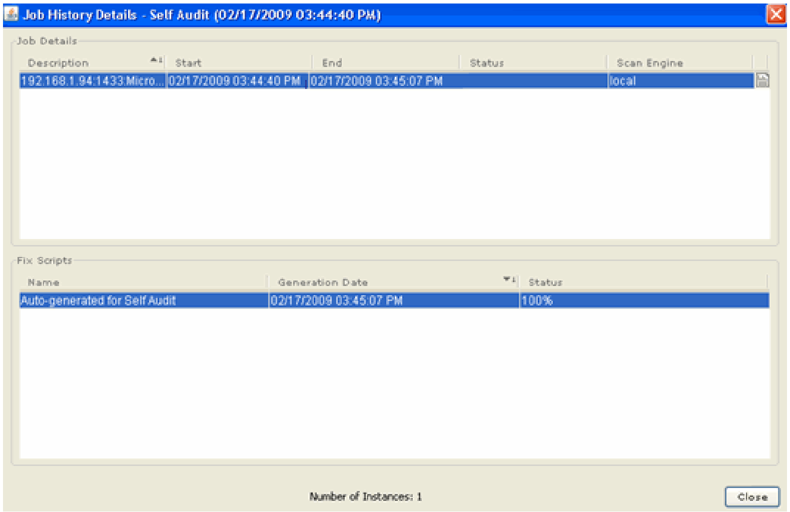
5. In the **Check Violation Messages** portion of the **Job Error Messages** dialog box, check the **Fix** checkbox next to one or more individual vulnerabilities.

6. Click the **Generate Fix Script** button at the bottom of the **Job Error Messages** dialog box).

DbProtect generates an "on demand" Fix Script to repair **individual vulnerabilities** (selected in Step 4) for the selected individual Audited database instance.

7. Click the **Close** button to close the **Job Error Messages** dialog box.
8. Do one of the following to display the **Job History Details** dialog box:
   - Double click a completed Audit Job.
   - Right click a completed Audit Job and choose **Show Details**.

The **Job History Details** dialog box is shown below.



Job History Details - Self Audit (02/17/2009 03:44:40 PM)

Job Details

Description	Start	End	Status	Scan Engine
192.168.1.94:1433:Micro...	02/17/2009 03:44:40 PM	02/17/2009 03:45:07 PM		local

Fix Scripts

Name	Generation Date	Status
Auto-generated for Self Audit	02/17/2009 03:45:07 PM	100%

Number of Instances: 1

FIGURE: **Job History Details** dialog box

The **Fix Scripts** portion of the **Job History Details** dialog box displays your "on demand" Fix Script.

You can:

- download the Fix Script and view its details; for more information, see *Downloading and viewing the details of a Fix Script*
- customize the Fix Script; for more information, see *Customizing a Fix Script*.

Automatically running a Fix Script

You can **automatically** generate a Fix Script (i.e., as soon as your Audit Job completes). to repair **all vulnerabilities** detected for **all Audited database instances**.

(Alternately, you can generate Fix Scripts "on demand", either for all vulnerabilities detected by an Audit, or for individual vulnerabilities; for more information, see *Running an "on-demand" Fix Script*.)

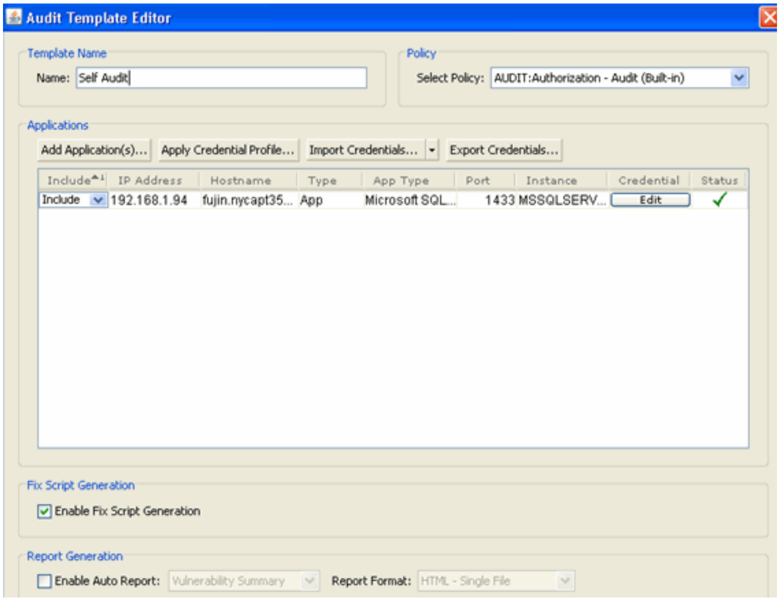
To automatically generate a Fix Script to repair **all vulnerabilities** detected for **all Audited database instances**:

Important: *Creating an Audit Job* and *Editing a Job* explain how to create and edit an Audit Job, respectively. The option to automatically generate a Fix Script is **just one part** of overall process of creating/editing an Audit Job.

1. If you are creating an Audit Job, do one of the following to display the **Audit Template Editor** dialog box:
   - Choose **Jobs** > **Templates** > **New Audit** from the menu.
   - Click the **Manage Jobs** tab, and choose **New Job** > **New Audit** in the **Job Setup Options** Toolbar on the **Manage Jobs** page.

   If you are editing an Audit Job, do one of the following to display the **Audit Template Editor** dialog box:
   - Right click the Job in the pane of the **Manage Jobs** page (**Job Setup** portion) and choose **Edit**.
   - Double click the Job in the pane of the **Manage Jobs** page (**Job Setup** portion).

The **Audit Template Editor** dialog box is shown below.



Audit Template Editor

Template Name

Name: Self Audit

Policy

Select Policy: AUDIT:Authorization - Audit (Built-in)

Applications

Include	IP Address	Hostname	Type	App Type	Port	Instance	Credential	Status
Include	192.168.1.94	fujin.nycapt35...	App	Microsoft SQL...	1433	MSSQLSERV...	Edit	✓

Fix Script Generation

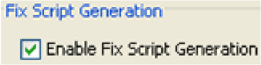
☑ Enable Fix Script Generation

Report Generation

☐ Enable Auto Report: Vulnerability Summary Report Format: HTML - Single File

FIGURE: **Audit Template Editor** dialog box

2. The **Fix Script Generation** section of the **Audit Template Editor** dialog box allows you to check the **Enable Fix Script Generation** checkbox (unchecked by default) to automatically generate a Fix Script to repair **all vulnerabilities** detected for **all database instances** that



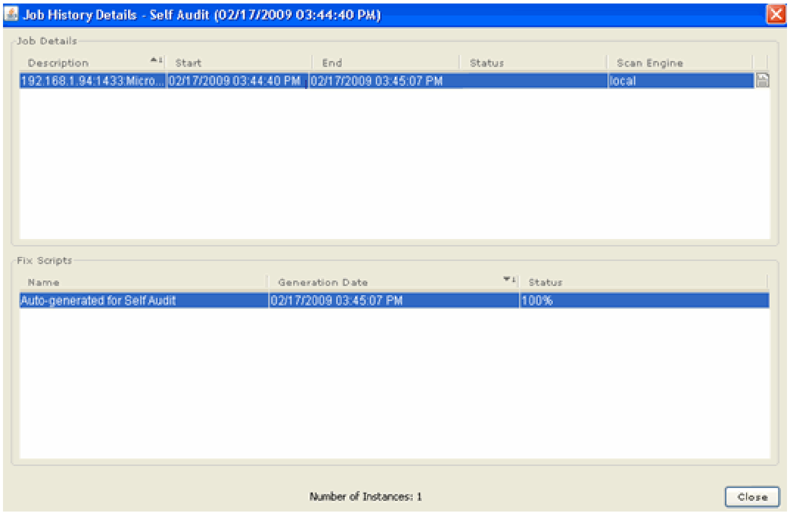
Fix Script Generation

☑ Enable Fix Script Generation

FIGURE: **Fix Script Generation** section of the **Audit Template Editor** dialog box

3. When your Audit Job completes, do one of the following to display the **Job History Details** dialog box:
   - Double click a completed Audit Job.
   - Right click a completed Audit Job and choose **Show Details**.

The **Job History Details** dialog box is shown below.



Job History Details - Self Audit (02/17/2009 03:44:40 PM)

Job Details

Description	Start	End	Status	Scan Engine
192.168.1.94:1433:Micro...	02/17/2009 03:44:40 PM	02/17/2009 03:45:07 PM		local

Fix Scripts

Name	Generation Date	Status
Auto-generated for Self Audit	02/17/2009 03:45:07 PM	100%

Number of Instances: 1

FIGURE: **Job History Details** dialog box

The **Fix Scripts** portion of the **Job History Details** dialog box displays your automatically-generated Fix Script.

You can:

- download the Fix Script and view its details; for more information, see *Downloading and viewing the details of a Fix Script*
- customize the Fix Script; for more information, see *Customizing a Fix Script*.

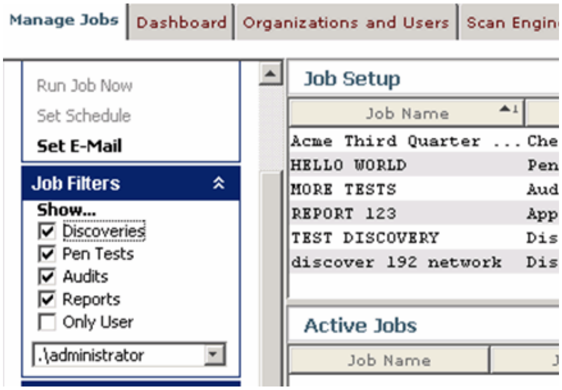
Downloading and viewing the details of a Fix Script

After you generate an "on demand" or automatic Fix Script (for more information, see *Running an "on-demand" Fix Script* and *Automatically running a Fix Script*, respectively), you can download and view the details of the Fix Script.

To download and view the details of a Fix Script:

1. Do one of the following to display the **Manage Jobs** page:

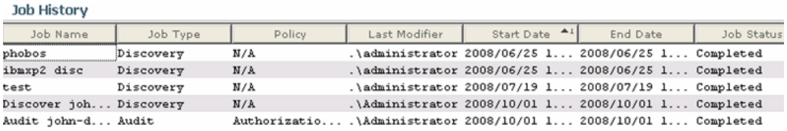
- Choose **Jobs** > **Manage** from the menu.
- Click the **Manage Jobs** tab.



Job Name	
Acme Third Quarter ...	Che
HELLO WORLD	Pen
MORE TESTS	Aud
REPORT 123	App
TEST DISCOVERY	Dis
discover 192 network	Dis

FIGURE: **Manage Jobs** page

2. Locate your completed Audit Jobs. They display in the **Job History** portion of the **Manage Jobs** page.



Job History

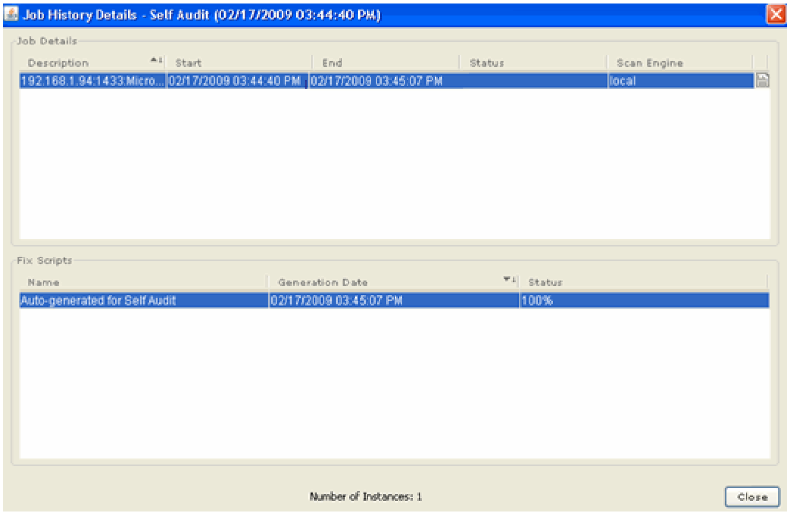
Job Name	Job Type	Policy	Last Modifier	Start Date	End Date	Job Status
phobos	Discovery	N/A	.\administrator	2008/06/25 1...	2008/06/25 1...	Completed
ibmxp2 disc	Discovery	N/A	.\administrator	2008/06/25 1...	2008/06/25 1...	Completed
test	Discovery	N/A	.\administrator	2008/07/19 1...	2008/07/19 1...	Completed
Discover joh...	Discovery	N/A	.\Administrator	2008/10/01 1...	2008/10/01 1...	Completed
Audit john-d...	Audit	Authorizatio...	.\Administrator	2008/10/01 1...	2008/10/01 1...	Completed

FIGURE: **Manage Jobs** page (**Job History** portion)

3. Do one of the following to display the **Job History Details** dialog box:

- Double click a completed Audit Job.
- Right click a completed Audit Job and choose **Show Details**.

The **Job History Details** dialog box is shown below.



Job History Details - Self Audit (02/17/2009 03:44:40 PM)

Job Details

Description	Start	End	Status	Scan Engine
192.168.1.94:1433:Micro...	02/17/2009 03:44:40 PM	02/17/2009 03:45:07 PM		local

Fix Scripts

Name	Generation Date	Status
Auto-generated for Self Audit	02/17/2009 03:45:07 PM	100%

Number of Instances: 1

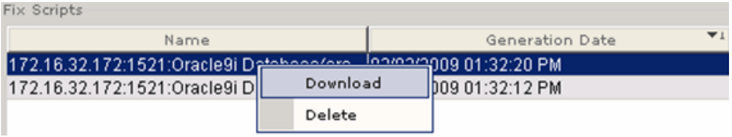
FIGURE: **Job History Details** dialog box

The lower **Fix Scripts** portion of the **Job History Details** dialog box displays information about any Fix Scripts that have already been run, including:

- **Name**
- **Generation Date**
- **Status**.

4. Do one of the following to download the Fix Script as a .zip file.

- Right click any completed Fix Script in the lower **Fix Scripts** portion of the **Job History Details** dialog box, and select **Download**.

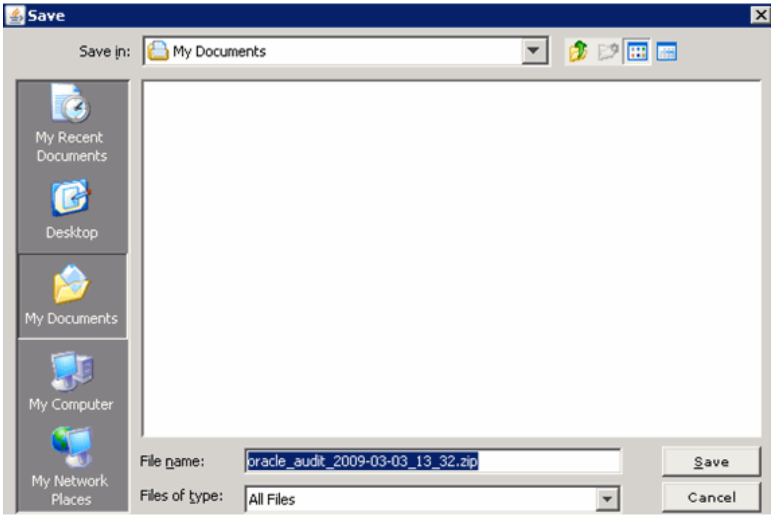


Fix Scripts

Name	Generation Date
172.16.32.172:1521:Oracle9i Database/ora	02/02/2009 01:32:20 PM
172.16.32.172:1521:Oracle9i D	009 01:32:12 PM

- Double click any completed Fix Script in the lower **Fix Scripts** portion of the **Job History Details** dialog box.

5. A **Save** dialog box displays, prompting you to save your Fix Script as a .zip file.



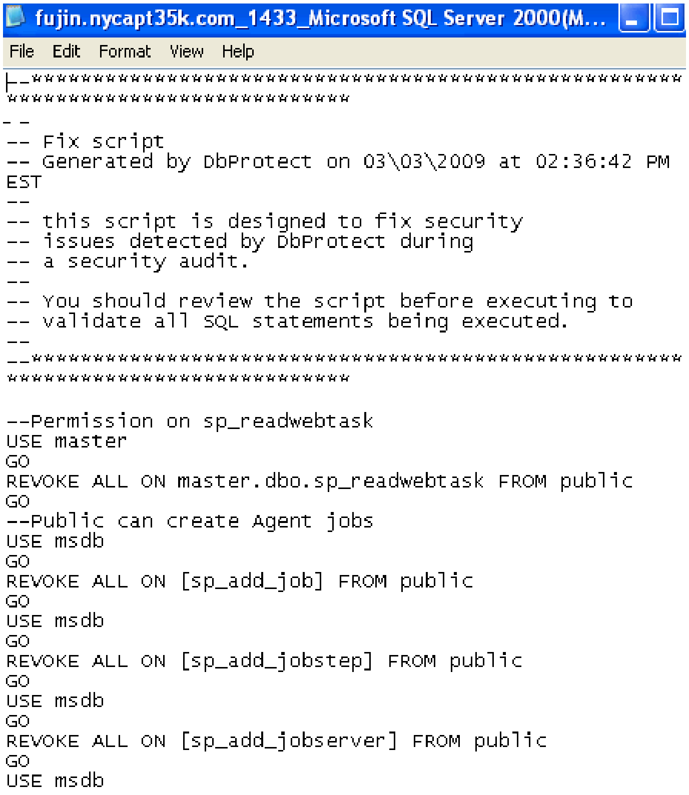
File name: oracle_audit_2009-03-03_13_32.zip

Files of type: All Files

FIGURE: **Save** dialog box

6. Save your Fix Script .zip file to a convenient location.

7. Unzip the Fix Script .zip file, and open individual Fix Scripts to view the SQL details. By default, Fix Scripts display in Notepad, as shown below (but you can select other applications).


fujin.nycapt35k.com_1433_Microsoft SQL Server 2000(M...
File Edit Format View Help

```
--*******************************************************
*****************************
- -
-- Fix script
-- Generated by DbProtect on 03\03\2009 at 02:36:42 PM
EST
--
-- this script is designed to fix security
-- issues detected by DbProtect during
-- a security audit.
--
-- You should review the script before executing to
-- validate all SQL statements being executed.
--
--*******************************************************
*****************************

--Permission on sp_readwebtask
USE master
GO
REVOKE ALL ON master.dbo.sp_readwebtask FROM public
GO
--Public can create Agent jobs
USE msdb
GO
REVOKE ALL ON [sp_add_job] FROM public
GO
USE msdb
GO
REVOKE ALL ON [sp_add_jobstep] FROM public
GO
USE msdb
GO
REVOKE ALL ON [sp_add_jobserver] FROM public
GO
USE msdb
```

FIGURE: Fix Script displayed in Notepad

You can customize the Fix Script before you deploy it to your database; for more information, see *Customizing a Fix Script*.

Customizing a Fix Script

Some Fix Scripts contain parameter placeholders that you need to replace before the you actually run the Fix Script. For example, if an Audit detects an easily-guessed password vulnerability, your DbProtect-generated Fix Script may look something like this:

```
--Easily-guessed password

USE master

GO

sp_password 'john', '<NEW PASSWORD>', 'john'

GO
```

Placeholders are enclosed in angle brackets. So, in this example, the placeholder is `<NEW PASSWORD>`. You should replace this placeholder value with the user's new password.

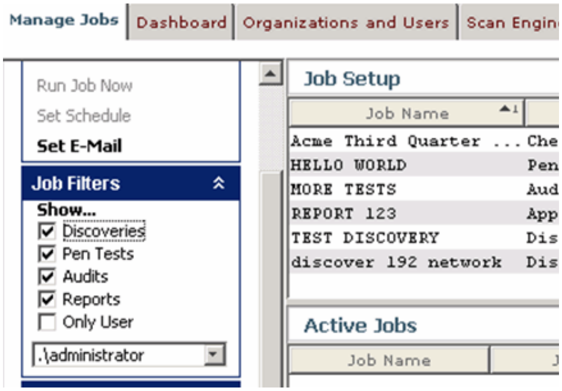
To customize a Fix Script:

1. Download and view a generated Fix Script, as explained in ***Downloading and viewing the details of a Fix Script***.
2. Customize the Fix Script using a standard text editing program like Notepad. Remember: placeholders are enclosed in angle brackets, e.g., `<NEW PASSWORD>`. When applicable, replace all placeholder values in Fix Script with actual values.
3. Save the Fix Script.

Deleting a Fix Script

To delete a Fix Script:

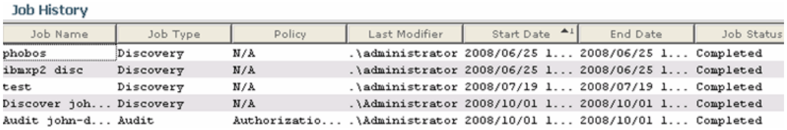
1. Do one of the following to display the **Manage Jobs** page:
   - Choose **Jobs** > **Manage** from the menu.
   - Click the **Manage Jobs** tab.



Job Name	
Acme Third Quarter ...	Che
HELLO WORLD	Pen
MORE TESTS	Aud
REPORT 123	App
TEST DISCOVERY	Dis
discover 192 network	Dis

FIGURE: **Manage Jobs** page

Locate your completed Audit Jobs. They display in the **Job History** portion of the **Manage Jobs** page.

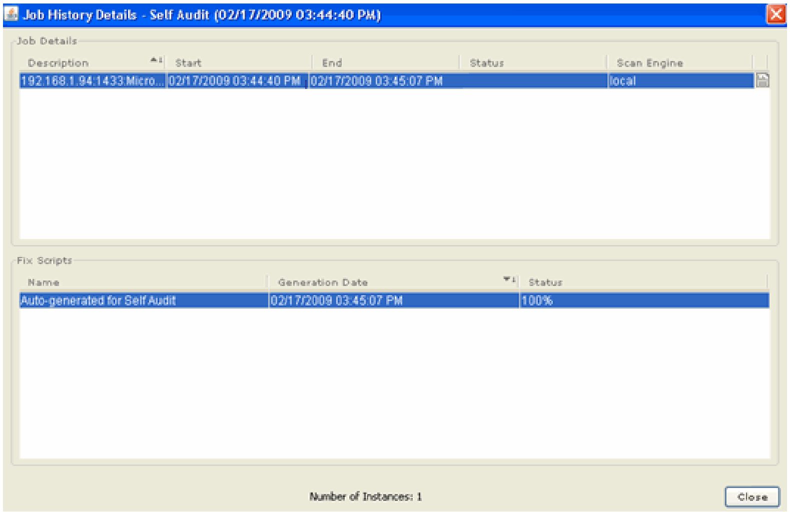

Job History

Job Name	Job Type	Policy	Last Modifier	Start Date	End Date	Job Status
phobos	Discovery	N/A	.\administrator	2008/06/25 1...	2008/06/25 1...	Completed
ibmxp2 disc	Discovery	N/A	.\administrator	2008/06/25 1...	2008/06/25 1...	Completed
test	Discovery	N/A	.\administrator	2008/07/19 1...	2008/07/19 1...	Completed
Discover joh...	Discovery	N/A	.\Administrator	2008/10/01 1...	2008/10/01 1...	Completed
Audit john-d...	Audit	Authorizatio...	.\Administrator	2008/10/01 1...	2008/10/01 1...	Completed

Manage Jobs page (**Job History** portion)

2. Do one of the following to display the **Job History Details** dialog box:

- Double click a completed Audit Job.
- Right click a completed Audit Job and choose **Show Details**.
- The **Job History Details** dialog box is shown below.



Job History Details - Self Audit (02/17/2009 03:44:40 PM)

Job Details

Description	Start	End	Status	Scan Engine
192.168.1.94:1433:Micro...	02/17/2009 03:44:40 PM	02/17/2009 03:45:07 PM		local

Fix Scripts

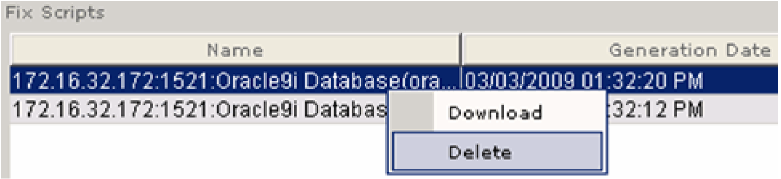
Name	Generation Date	Status
Auto-generated for Self Audit	02/17/2009 03:45:07 PM	100%

Number of Instances: 1

FIGURE: **Job History Details** dialog box

3. Do the following:

- Right click any completed Fix Scripts in the lower **Fix Scripts** portion of the **Job History Details** dialog box, and select **Delete**.



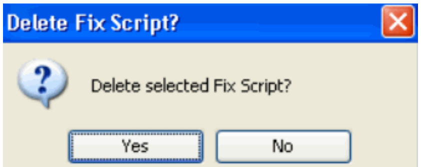
Fix Scripts

Name	Generation Date
172.16.32.172:1521:Oracle9i Database(ora...	03/03/2009 01:32:20 PM
172.16.32.172:1521:Oracle9i Databas	:32:12 PM

Hint: Click <CTRL> to highlight non-sequential Fix Scripts.

Caution! You **cannot** un-delete a deleted Fix Script.

- Right click any completed Fix Script in the lower **Fix Scripts** portion of the **Job History Details** dialog box.
- A **Delete Fix Script?** pop up prompts you to confirm the deletion.


Delete Fix Script?

Delete selected Fix Script?

FIGURE: **Delete Fix Script?** pop up

- Click the **Yes** button to delete the Fix Script(s).
- The deleted Fix Script(s) disappear from the lower **Fix Scripts** portion of the **Job History Details** dialog box.

Audit and Threat Management

A real-time database **Audit and Threat Management** solution, DbProtect delivers database-specific protection and alerting for best-in-class protection of enterprise organizations.

DbProtect allows you to create Policies and Filters and to tune your detection parameters to customize which audit and security events you want to monitor. This helps you focus security efforts on information that is relevant, while bypassing false positives and irrelevant events.

This chapter of the *DbProtect User’s Guide* discusses how to use **DbProtect Audit and Threat Management** features on your enterprise database applications.

This section consists of the following chapters:

- *Understanding the DbProtect Audit and Threat Management User Interface (UI)*
- *Audit and Threat Management User Roles*
- *Sensors*
- *Alerts*
- *Policies*
- *Dashboard*
- *Filters*
- *Reports*
- *System Settings: Email Forwarding Rules, Forwarding Settings, Email Server Settings.*

Understanding the DbProtect Audit and Threat Management User Interface (UI)

This chapter consists of the following topics:

- *What is the DbProtect Audit and Threat Management UI?*
- *DbProtect Audit and Threat Management UI components*
- *Navigating the DbProtect Audit and Threat Management UI using the tabs*
- *Navigating the DbProtect Audit and Threat Management UI using the workflow diagram*
- *Understanding result sets*.

What is the DbProtect Audit and Threat Management UI?

The **DbProtect Audit and Threat Management UI** is the web browser-based, graphical component of DbProtect that allows you to navigate to the various features of DbProtect Audit and Threat Management.

The **DbProtect Audit and Threat Management UI** is comprised of the:

- **Home** page; for more information, see *Understanding the Home page*
- **Alert Manager** page; for more information, see *Understanding the Alert Manager page*
- **Dashboard**; for more information, see *Understanding the Dashboard*
- **Report Manager** page; for more information, see *Understanding the Report Manager Page*
- **Policy Manager** page; for more information, see *Understanding the Policy Manager page*
- **Filter Manager** page; for more information, see *Understanding the Filter Manager page*
- **Sensor Manager** page; for more information, see *Understanding the Sensor Manager page*
- **System Settings** page; for more information, see *Understanding the System Settings page*.

UNDERSTANDING THE HOME PAGE

The **Home** page (shown below) contains tabs, which allow you to navigate the UI. Every UI page has tabs. For more information, see *Navigating the DbProtect Audit and Threat Management UI using the tabs*.

The **Home** page also includes a workflow diagram, which consists of:

- a graphical depiction of the DbProtect database monitoring and data tuning processes; for more information, see *Introduction/Next Steps portion of the DbProtect Audit and Threat Management workflow diagram*
- interactive **tools** with links to appropriate DbProtect Audit and Threat Management UI pages; for more information, see:

  -*Configuration Tools portion of the DbProtect Audit and Threat Management workflow diagram*

  -*Analysis Tools portion of the DbProtect Audit and Threat Management workflow diagram*

  -*Alerting Action tools portion of the DbProtect Audit and Threat Management workflow diagram*.

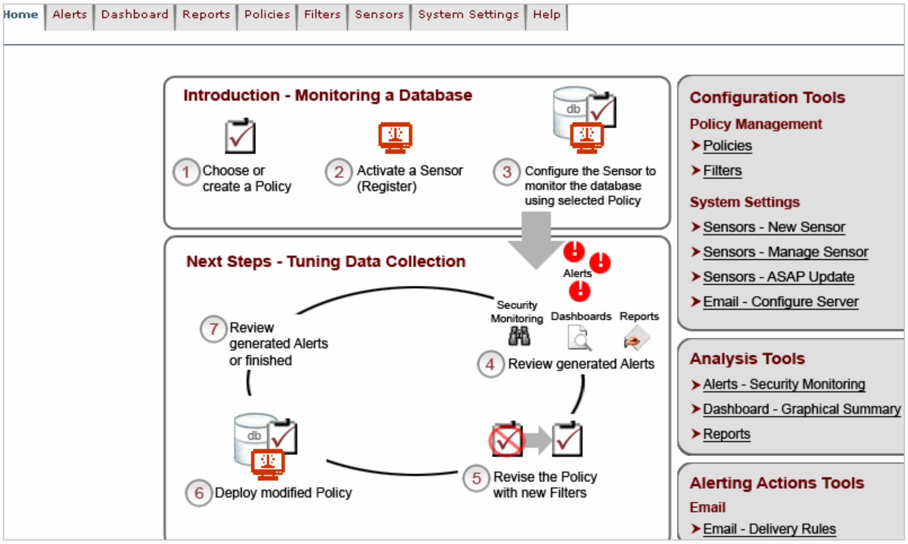


FIGURE: **Home** page

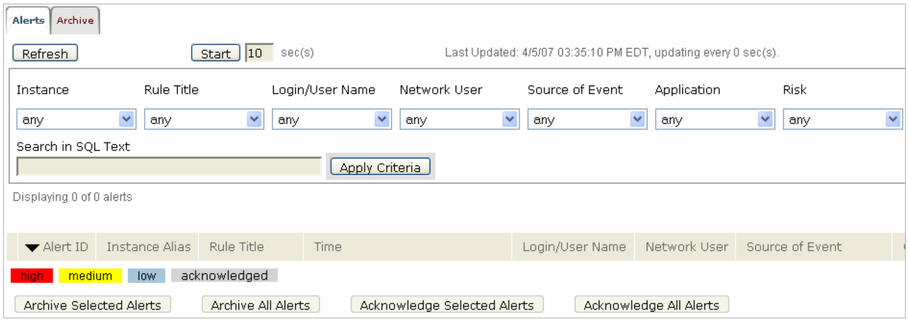
UNDERSTANDING THE ALERT MANAGER PAGE

The **Alert Manager** page (shown below) allows you to monitor, filter, archive, and delete Alerts. This page displays real-time Alerts, color-coded for easy identification of risk level. Sorting, grouping, and criteria matching features allow you to Filter views of incoming Alerts. The notification refresh rate is customizable; for more information, see *Monitoring, filtering, acknowledging, and archiving Alerts (via the Alert Manager)*.

DbProtect Audit and Threat Management only receives Alerts from properly-registered, -configured, and -deployed Sensors. In order to receive Alerts, you must:

- **install and initialize** a host-based or network-based Sensor on the database instance you want to monitor (explained in the *DbProtect Installation Guide*)
- **register** your Sensor (explained in *Registering a Sensor*)
- **configure** your Sensor and **deploy** it on your database instance (explained in *Understanding the Sensor Manager*).

For more information on using the monitoring Alerts via the **Alert Manager**, see *Monitoring, filtering, acknowledging, and archiving Alerts (via the Alert Manager)*.



10 sec(s)

Last Updated: 4/5/07 03:35:10 PM EDT, updating every 0 sec(s).

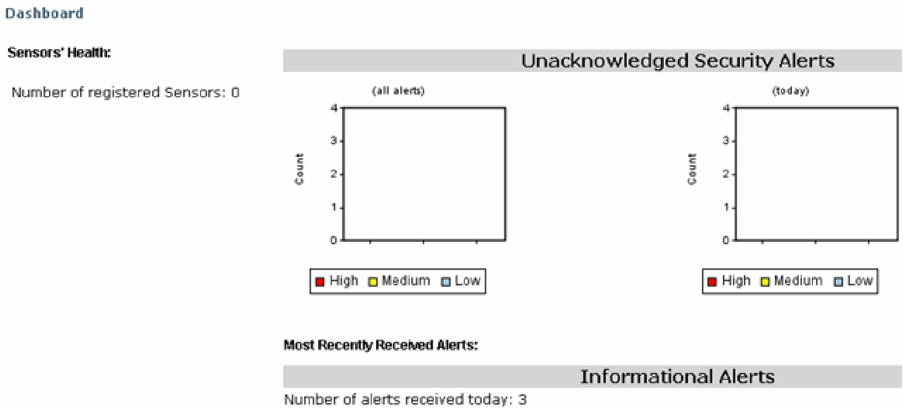
Instance	Rule Title	Login/User Name	Network User	Source of Event	Application	Risk
any	any	any	any	any	any	any

Displaying 0 of 0 alerts

FIGURE: **Alert Manager** page

UNDERSTANDING THE DASHBOARD

The **Dashboard** (shown below) provides a graphical, high-level summary of Alerts, audits, and total Alert volume. The **Dashboard** automatically refreshes itself every 30 seconds to update the display of new, real-time Alerts. In addition, the **Dashboard** allows you to drill down to the **Alert Manager**, and view Alert data in detail. For more information, see *Monitoring Alerts (via the Dashboard)*.



Dashboard

Sensors' Health:

Number of registered Sensors: 0

Unacknowledged Security Alerts

Most Recently Received Alerts:

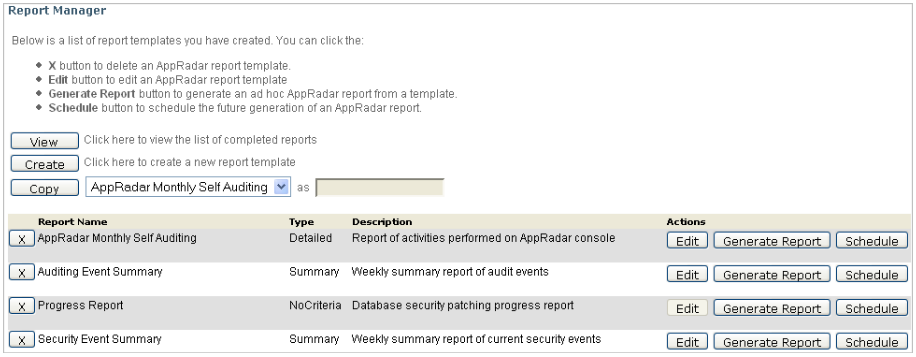
Informational Alerts

Number of alerts received today: 3

FIGURE: Dashboard

UNDERSTANDING THE REPORT MANAGER PAGE

The **Report Manager** page (shown below) allows you to create and manage the templates used to create Reports for Alerts generated by the Sensors. For more information, see *Understanding the Report Manager*.



Report Manager

Below is a list of report templates you have created. You can click the:

- **X** button to delete an AppRadar report template.
- **Edit** button to edit an AppRadar report template
- **Generate Report** button to generate an ad hoc AppRadar report from a template.
- **Schedule** button to schedule the future generation of an AppRadar report.

View Click here to view the list of completed reports

Create Click here to create a new report template

Copy AppRadar Monthly Self Auditing as

	Report Name	Type	Description	Actions
X	AppRadar Monthly Self Auditing	Detailed	Report of activities performed on AppRadar console	Edit Generate Report Schedule
X	Auditing Event Summary	Summary	Weekly summary report of audit events	Edit Generate Report Schedule
X	Progress Report	NoCriteria	Database security patching progress report	Edit Generate Report Schedule
X	Security Event Summary	Summary	Weekly summary report of current security events	Edit Generate Report Schedule

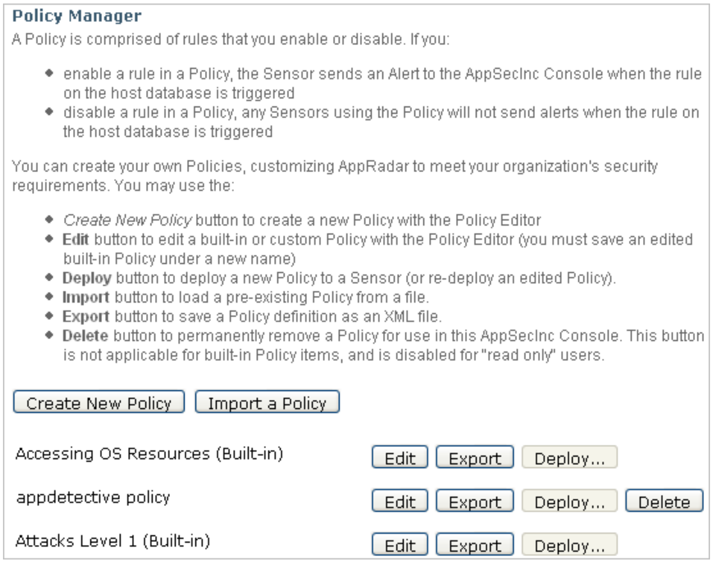
FIGURE: **Report Manager** page

UNDERSTANDING THE POLICY MANAGER PAGE

The **Policy Manager** page (shown below) allows you to create, edit, and deploy Policies which associate Alert-triggering Rules with the Sensors. This page also allows you to either **export** a Policy to use on another DbProtect Audit and Threat Management installation, or **import** a Policy created on another DbProtect Audit and Threat Management installation.

You deploy Policies at the database instance level. Each configured instance of a registered Sensor **must** have a Policy deployed to it (for more information, see *Configuring a Sensor and deploying the configuration information*). If you are monitoring multiple instances with a single Sensor, the Policy may or may not be the same for all instances.

For more information, see *Understanding the Policy Manager*.



Policy Manager

A Policy is comprised of rules that you enable or disable. If you:

- enable a rule in a Policy, the Sensor sends an Alert to the AppSecInc Console when the rule on the host database is triggered
- disable a rule in a Policy, any Sensors using the Policy will not send alerts when the rule on the host database is triggered

You can create your own Policies, customizing AppRadar to meet your organization's security requirements. You may use the:

- *Create New Policy* button to create a new Policy with the Policy Editor
- **Edit** button to edit a built-in or custom Policy with the Policy Editor (you must save an edited built-in Policy under a new name)
- **Deploy** button to deploy a new Policy to a Sensor (or re-deploy an edited Policy).
- **Import** button to load a pre-existing Policy from a file.
- **Export** button to save a Policy definition as an XML file.
- **Delete** button to permanently remove a Policy for use in this AppSecInc Console. This button is not applicable for built-in Policy items, and is disabled for "read only" users.

Accessing OS Resources (Built-in)

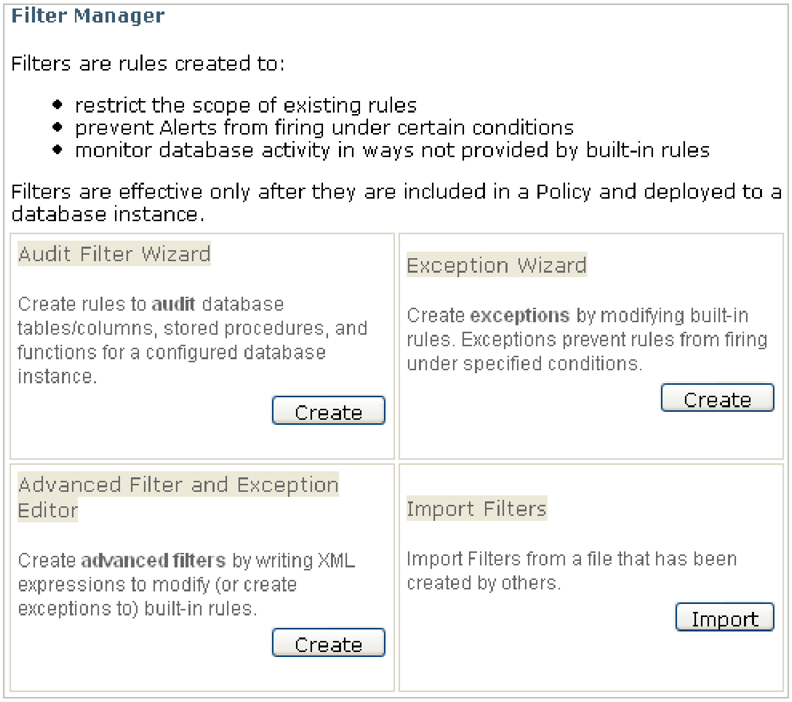
appdetective policy

Attacks Level 1 (Built-in)

FIGURE: **Policy Manager** page

UNDERSTANDING THE FILTER MANAGER PAGE

The **Filter Manager** page (shown below) allows you to create and edit Filters, which customize the functionality of built-in Rules and Policies. This page also allows you to import and export Filters. For more information, see *Understanding the Filter Manager*.



Filter Manager

Filters are rules created to:

- restrict the scope of existing rules
- prevent Alerts from firing under certain conditions
- monitor database activity in ways not provided by built-in rules

Filters are effective only after they are included in a Policy and deployed to a database instance.

Audit Filter Wizard

Create rules to **audit** database tables/columns, stored procedures, and functions for a configured database instance.

Exception Wizard

Create **exceptions** by modifying built-in rules. Exceptions prevent rules from firing under specified conditions.

Advanced Filter and Exception Editor

Create **advanced filters** by writing XML expressions to modify (or create exceptions to) built-in rules.

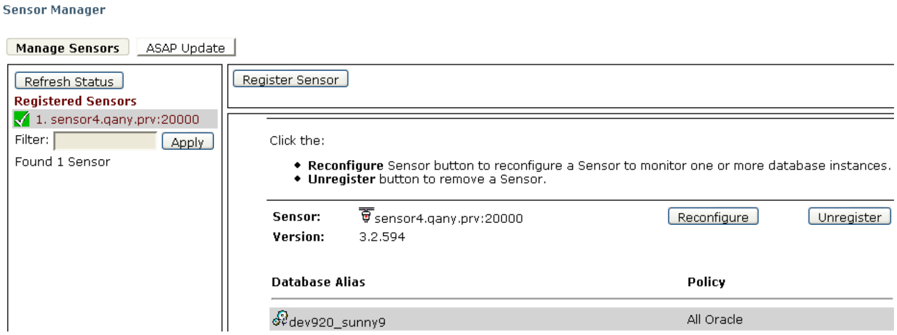
Import Filters

Import Filters from a file that has been created by others.

FIGURE: **Filter Manager**

UNDERSTANDING THE SENSOR MANAGER PAGE

The **Sensor Manager** page (shown below) allows you to configure and deploy registered Sensors. This page also allows you to perform an ASAP Update of a registered Sensor (i.e., downloading the latest version of DbProtect Audit and Threat Management). For more information, see *Configuring a Sensor and deploying the configuration information*.



Registered Sensors

✓ 1. sensor4.qany.prv:20000

Filter:

Found 1 Sensor

Click the:

- **Reconfigure** Sensor button to reconfigure a Sensor to monitor one or more database instances.
- **Unregister** button to remove a Sensor.

Sensor: sensor4.qany.prv:20000

Version: 3.2.594

Database Alias	Policy
dev920_sunny9	All Oracle

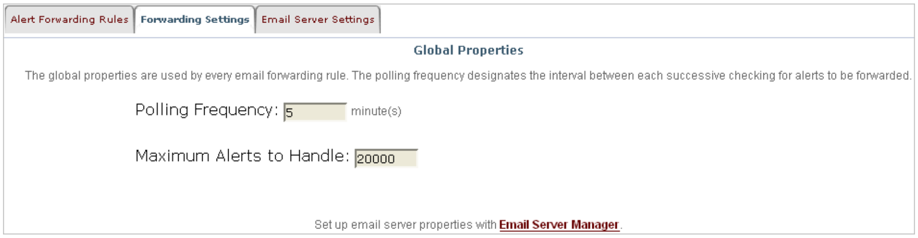
FIGURE: **Sensor Manager** page

UNDERSTANDING THE SYSTEM SETTINGS PAGE

The **System Settings** page (shown below) consists of the following sub-pages:

- **Email Forwarding Rules**, which allows you to email Alerts, instead of/in addition to the SNMP trap or file methods specified during the configuration/ deployment of an instance for a registered Sensor.
- **Forwarding Settings**, which allows you to specify the "polling frequency", i.e., the interval between each successive check for Alerts to be forwarded via email.
- **Email Server Settings**, which allows you to configure your email server to accommodate the forwarding of Alerts and Reports via email.

For more information, see *System Settings: Email Forwarding Rules, Forwarding Settings, Email Server Settings*.



Global Properties

The global properties are used by every email forwarding rule. The polling frequency designates the interval between each successive checking for alerts to be forwarded.

Polling Frequency: 5 minute(s)

Maximum Alerts to Handle: 20000

Set up email server properties with **Email Server Manager**.

FIGURE: **System Settings** page (**Forwarding Settings** tab selected)

DbProtect Audit and Threat Management UI components

A portion of the DbProtect Audit and Threat Management UI (the **Home** page) is shown below, with its parts labeled.

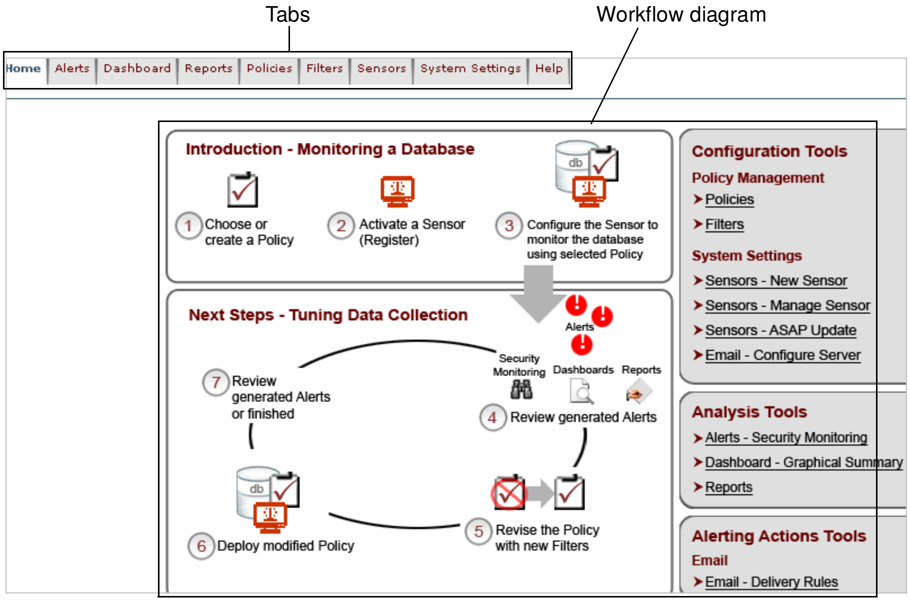


FIGURE: DbProtect Audit and Threat Management UI components (example from the **Home** page)

In addition, the upper right portion of every DbProtect Audit and Threat Management UI page displays your **User ID** and your associated "effective" **Organization**. If you are a Super User or an Admin User, and your User ID is associated with multiple Organizations, you can toggle between Organizations. For more information, see *Setting Your "Effective" Organization*.

For more information, on:

- how Organizations work in DbProtect, see *DbProtect Organizations, Users, and User Roles*
- user roles in DbProtect, see *DbProtect Organizations, Users, and User Roles*.

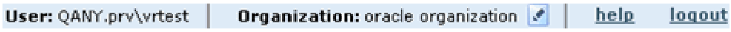

User: QANY.prv\vrtest | **Organization:** oracle organization | help logout

FIGURE: User ID/"effective" Organization information

Finally, the upper right portion of every DbProtect Audit and Threat Management UI page displays **Help** and **Logout** links, which allow you to display the online help and log out of DbProtect, respectively.

The **Home** page also has an interactive **workflow diagram**, which consists of:

- a graphical depiction of the DbProtect database monitoring and data tuning processes; for more information, see *Introduction/Next Steps portion of the DbProtect Audit and Threat Management workflow diagram*
- interactive **workflow links** to appropriate DbProtect Audit and Threat Management UI pages; for more information, see:

  -*Configuration Tools portion of the DbProtect Audit and Threat Management workflow diagram*,

  -*Analysis Tools portion of the DbProtect Audit and Threat Management workflow diagram*

  -*Alerting Action tools portion of the DbProtect Audit and Threat Management workflow diagram*.

Navigating the DbProtect Audit and Threat Management UI using the tabs

The upper portion of **every** DbProtect Audit and Threat Management UI page displays a row of **tabs**.

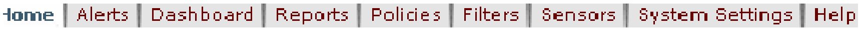


FIGURE: Tabs

From **every** DbProtect Audit and Threat Management UI page you can click the:

- **Home** tab to display the **Home** page.
- **Alerts** tab to display the **Alert Manager** page, which allows you to monitor, filter, archive, and delete Alerts. DbProtect Audit and Threat Management receives Alerts from your registered Sensors. For more information, see *Monitoring, filtering, acknowledging, and archiving Alerts (via the Alert Manager)*.
- **Dashboard** tab to display the **Dashboard**, which provides a graphical, high-level summary of Alerts, audits, and total Alert volume. It allows you to drill down to the **Alerts** page, and view Alert data in detail. For more information, see *Monitoring, filtering, acknowledging, and archiving Alerts (via the Alert Manager)*.
- **Reports** tab to display **Report Manager**, which allows you to create and manage Reports for Alerts generated by the Sensors. For more information, see *Understanding the Report Manager*.
- **Policies** tab to display the **Policy Manager**, which allows you to create, edit, and deploy Policies which associate Alert-triggering Rules with the Sensors. For more information, see *Understanding the Policy Manager*.
- **Filters** tab to display the **Filter Manager**, which allows you to create and edit Filters, which customize the functionality of built-in Rules and Policies. For more information, see *Understanding the Filter Manager*.
- **Sensors** tab to display the **Sensor Manager**, which allows you to configure and deploy registered Sensors. For more information, see *Configuring a Sensor and deploying the configuration information*.

- **System Settings** tab to display the **System Settings** page, which consists of the following sub-pages:

  -**Email Forwarding Rules**, which allows you to email Alerts, instead of/in addition to the SNMP trap or file methods specified during the configuration/deployment of an instance for a registered Sensor.

  -**Forwarding Settings**, which allows you to specify the “polling frequency”, i.e., the interval between each successive check for Alerts to be forwarded via email.

  -**Email Server Settings**, which allows you to configure your email server to accommodate the forwarding of Alerts and Reports via email.

  For more information, see ***System Settings: Email Forwarding Rules, Forwarding Settings, Email Server Settings***.

- **Help** tab to display the DbProtect Audit and Threat Management online help.

Navigating the DbProtect Audit and Threat Management UI using the workflow diagram

The **Home** page includes a DbProtect Audit and Threat Management **workflow diagram**.

Introduction and **Next Steps** portions

Workflow links

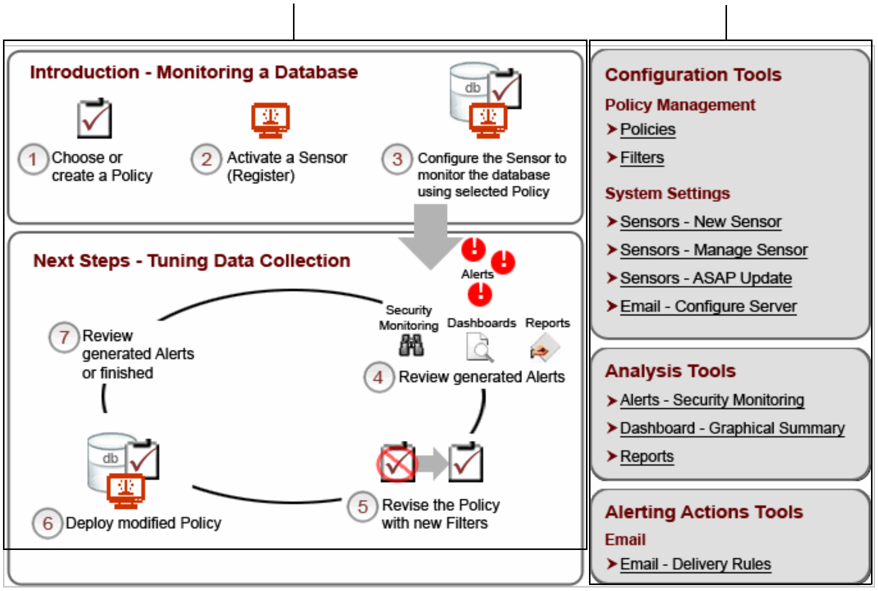

Introduction - Monitoring a Database
1 Choose or create a Policy
2 Activate a Sensor (Register)
db
3 Configure the Sensor to monitor the database using selected Policy
Next Steps - Tuning Data Collection
Alerts
Security Monitoring
Dashboards
Reports
4 Review generated Alerts
5 Revise the Policy with new Filters
db
6 Deploy modified Policy
7 Review generated Alerts or finished
Configuration Tools
Policy Management
Policies
Filters
System Settings
Sensors - New Sensor
Sensors - Manage Sensor
Sensors - ASAP Update
Email - Configure Server
Analysis Tools
Alerts - Security Monitoring
Dashboard - Graphical Summary
Reports
Alerting Actions Tools
Email
Email - Delivery Rules

FIGURE: DbProtect Audit and Threat Management workflow diagram (from the **Home** page)

The **Home** page workflow diagram consists of:

- a graphical depiction of the DbProtect database monitoring (i.e., the **Introduction - Monitoring a Database** portion of the **Home** page workflow diagram) and data tuning processes (i.e., the **Next Steps - Tuning Data Collection** portion of the **Home** page workflow diagram); for more information, see *Introduction/Next Steps portion of the DbProtect Audit and Threat Management workflow diagram*
- interactive **workflow links** to the appropriate DbProtect Audit and Threat Management pages; for more information, see:

  -*Configuration Tools portion of the DbProtect Audit and Threat Management workflow diagram*

  -*Analysis Tools portion of the DbProtect Audit and Threat Management workflow diagram*

  -*Alerting Action tools portion of the DbProtect Audit and Threat Management workflow diagram*.

INTRODUCTION/NEXT STEPS PORTION OF THE DBPROTECT AUDIT AND THREAT MANAGEMENT WORKFLOW DIAGRAM

The **Introduction/Next Steps** portion of the **Home** page workflow diagram is shown below.

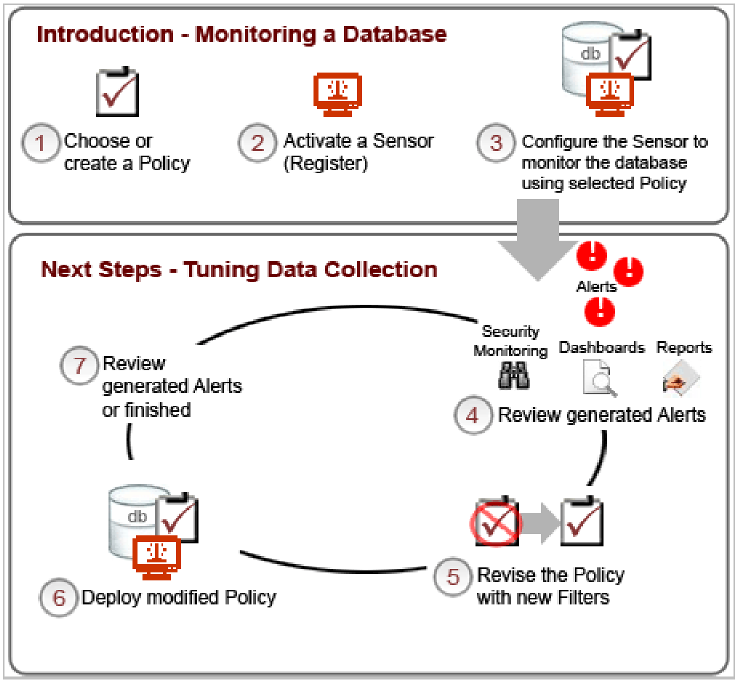

Introduction - Monitoring a Database
1 Choose or create a Policy
2 Activate a Sensor (Register)
db
3 Configure the Sensor to monitor the database using selected Policy
Next Steps - Tuning Data Collection
Alerts
Security Monitoring
Dashboards
Reports
4 Review generated Alerts
5 Revise the Policy with new Filters
db
6 Deploy modified Policy
7 Review generated Alerts or finished

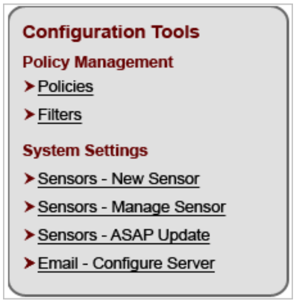
FIGURE: **Home** page workflow diagram (**Introduction/Next Steps** portion)

This portion of the **Home** page workflow diagram graphically depicts *how* DbProtect Audit and Threat Management works in a typical new customer scenario (following the successful installation of DbProtect and the successful installation/initialization of one or more Sensors). It consists of two parts, explained in the table below.

Part	Steps	For more information, see:
Introduction - Monitoring a Database	1. Choose or create a Policy	*Policies*
	2. Activate a Sensor (Register)	*Sensors*
	3. Configure the Sensor to monitor the database using selected Policy	
Next Steps - Tuning Data Collection	4. Review generated Alerts	*Alerts*
	5. Revise the Policy with new Filters	*Filters*
	6. Deploy modified Policy	*Policies*
	7. Review generated Alerts or finished	*Alerts*

CONFIGURATION TOOLS PORTION OF THE DBPROTECT AUDIT AND THREAT MANAGEMENT WORKFLOW DIAGRAM

The **Configuration Tools** portion of the **Home** page workflow diagram is shown below.


Configuration Tools

Policy Management

- Policies
- Filters

System Settings

- Sensors - New Sensor
- Sensors - Manage Sensor
- Sensors - ASAP Update
- Email - Configure Server

FIGURE: **Home** page workflow diagram (**Configuration Tools** portion)

This portion of the **Home** page workflow diagram (divided into **Policy Management** and **System Settings** sub-portions) allows you to click the:

- **Policies** workflow link (in the **Policy Management** sub-portion) to display the **Policy Manager**, which allows you to create, edit, and deploy Policies which associate Alert-triggering Rules with the Sensors. For more information, see *Understanding the Policy Manager*.

Note: You can also display the **Policy Manager** by clicking the **Policies** tab on any DbProtect Audit and Threat Management UI page. For more information on the tabs, see *Navigating the DbProtect Audit and Threat Management UI using the tabs.*

- **Filters** workflow link (in the **Policy Management** sub-portion) to display the **Filter Manager**, which allows you to create and edit Filters. Filters are used to customize the functionality of built-in Rules and Policies. For more information, see *Understanding the Filter Manager*.

Note: You can also display the **Filter Manager** by clicking the **Filters** tab on any DbProtect Audit and Threat Management UI page. For more information on the tabs, see *Navigating the DbProtect Audit and Threat Management UI using the tabs.*

- **Sensors - New Sensor** workflow link (in the **System Settings** sub-portion) to display the **Registration Manager**, which allows you to register and configure installed Sensors. Registration establishes a secure connection between the Sensor and DbProtect Audit and Threat Management, and enables the Sensor to receive Alerts. For more information, see *Registering a Sensor*.
- **Sensors - Manage Sensor** workflow link (in the **System Settings** sub-portion) to display the **Sensor Manager**, which allows you to configure and deploy your registered Sensors. For more information, see *Understanding the Sensor Manager*.

Note: You can also display the **Sensor Manager** by clicking the **Sensors** tab on any DbProtect Audit and Threat Management portal page. For more information on the tabs, see *Navigating the DbProtect Audit and Threat Management UI using the tabs.*

- **Sensors - ASAP Update** workflow link (in the **System Settings** sub-portion) to display the **Sensor Manager**, which allows you to perform an ASAP Update of your ASAP Updateable Sensors with the latest available security Rules. For more information, see *Performing an ASAP Update of Rules in your Sensors*.

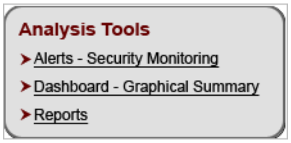
Note: You can also display the **Sensor Manager** by clicking the **Sensors** tab on any DbProtect Audit and Threat Management portal page. For more information on the tabs, see *Navigating the DbProtect Audit and Threat Management UI using the tabs.*

- **Email - Configure Server** workflow link (in the **System Settings** sub-portion) to display the **System Settings** page, which allows you to configure the properties of your outbound SMTP Server. DbProtect Audit and Threat Management uses these values to forward Alerts and send Reports via email. For more information, see *Understanding the System Settings page*.

Note: You can also display the **System Settings** page by clicking the **System Settings** tab on any DbProtect Audit and Threat Management UI page. For more information on the tabs, see *Navigating the DbProtect Audit and Threat Management UI using the tabs.*

ANALYSIS TOOLS PORTION OF THE DBPROTECT AUDIT AND THREAT MANAGEMENT WORKFLOW DIAGRAM

The **Analysis Tools** portion of the **Home** page workflow diagram is shown below.



Analysis Tools

- Alerts - Security Monitoring
- Dashboard - Graphical Summary
- Reports

FIGURE: DbProtect Audit and Threat Management workflow diagram (**Analysis Tools** portion)

This portion of the **Home** page workflow diagram allows you to click the:

- **Alerts - Security Monitoring** workflow link to display the **Alert Manager** page, which allows you to view or delete your archived Alerts, view/sort Alerts, filter Alerts, edit the Alert notification rate, edit the number of Alerts that display on the **Alert Manager**, acknowledge and archive your Alert, and to view your Alert detail. For more information, see *Understanding the Alert Manager*.

Note: You can also display the **Alert Manager** page by clicking the **Alerts** tab on any DbProtect Audit and Threat Management UI page. For more information on the tabs, see *Navigating the DbProtect Audit and Threat Management UI using the tabs.*

- **Dashboard - Graphical Summary** workflow link to display the **Dashboard**, which provides a graphical summary of Alerts, audits, and total Alert volume. For more information, see *Dashboard*.

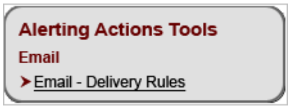
Note: You can also display the **Dashboard** by clicking the **Dashboard** tab on any DbProtect Audit and Threat Management UI page. For more information on the tabs, see *Navigating the DbProtect Audit and Threat Management UI using the tabs.*

- **Reports** workflow link to display the **Report Manager**, which allows you to run **Reports** on Alerts received from registered Sensors. A Report is a tabular and graphical display of the results of a query constrained by user-supplied criteria entered during the Report generation process. The **Report Manager** allows you to view a generated Report, create/copy/edit/delete Report templates, generate a Report now, or schedule a Report to get generated in the future.For more information, see *Understanding the Report Manager*.

Note: You can also display the **Report Manager** by clicking the **Reports** tab on any DbProtect Audit and Threat Management UI page. For more information on the tabs, see *Navigating the DbProtect Audit and Threat Management UI using the tabs.*

ALERTING ACTION TOOLS PORTION OF THE DBPROTECT AUDIT AND THREAT MANAGEMENT WORKFLOW DIAGRAM

The **Alerting Action Tools** portion of the **Home** page workflow diagram is shown below.



Alerting Actions Tools

Email

FIGURE: DbProtect Audit and Threat Management workflow diagram (**Alerting Action Tools** portion)

This portion of the DbProtect Audit and Threat Management workflow diagram allows you to click the **Email - Delivery Rules** link to display the **System Settings** page, which allows you to specify Email Forwarding Rules (i.e., user-defined criteria for forwarding your Alerts via email). When the criteria are met, DbProtect Audit and Threat Management emails the Alerts to your list of recipients, which is also specified in your Email Forwarding Rule. For more information, see *Email Forwarding Rules*.

Note: You can also display the **System Settings** page by clicking the **System Settings** tab on any DbProtect Audit and Threat Management UI page. For more information on the tabs, see *Navigating the DbProtect Audit and Threat Management UI using the tabs.*

Understanding result sets

Result sets refer to the number of **records returned** or **records affected** as the result of executing a SQL statement.

Caution! In some cases, DbProtect Audit and Threat Management does **not** return result sets. For example, DML statements indicate records affected, but DDL statements do **not**. Each database vendor's architecture is different. In the case of network-based Sensors for DB2, it also relies on the *client* requesting the number of records affected.

DbProtect Audit and Threat Management displays result set information in the following parts of the application:

- **Alert detail.** The Alert detail portion of the **Alert page** displays a count of records affected; *Monitoring, filtering, acknowledging, and archiving Alerts (via the Alert Manager)*.
- **Advanced Filter Wizard**. `RecordsAffected` is a valid SQL Server name attribute when writing expressions in the **Advanced Filter Wizard**; for more information, see *SQL Server name attributes*.

- **Reports.** The one built-in **Detail Report** (i.e., the **AppRadar Monthly Self-Auditing Report**) includes detailed values of "records affected"; for more information, see *Understanding the Built-In Auditing Event Summary Report*.

  The two built-in **Summary Reports** (i.e., the **Auditing Event Summary Report** and the **Security Event Summary Report**) only include a count of "records affected", but no details; for more information, see *Understanding the Built-In Auditing Event Summary Report* and *Understanding the Built-In Security Event Summary Report*, respectively.

Audit and Threat Management User Roles

For information on **Audit and Threat Management user roles**, and all other roles (and associated privileges) in DbProtect, see *DbProtect Organizations, Users, and User Roles*.

Sensors

This chapter consists of the following topics:

- *What is a Sensor?*
- *DbProtect audit and threat management limitations (based on Sensor type, activity, target database, and operating system)*
- *Monitoring Oracle databases on an Oracle RAC*
- *Monitoring Oracle databases in an Oracle Fail Safe cluster environment*
- *Troubleshooting connection problems between the Console and a Sensor installed on Microsoft Windows 2008*
- *Understanding the Sensor Manager*
- *Registering a Sensor*
- *Configuring a Sensor and deploying the configuration information*
- *Deleting configured Sensors*
- *Performing an ASAP Update of Rules in your Sensors*
- *Monitoring the “health” of your Sensors (via the Sensor Manager)*
- *Unregistering a Sensor*
- *Manually removing a Sensor.*

What is a Sensor?

Sensors monitor your database for a variety of events, such as intrusion attempts or auditing of normal usage.

Two types of **Sensors** are available:

- **host-based** to monitor your SQL Server, Oracle, Sybase, or DB2 databases
- **network-based** to monitor your Oracle, DB2, or Sybase databases.

The Sensor fires Alerts when a real-time monitored event occurs. For more information, see *What is an Alert?*

Important: For information on installing and uninstalling Sensors, including Sensors in a SQL Server cluster, see the *DbProtect Installation Guide*.

DbProtect audit and threat management limitations (based on Sensor type, activity, target database, and operating system)

DbProtect audit and threat management may have limitations based on the type of Sensor, the nature of the activity.

Network-based Sensors fire Alerts for **all** remote connections, e.g., from a web server communicating to its remote back-end database. However, they do **not** detect activity originating from the database host.

Host-based Sensors detect both local and remote attacks. However, they detect only successfully executed commands. For example, a vulnerable database system may permit a certain type of attack, and that attack causes the host-based Sensor to generate an Alert. Importantly, a patched system generally rejects the same command, thus preventing a host-based Sensor from detecting an attempted breach.

In the special case of **host-based monitoring of Oracle on Microsoft Windows**, Sensors use a hybrid of network-based and host-based architectures. These **"hybrid Sensors"** detect **all** attacks originating remotely, but only those local commands that are successfully executed. This does **not** apply to monitoring Oracle using a network-based Sensor, or using a host-based Sensor on any *nix platform (i.e., Solaris, AIX, HP-UX, or Red Hat Enterprise Linux) as these platforms follow the guidelines described above.

Any audit and threat management rules that do not follow the above guidelines have a note in their description indicating such discrepancies.

Monitoring Oracle databases on an Oracle RAC

If you installed a host-based Sensor for Oracle to monitor Oracle databases on an **Oracle RAC** (regardless of host platform) you must appropriately configure the host-based Sensor. For more information, see *Appendix C: Installing and Configuring a Host-Based Sensor for Oracle to Monitor Oracle Databases on an Oracle RAC*.

Monitoring Oracle databases in an Oracle Fail Safe cluster environment

If you installed a host-based Sensor for Oracle (on Windows) to monitor **Oracle databases in an Oracle Fail Safe cluster environment**, you must appropriately configure your:

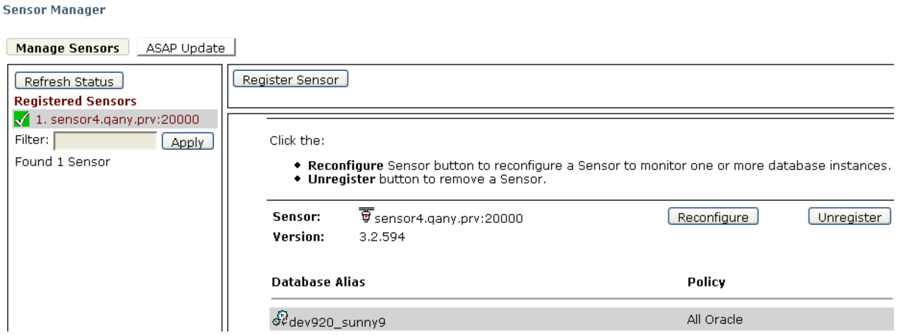
- host-based Sensor for Oracle (on Windows); for more information, see *Configuring a host-based Sensor to monitor Oracle SIDs and services and deploying the configuration information (when Sensor is installed on Windows)*
- Oracle Fail Safe cluster; for more information, see *Appendix B: Monitoring Oracle Databases in an Oracle Fail Safe Environment: Sensor and Cluster Configuration Steps*.

Troubleshooting connection problems between the Console and a Sensor installed on Microsoft Windows 2008

If you're having trouble establishing a connection between the Console and a Sensor installed on Microsoft Windows 2008 (i.e., a host-based Sensor for Oracle on Windows, a host-based Sensor for DB2 on Windows, a host-based Sensor for Microsoft SQL Server on Windows, or any network-based Sensor), make sure IPV6 support is **not** enabled on the network adapter, and that your Microsoft Windows Firewall is disabled.

Understanding the Sensor Manager

The **Sensor Manager** is shown below.



Registered Sensors

✓ 1. sensor4.qany.prv:20000

Filter:

Found 1 Sensor

Click the:

- **Reconfigure** Sensor button to reconfigure a Sensor to monitor one or more database instances.
- **Unregister** button to remove a Sensor.

Sensor: sensor4.qany.prv:20000

Version: 3.2.594

Database Alias	Policy
dev920_sunny9	All Oracle

FIGURE: Sensor Manager

The Sensor Manager allows you to:

- access the **Registration Manager** and register new Sensors; for more information, see *Registering a Sensor*
- configure and deploy your Sensors; for more information, see *Configuring a Sensor and deploying the configuration information*
- ASAP Update your ASAP Pocketable Sensors with the latest available security Rules; for more information, see *Performing an ASAP Update of Rules in your Sensors*
- monitor the "health" of your Sensors; for more information, see *Monitoring the "health" of your Sensors (via the Sensor Manager)*
- unregister Sensors; for more information, see *Unregistering a Sensor*.

Registering a Sensor

Once you have installed the DbProtect and installed/initialized your Sensors (for more information, see the *DbProtect Installation Guide*), you must use the **Registration Manager** to register each Sensor you want the DbProtect Audit and Threat Management to monitor.

Registration establishes a secure connection between DbProtect Audit and Threat Management and a Sensor. You can only register your Sensors through DbProtect Audit and Threat Management.

Note: If you plan to monitor a Microsoft SQL Server cluster, you only need to register and configure the Sensor that monitors a clustered Microsoft SQL Server instance **once** -- regardless of how many nodes are in your cluster.

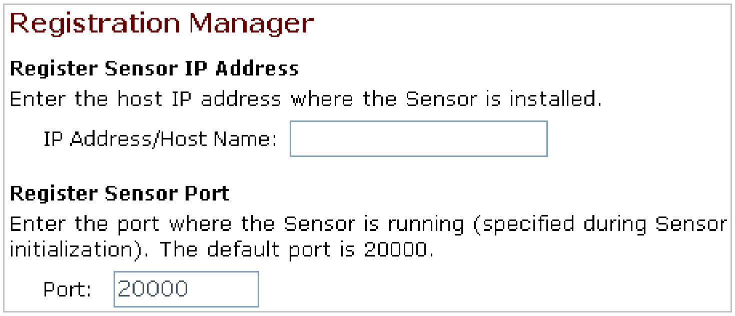
To register a Sensor (for Microsoft SQL Server, Oracle, Sybase, or DB2):

1. Do one of the following to display the **Registration Manager** page:

- Click the **Sensors - Manage Sensor** workflow link on the **Home** page to display the **Sensor Manager**, then click the **Registration Manager** link.

Note: If you have not registered any Sensors, the **Registration Manager** page displays when you click the **Sensors - Manage Sensor** workflow link.

- Click the **Sensors** tab from anywhere on the page to display the **Sensor Manager**, then click the **Registration Manager** link.



Registration Manager

Register Sensor IP Address

Enter the host IP address where the Sensor is installed.

IP Address/Host Name:

Register Sensor Port

Enter the port where the Sensor is running (specified during Sensor initialization). The default port is 20000.

Port: 20000

FIGURE: Registration Manager

2. In the **IP Address/Host Name** field, enter either the host IP address or the host name where the Sensor is installed.

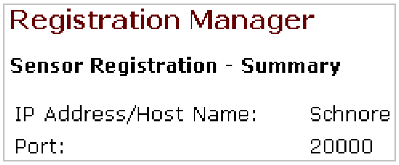
Note: If you are using Microsoft Clustering Services (MSCS), enter one of the following: a.) the Microsoft SQL Server Virtual Server name or, b.) the IP address associated with the Microsoft SQL Server Virtual Server name. Currently, DbProtect Audit and Threat Management only supports Microsoft SQL 2000 clusters.

3. In the **Port** field, enter the port where the Sensor is running (specified during Sensor initialization; for more information, see the *DbProtect Installation Guide*). This is the port where the Sensor "listens" for commands from DbProtect Audit and Threat Management. The default port is `20000`.

Note: At any time you can change the port number in the `sensor.xml` and `sensor_original.xml` files; for more information, see the *DbProtect Administrator's Guide*.

Specify which port number the Sensor should use to receive commands from the DbProtect Console. The default port (`20000`) is recommended for most configurations. If necessary, enter a different port number (`1-65535`). Consult your network administrator to determine which network port is acceptable. For more information, see the *DbProtect Installation Guide*.

4. Click the **Next** button to display the next **Registration Manager** page.



Registration Manager

Sensor Registration - Summary

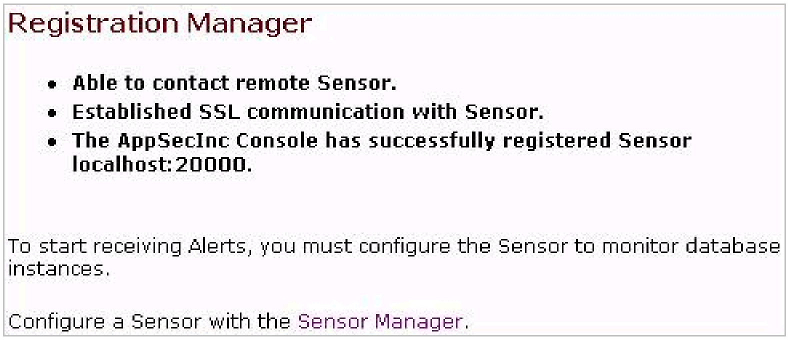
IP Address/Host Name:	Schnore
Port:	20000

FIGURE: Registration Manager

5. At this point, the **Registration Manager** has enough information to register your Sensor. If you:

   - want to review or change any settings you can click the **Back** button or any link that displays on the page
   - are satisfied with your settings and ready to register the Sensor, click the **Finish** button.

The **Registration Manager** confirmation page displays your registered Sensor information.



Registration Manager

- **Able to contact remote Sensor.**
- **Established SSL communication with Sensor.**
- **The AppSecInc Console has successfully registered Sensor localhost:20000.**

To start receiving Alerts, you must configure the Sensor to monitor database instances.

Configure a Sensor with the Sensor Manager.

FIGURE: **Registration Manager** confirmation page

6. Click the **Sensor Manager** link (or the **Sensors** tab) to display the **Sensor Manager** and configure your registered Sensor; for more information, see *Configuring a Sensor and deploying the configuration information.*

Configuring a Sensor and deploying the configuration information

After you install and register the Sensor, you must **configure** it to "listen" to your:

- SQL Server instances (host-based only)
- Oracle SIDs or services (host-based or network-based)
- DB2 database servers (host-based or network-based)
- Sybase database servers (host-based or network-based).

Configured Sensors fire Alerts when conditions in the deployed Policy are met. (Alerts are notifications to DbProtect of the occurrence of a monitored event on the database host. A Policy is a set of Rules which identifies the conditions under which Alerts are fired and sent to DbProtect.)

Note: DbProtect may have limitations based on the type of Sensor, the nature of the activity, the target database, and the operating system. For more information, see *DbProtect audit and threat management limitations (based on Sensor type, activity, target database, and operating system).*

Hint: If you have trouble establishing a connection between the Console and a Sensor installed on Microsoft Windows 2008 (i.e., a host-based Sensor for Oracle on Windows, a host-based Sensor for DB2 on Windows, a host-based Sensor for Microsoft SQL Server on Windows, or any network-based Sensor), make sure IPV6 support is **not** enabled on the network adapter, and that your Microsoft Windows Firewall is disabled.

After configuring the Sensor, you must **deploy** the configuration information to the Sensor.

This topic explains how to configure your:

- **host-based Sensor** to monitor a **SQL Server** instance and deploy the configuration information (when Sensor is installed on **Windows**); for more information, see *Configuring a host-based Sensor to monitor a SQL Server instance and deploying the configuration information (when Sensor is installed on Windows)*
- **host-based Sensor** to monitor a **DB2** database server and deploy the configuration information (when Sensor is installed on <u>**any**</u> **operating system**); for more information, see *Configuring a host-based Sensor to monitor a DB2 database server and deploying the configuration information (when Sensor is installed on any operating system)*
- **host-based Sensor** to monitor a **Sybase** database server and deploy the configuration information (when Sensor is installed on a supported *nix-based operating system, i.e., **Solaris** or **AIX**); for more information, see *Configuring a host-based Sensor to monitor Sybase databases and deploying the configuration information (when Sensor is installed on a supported *nix-based operating system)*
- **host-based Sensor** to monitor **Oracle** SIDs or services and deploy the configuration information (when Sensor is installed on **Windows** or on a *nix-based operating system, i.e., **Solaris, AIX, HP-UX, or Red Hat Enterprise Linux**); for more information, see:

  -Configuring a host-based Sensor to monitor Oracle SIDs and services and deploying the configuration information (when Sensor is installed on Windows)

  *-Configuring a host-based Sensor to monitor Oracle SIDs and services and deploying the configuration information (when Sensor is installed on a *nix-based operating system)*

Important: If you installed a host-based Sensor for Oracle to monitor Oracle databases on an Oracle RAC (regardless of host platform) you must appropriately configure the host-based Sensor. For more information, see *Appendix C: Installing and Configuring a Host-Based Sensor for Oracle to Monitor Oracle Databases on an Oracle RAC*.

- **network-based Sensor** to monitor a **Sybase** database server and deploy the configuration information (on **Windows**); for more information, see *Configuring a network-based Sensor to monitor a Sybase database server and deploying the configuration information (when Sensor is installed on Windows)*
- **network-based Sensor** to monitor a **DB2** database server and deploy the configuration information (on **Windows**); for more information, see *Configuring a network-based Sensor to monitor a DB2 database server and deploying the configuration information (when Sensor is installed on Windows)*
- **network-based Sensor** to monitor **Oracle** SIDs or services and deploy the configuration information (on **Windows**); for more information, see *Configuring a network-based Sensor to monitor Oracle SIDs and services and deploying the configuration information (when Sensor is installed on Windows)*.

CONFIGURING A HOST-BASED SENSOR TO MONITOR A SQL SERVER INSTANCE AND DEPLOYING THE CONFIGURATION INFORMATION (WHEN SENSOR IS INSTALLED ON WINDOWS)

Note: DbProtect audit and threat management may have limitations based on the type of Sensor, the nature of the activity, the target database, and the operating system.

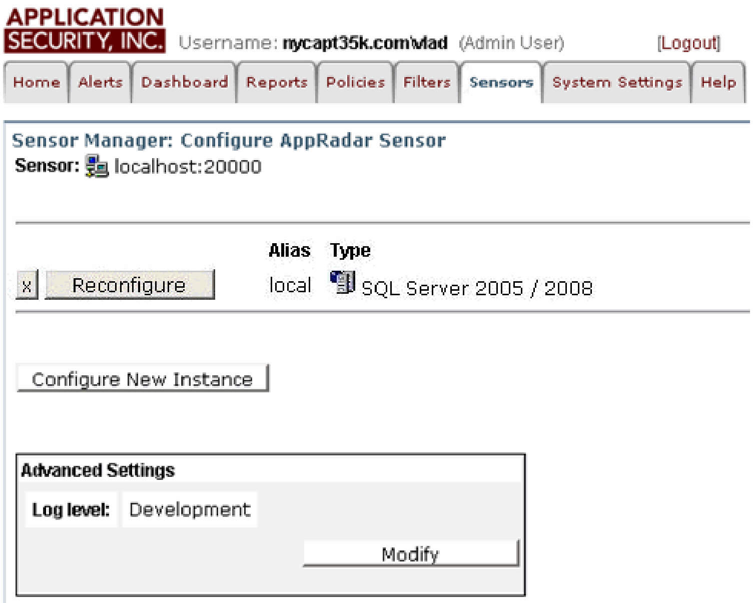
Host-based Sensors detect both local and remote attacks. However, they detect only successfully executed commands. For example, a vulnerable database system may permit a certain type of attack, and that attack causes the host-based Sensor to generate an Alert. Importantly, a patched system generally rejects the same command, thus preventing a host-based Sensor from detecting an attempted breach.

For more information, see *DbProtect audit and threat management limitations (based on Sensor type, activity, target database, and operating system).*

To configure a host-based Sensor to monitor a SQL Server instance and deploy the configuration information (when Sensor is installed on Windows):

1. Do one of the following to display the **Sensor Manager: Configure Sensor** page:
   - Click the **Sensors - Manage Sensor** workflow link on the **Home** page.
   - Click the **Sensors** tab from anywhere on the page.

2. The **Sensor Manager: Configure Sensor** page displays your registered Sensors.



Username: nycapt35k.com\vlad (Admin User)

Sensor Manager: Configure AppRadar Sensor

Sensor: localhost:20000

Alias	Type
local	SQL Server 2005 / 2008

Advanced Settings

Log level: Development

FIGURE: **Sensor Manager: Configure Sensor** page

This **Sensor Manager** page shows the:

- **Alias** of any host server you have configured for your Sensor
- database **Type** of the instance where your Sensor is registered
- database instance **(DB Instance)** where your Sensor is registered
- **Policy** associated with the registered Sensor.

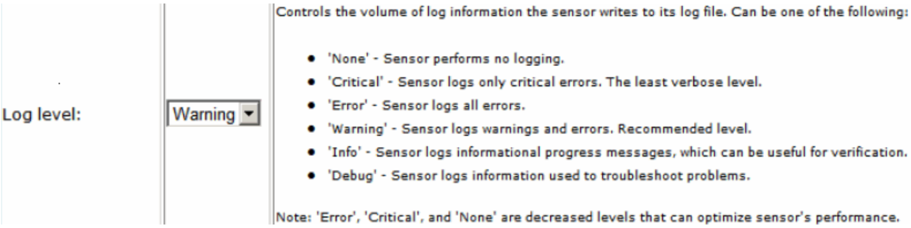
Note: The Console also displays whether the rules in your **Policy** are up-to-date or out-of-date. If a Policy is out-of-date, you can ASAP Update your Sensor with the latest security Rules (for more information, see *Performing an ASAP Update of Rules in your Sensors*), then use the **Policy Editor** to update Policies (deployed to your Sensors) with the new security Rules (for more information, see *Creating a Policy* and *Editing a Policy*).

You can click the:

- **Modify** button in the **Advanced Settings** portion of the page to display the **Advanced Sensor Settings** page, which allows you to select the Sensor's logging level (i.e., the volume of log information the Sensor outputs to its log file) (see Step 3)
- **Configure New Instance** button to configure a new **SQL Server instance** for the Sensor (see Steps 5-14)

- **Reconfigure** button to modify a current configuration of a **SQL Server instance** for the Sensor. See Steps 6-14)
- **X** button to delete a configured Sensor monitoring an instance; for more information, see *Deleting configured Sensors*.

The **Advanced Sensor Settings** page allows you to modify the Sensor's **logging level**.



Log level: Warning

Controls the volume of log information the sensor writes to its log file. Can be one of the following:

- 'None' - Sensor performs no logging.
- 'Critical' - Sensor logs only critical errors. The least verbose level.
- 'Error' - Sensor logs all errors.
- 'Warning' - Sensor logs warnings and errors. Recommended level.
- 'Info' - Sensor logs informational progress messages, which can be useful for verification.
- 'Debug' - Sensor logs information used to troubleshoot problems.

Note: 'Error', 'Critical', and 'None' are decreased levels that can optimize sensor's performance.

FIGURE: **Advanced Sensor Settings** page

Use the **Log level:** drop-down to select the Sensor's logging level, which controls the volume of log information the Sensor outputs to its log file. You can select:

- **None.** Sensor performs no logging.
- **Critical.** Sensor logs only critical errors. The **least** verbose level.
- **Error.** Sensor logs **all** errors.
- **Warning.** Sensor logs warnings and errors. Recommended level.
- **Info.** Sensor logs informational progress messages, which can be useful for verification.
- **Debug.** Logs information used to troubleshoot Sensor problems at runtime.

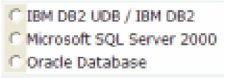
Note: **Error**, **Critical**, and **None** are all decreased logging levels which you can use to optimize Sensor performance.

When you're done, you can click the **Next** button to display the **Sensor Manager** page from Step 2. You can click the:

- **Configure New Instance** button to configure a new **SQL Server instance** for the Sensor (and go to Step 3)
- **Reconfigure** button to modify the current configuration of a **SQL Server instance** for the Sensor (and go to Step 4)
- **X** button to delete a configured Sensor monitoring an instance; for more information, see *Deleting configured Sensors*.

3. Configuring a new instance.

The **Sensor Manager** page prompts you to select a database platform for the host-based Sensor to monitor.

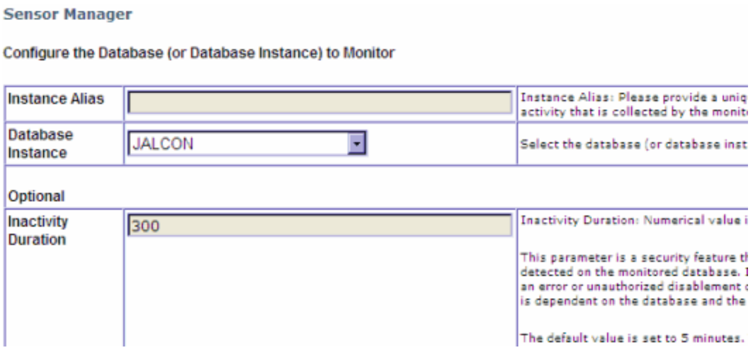


○ IBM DB2 UDB / IBM DB2
○ Microsoft SQL Server 2000
○ Oracle Database

FIGURE: **Sensor Manager** page

- Select **Microsoft SQL Server 2000/2005/2008**.
- Click the **Next** button.

The **Sensor Manager** page shown below allows you to configure/re-configure a Sensor for host-based **SQL Server**.



Sensor Manager

Configure the Database (or Database Instance) to Monitor

Instance Alias		Instance Alias: Please provide a uniq activity that is collected by the monit
Database Instance	JALCON	Select the database (or database inst
Optional		
Inactivity Duration	300	Inactivity Duration: Numerical value i This parameter is a security feature t detected on the monitored database. I an error or unauthorized disablement is dependent on the database and the The default value is set to 5 minutes.

FIGURE: Sensor Manager

- Enter a meaningful alias (e.g., `MEMBERSHIP MSSQL DB1`) in the **Instance Alias** field for the database instance you want this configuration of the Sensor to monitor. DbProtect Audit and Threat Management uses this alias to identify the SQL Server instance from which Alerts are received.

Important: The value you enter **must** start with a letter and is restricted to a maximum of 128 characters.Your instance alias can only contain alphanumeric, underscore (_), period (`.`), and hyphen (`-`) characters, or spaces. **Acceptable** examples: `MEMBERSHIP MSSQL DB1`, `MEMBERSHIP.MSSQLDB1`, `MEMBERSHIP_MSSQL_DB1`, `MEMBERSHIP-MSSQLDB1`, etc. **Unacceptable** examples: `MEMBERSHIP:MSSQLDB1`, `MEMBERSHIP/MSSQLDB1`, etc.

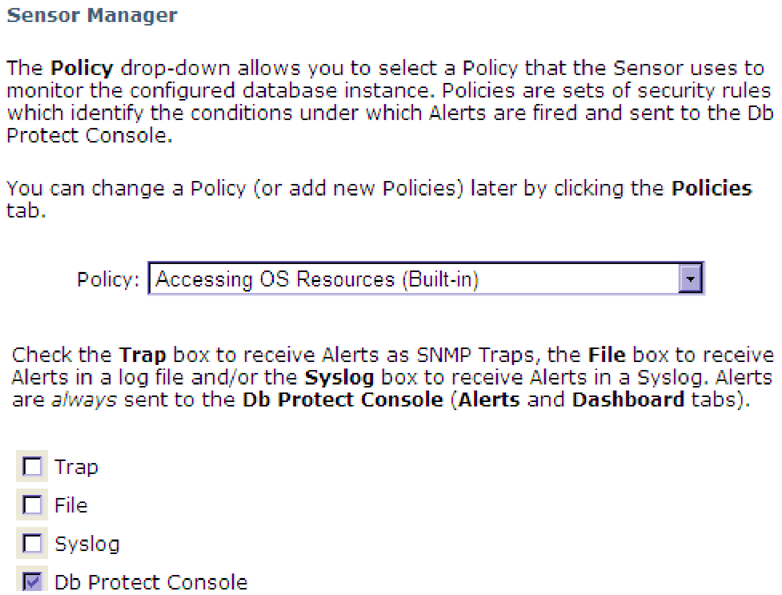
- Use the **Database instance** drop-down to select the SQL Server instance you want to monitor.

Note: If you are configuring the Sensor in a cluster, this value must be the instance of the virtual SQL Server server name that this Sensor should monitor. The virtual server name should automatically display in the drop-down list.

- Optionally, in the **Optional** portion of the page, you can modify the value in the **Inactivity duration** field. The "inactivity duration" is the amount of time (in seconds) that must elapse with no activity on the SQL Server instance before the Sensor generates an inactivity Alert. The default value is 5 minutes (`300` seconds). Valid values are `0` to `86400` seconds (i.e., 24 hours).

Note: Entering the value `0` (seconds) disables inactivity monitoring.

4. Click the **Next** button to display the next **Sensor Manager** page.



Sensor Manager

The **Policy** drop-down allows you to select a Policy that the Sensor uses to monitor the configured database instance. Policies are sets of security rules which identify the conditions under which Alerts are fired and sent to the Db Protect Console.

You can change a Policy (or add new Policies) later by clicking the **Policies** tab.

Policy: Accessing OS Resources (Built-in)

Check the **Trap** box to receive Alerts as SNMP Traps, the **File** box to receive Alerts in a log file and/or the **Syslog** box to receive Alerts in a Syslog. Alerts are *always* sent to the **Db Protect Console** (**Alerts** and **Dashboard** tabs).

☐ Trap

☐ File

☐ Syslog

☑ Db Protect Console

FIGURE: Sensor Manager

This page allows you to select a Policy the Sensor uses to monitor the configured SQL Server instance. Policies are sets of rules which identify the conditions under which Alerts are fired and sent to DbProtect Audit and Threat Management.

Use the **Policy:** drop-down to select a built-in or custom Policy that the Sensor will use to monitor the configured SQL Server instance.

Note: Deploying a Policy via the **Policy Manger** allows you to deploy Policies to multiple SQL Server instances simultaneously, which may (or may not) be monitored by the same Sensor. Additionally, you can change the Policies deployed (or deploy multiple additional Policies) any time by clicking the **Policies** tab; for more information, see *Deploying a Policy*.

5. The grayed-out **DbProtect Console** checkbox indicates Alerts are **always** sent to the DbProtect Console.

You can monitor these Alerts in real-time via the **Alert Manager** and the **Dashboard**; for more information, see *Monitoring, filtering, acknowledging, and archiving Alerts (via the Alert Manager)* and *Monitoring Alerts (via the Dashboard)* respectively. In addition, the **Report Manager** allows you to run **Detail Reports** and **Summary Reports** for Alerts.

Optionally, on this page you can check:

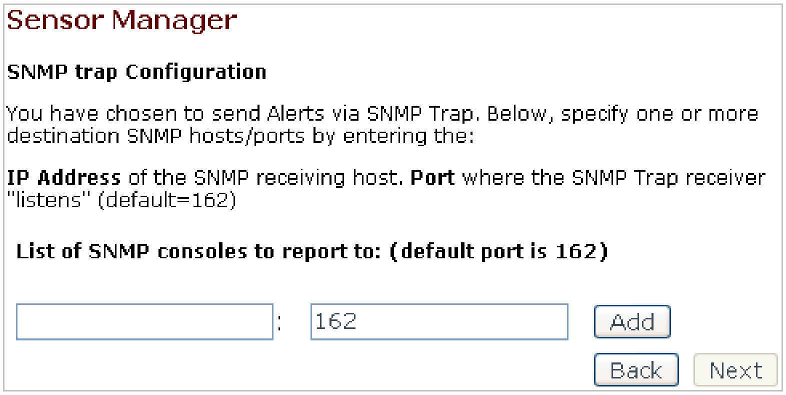
- **Trap** to receive Alerts also as SNMP traps
- **File** to receive Alerts also in a log file
- **Syslog** to receive Alerts also as Syslog messages.

6. Click the **Next** button. If you checked:

- **Trap**, then go to Step 7
- **File**, then go to Step 8
- **Syslog**, then go to Step 9.

7. Receiving Alerts as SNMP traps.

The **SNMP trap Configuration** page displays (if you checked **Trap**).



Sensor Manager

SNMP trap Configuration

You have chosen to send Alerts via SNMP Trap. Below, specify one or more destination SNMP hosts/ports by entering the:

IP Address of the SNMP receiving host. **Port** where the SNMP Trap receiver "listens" (default=162)

List of SNMP consoles to report to: (default port is 162)

: 162

FIGURE: Sensor Manager

- Specify the SNMP server **IP Address** (**not** the host name) of the SNMP receiving host, and the **port** number where the SNMP trap receiver "listens".

Note: The default port is `162`, not `80`.

- Optionally, click the **Add** button and specify an additional SNMP server IP Address (**not** the host name), and an additional port number of the target SNMP server where you want Alerts sent.
- When you're done, click the **Next** button.

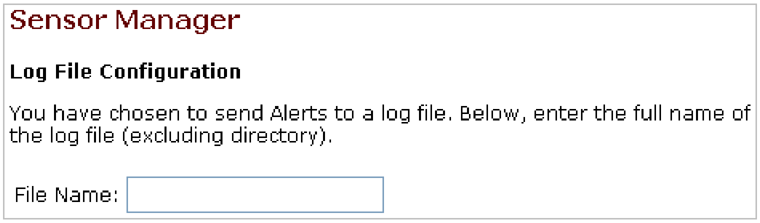
If you also checked:

- **File**, then go to Step 8
- **Syslog**, then go to Step 9.

Otherwise, go to Step 10.

8. Receiving Alerts as Log Files.

The **Log File Configuration** page displays (if you checked **File**).



Sensor Manager

Log File Configuration

You have chosen to send Alerts to a log file. Below, enter the full name of the log file (excluding directory).

File Name:

FIGURE: Sensor Manager

Do the following:

- Enter an Alert log file name in **File Name** field.

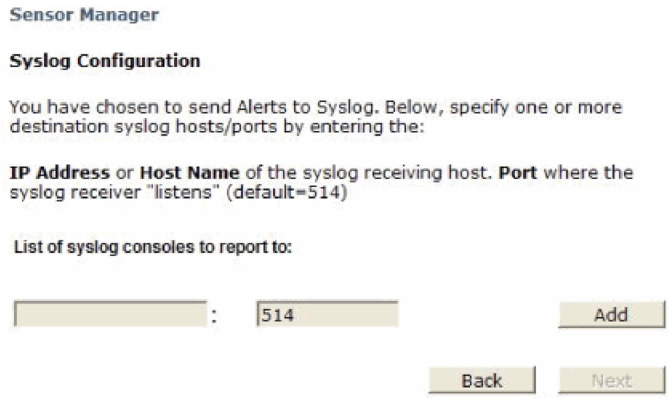
  Be sure to enter the full name of the log file (including the directory), and the log file's extension (e.g., `.txt`, `.rtf`, `.log`, etc.).

  The Alert log file is stored in the `Sensor_installation_directory\logs` directory, where `Sensor_installation_directory` is where the Sensor is installed.
- Click the **Next** button.

If you also checked **Syslog**, then go to Step 9. Otherwise, go to Step 10.

9. Receiving Alerts as Syslog messages.

The **Syslog File Configuration** page displays (if you checked **Syslog**). For a sample Syslog message, see the *DbProtect Administrator's Guide*.



Sensor Manager

Syslog Configuration

You have chosen to send Alerts to Syslog. Below, specify one or more destination syslog hosts/ports by entering the:

IP Address or **Host Name** of the syslog receiving host. **Port** where the syslog receiver "listens" (default=514)

List of syslog consoles to report to:

FIGURE: Sensor Manager

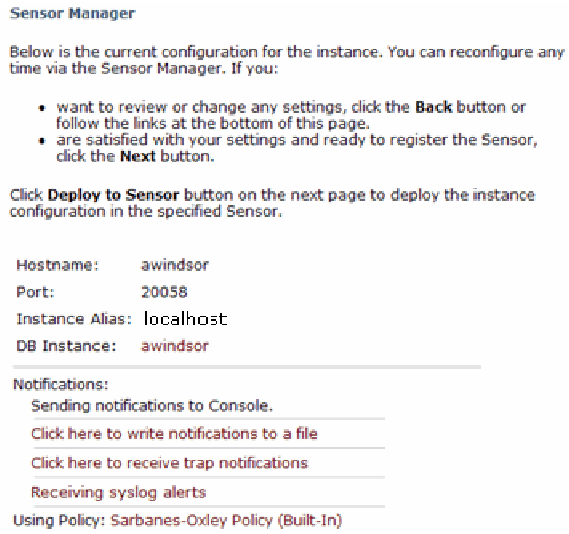
- Specify the Syslog server IP Address (or the host name), and the port number of the target Syslog server where you want Alerts sent.

Note: The default port is `514` (not `80`).

Caution! The Syslog port is a User Datagram Protocol (UDP) port, as opposed to Transmission Control Protocol (TCP).

- Optionally, click the **Add** button and specify an additional Syslog server IP Address (or the host name), and an additional port number of the target Syslog server where you want Alerts sent.
- When you're done, click the **Next** button.

After you finish specifying the SNMP trap, and/or log file, and/or Syslog parameters, then the **Sensor Manager** summary page displays.



Sensor Manager

Below is the current configuration for the instance. You can reconfigure any time via the Sensor Manager. If you:

- want to review or change any settings, click the **Back** button or follow the links at the bottom of this page.
- are satisfied with your settings and ready to register the Sensor, click the **Next** button.

Click **Deploy to Sensor** button on the next page to deploy the instance configuration in the specified Sensor.

Hostname:	awindsor
Port:	20058
Instance Alias:	localhost
DB Instance:	awindsor

Notifications:

Sending notifications to Console.

Click here to write notifications to a file

Click here to receive trap notifications

Receiving syslog alerts

Using Policy: Sarbanes-Oxley Policy (Built-In)

FIGURE: Sensor Manager

If you:

- want to review or change any settings you can click the **Back** button or any link that displays on the page
- are satisfied with your settings and ready to deploy the configuration to the Sensor, click the **Next** button.

Note: You can reconfigure the Sensor any time via the Sensor Manager.

The **Sensor Manager** page re-displays.

10. In the bottom, right corner of the page you can click the:

- **Deploy to Sensor** button to deploy this configured instance to the specified Sensor
- **Cancel** button to cancel the Sensor configuration.

Caution! All your configuration changes will be lost if you click the **Cancel** button.

FIGURE: **Cancel** and **Deploy to Sensor** buttons

Or you can click the:

- **Reconfigure Sensor** button to reconfigure the Sensor before deploying the instance configuration in the specified Sensor
- **Configure New Instance** button, if available (for a host-based Sensor, this button may be disabled if DbProtect Audit and Threat Management does **not** detect additional database instances for this server).

CONFIGURING A HOST-BASED SENSOR TO MONITOR A DB2 DATABASE SERVER AND DEPLOYING THE CONFIGURATION INFORMATION (WHEN SENSOR IS INSTALLED ON ANY OPERATING SYSTEM)

Note: DbProtect Audit and Threat Management may have limitations based on the type of Sensor, the nature of the activity, the target database, and the operating system.

Host-based Sensors detect both local and remote attacks. However, they detect only successfully executed commands. For example, a vulnerable database system may permit a certain type of attack, and that attack causes the host-based Sensor to generate an Alert. Importantly, a patched system generally rejects the same command, thus preventing a host-based Sensor from detecting an attempted breach.

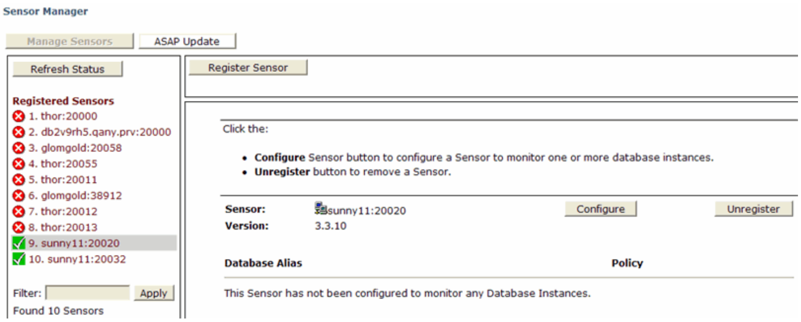
For more information, see *DbProtect audit and threat management limitations (based on Sensor type, activity, target database, and operating system).*

To configure a host-based Sensor to monitor a DB2 database server and deploy the configuration information (when Sensor is installed on any operating system, i.e., Windows, Red Hat Enterprise Linux, Solaris, and AIX):

1. Do one of the following to display the **Sensor Manager** page:

- Click the **Sensors - Manage Sensor** workflow link on the **Home** page.
- Click the **Sensors** tab from anywhere on the page.

The first **Sensor Manager** page displays your registered Sensors.



Registered Sensors

1. thor:20000
2. db2v9rh5.qany.prv:20000
3. glomgold:20058
4. thor:20055
5. thor:20011
6. glomgold:38912
7. thor:20012
8. thor:20013
9. sunny11:20020
10. sunny11:20032

Filter:

Found 10 Sensors

Click the:

- **Configure** Sensor button to configure a Sensor to monitor one or more database instances.
- **Unregister** button to remove a Sensor.

Sensor: sunny11:20020

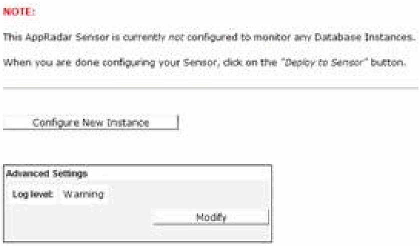
Version: 3.3.10

Database Alias	Policy
This Sensor has not been configured to monitor any Database Instances.	

FIGURE: Sensor Manager

2. Click the **Configure** button (if you are configuring a Sensor for the first time), or the **Reconfigure** button (if you are reconfiguring a Sensor).

The next **Sensor Manager** page displays.



NOTE:

This AppRadar Sensor is currently *not* configured to monitor any Database Instances.

When you are done configuring your Sensor, click on the *"Deploy to Sensor"* button.

Log level: Warning

FIGURE: Sensor Manager

This **Sensor Manager** page shows the:

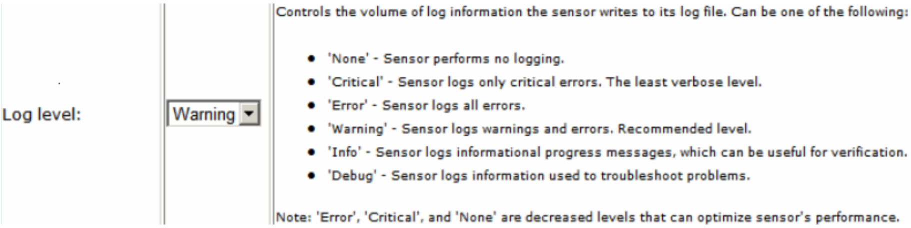
- **Alias** of any host server you have configured for your Sensor
- database **Type** of the instance where your Sensor is registered
- database instance **(DB Instance)** where your Sensor is registered
- **Policy** associated with the registered Sensor.

Note: The Console also displays whether the rules in your **Policy** are up-to-date or out-of-date. If a Policy is out-of-date, you can ASAP Update your Sensor with the latest security Rules (for more information, see *Performing an ASAP Update of Rules in your Sensors*), then use the **Policy Editor** to update Policies (deployed to your Sensors) with the new security Rules (for more information, see *Creating a Policy* and *Editing a Policy*).

When you're done, you can click the:

- **Modify** button in the **Advanced Settings** portion of the page to display the **Advanced Sensor Settings** page, which allows you to select the Sensor's **logging level** (and go to Step 3)
- **Configure New Instance** button to configure a new **DB2 database server** for the Sensor (and go to Step 4)
- **Reconfigure** button to modify the current configuration of a **DB2 database server** for the Sensor (and go to Step 5)
- **X** button to delete a configured Sensor monitoring an instance; for more information, see *Deleting configured Sensors*.

3. The **Advanced Sensor Settings** page allows you to modify the Sensor's **logging level**.



Log level: Warning

Controls the volume of log information the sensor writes to its log file. Can be one of the following:

- 'None' - Sensor performs no logging.
- 'Critical' - Sensor logs only critical errors. The least verbose level.
- 'Error' - Sensor logs all errors.
- 'Warning' - Sensor logs warnings and errors. Recommended level.
- 'Info' - Sensor logs informational progress messages, which can be useful for verification.
- 'Debug' - Sensor logs information used to troubleshoot problems.

Note: 'Error', 'Critical', and 'None' are decreased levels that can optimize sensor's performance.

FIGURE: **Advanced Sensor Settings** page

To modify the Sensor's logging level:

Use the **Log level:** drop-down to select the Sensor's logging level, which controls the volume of log information the Sensor outputs to its log file. You can select:

- **None.** Sensor performs no logging.
- **Critical.** Sensor logs only critical errors. The **least** verbose level.
- **Error.** Sensor logs **all** errors.
- **Warning.** Sensor logs warnings and errors. Recommended level.
- **Info.** Sensor logs informational progress messages, which can be useful for verification.
- **Debug.** Logs information used to troubleshoot Sensor problems at runtime.

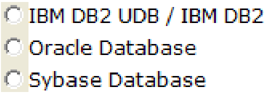
Note: **Error**, **Critical**, and **None** are all decreased logging levels which you can use to optimize Sensor performance.

When you're done, you can click the **Next** button to re-display the second **Sensor Manager** page (see Step 2), then click the:

- **Configure New Instance** button to configure a new **DB2 database server** for the Sensor (and go to Step 4)
- **Reconfigure** button to modify the current configuration of a **DB2 database server** for the Sensor (and go to Step 5)
- **X** button to delete a configured Sensor monitoring an instance; for more information, see *Deleting configured Sensors*.

4. Configuring a **new** instance.

The **Sensor Manager** page prompts you to select a database platform for the host-based Sensor to monitor.



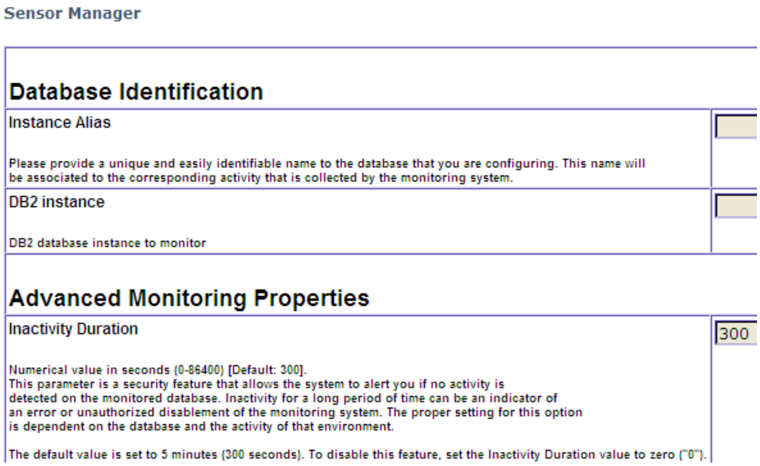
○ IBM DB2 UDB / IBM DB2
○ Oracle Database
○ Sybase Database

FIGURE: **Sensor Manager** page

Note: Microsoft SQL Server 2000 does not display as an option if your host-based Sensor for DB2 is installed on a *nix operating system.

- Select **IBM DB2 UDB / IBM DB2**.
- Click the **Next** button.

5. The **Sensor Manager** page shown below allows you to **configure/re-configure** a Sensor for host-based **DB2**.



Sensor Manager

Database Identification

Instance Alias

Please provide a unique and easily identifiable name to the database that you are configuring. This name will be associated to the corresponding activity that is collected by the monitoring system.

DB2 instance

DB2 database instance to monitor

Advanced Monitoring Properties

Inactivity Duration: 300

Numerical value in seconds (0-86400) [Default: 300].
This parameter is a security feature that allows the system to alert you if no activity is detected on the monitored database. Inactivity for a long period of time can be an indicator of an error or unauthorized disablement of the monitoring system. The proper setting for this option is dependent on the database and the activity of that environment.

The default value is set to 5 minutes (300 seconds). To disable this feature, set the Inactivity Duration value to zero ("0").

FIGURE: Sensor Manager

Do the following:

- Enter a meaningful DB2 database server alias (e.g., `DB2_JAPAN`) in the **Instance Alias:** field for the database instance you want this configuration of the Sensor to monitor. DbProtect uses this alias to identify the DB2 database server from which Alerts are received.

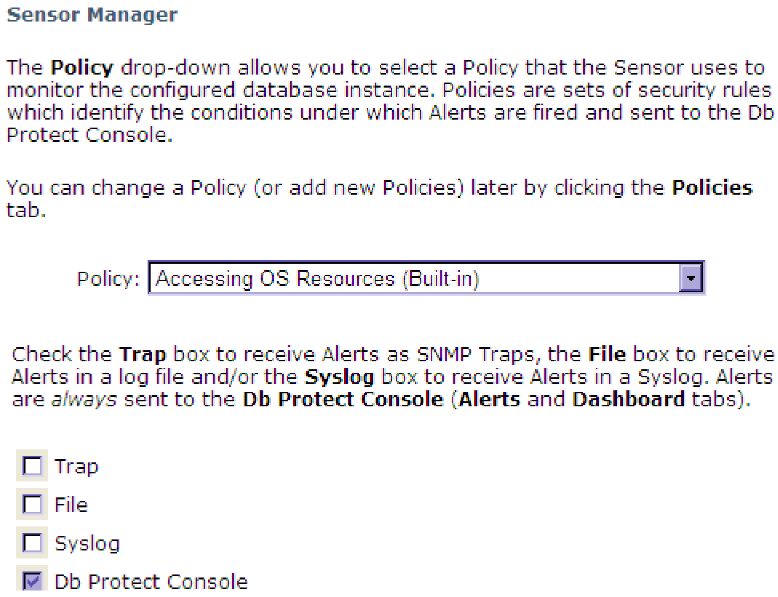
Important: The value you enter **must** start with a letter and is restricted to a maximum of 128 characters.Your instance alias can only contain alphanumeric, underscore (_), period (`.`), and hyphen (`-`) characters, or spaces. **Acceptable** examples: `MEMBERSHIP DB2 DB1`, `MEMBERSHIP.DB2DB1`, `MEMBERSHIP_DB2_DB1`, `MEMBERSHIP-DB2DB1`, etc. **Unacceptable** examples: `MEMBERSHIP:DB2DB1`, `MEMBERSHIP/DB2DB1`, etc.

- Enter the name of the DB2 database server you want to monitor in the **DB2 instance** field.
- Optionally, in the **Advanced Monitoring Properties** portion of the page, you can modify the value in the **Inactivity duration** field. The "inactivity duration" is the amount of time (in seconds) that must elapse with no activity on a DB2 server instance before the Sensor generates an inactivity Alert. The default value is 5 minutes (`300` seconds). Valid values are `0` to `86400` seconds (i.e., 24 hours).

Note: Entering the value `0` (seconds) disables inactivity monitoring.

- Click the **Next** button.

6. The next **Sensor Manager** page displays. It allows you to select a Policy that the Sensor uses to monitor the configured DB2 database server. Policies are sets of rules which identify the conditions under which Alerts are fired and sent to DbProtect Audit and Threat Management.



Sensor Manager

The **Policy** drop-down allows you to select a Policy that the Sensor uses to monitor the configured database instance. Policies are sets of security rules which identify the conditions under which Alerts are fired and sent to the Db Protect Console.

You can change a Policy (or add new Policies) later by clicking the **Policies** tab.

Policy: Accessing OS Resources (Built-in)

Check the **Trap** box to receive Alerts as SNMP Traps, the **File** box to receive Alerts in a log file and/or the **Syslog** box to receive Alerts in a Syslog. Alerts are *always* sent to the **Db Protect Console** (**Alerts** and **Dashboard** tabs).

☐ Trap
☐ File
☐ Syslog
☑ Db Protect Console

FIGURE: Sensor Manager

Use the **Policy:** drop-down to select a built-in or custom Policy the Sensor will use to monitor the configured DB2 database server.

Note: Deploying a Policy via the **Policy Manger** allows you to deploy Policies to multiple DB2 database instances simultaneously, which may (or may not) be monitored by the same Sensor. Additionally, you can change the Policies deployed (or deploy multiple additional Policies) any time by clicking the **Policies** tab; for more information, see *Deploying a Policy*.

7. The grayed-out **DbProtect Console** checkbox indicates Alerts are **always** sent to the DbProtect Console.

You can monitor these Alerts in real-time via the **Alert Manager** and the **Dashboard**; for more information, see *Monitoring, filtering, acknowledging, and archiving Alerts (via the Alert Manager)* and *Monitoring Alerts (via the Dashboard)* respectively. In addition, the **Report Manager** allows you to run **Detail Reports** and **Summary Reports** for Alerts.

Optionally, on this page you can check:

- **Trap** to receive Alerts also as SNMP traps
- **File** to receive Alerts also in a log file
- **Syslog** to receive Alerts also as Syslog messages.

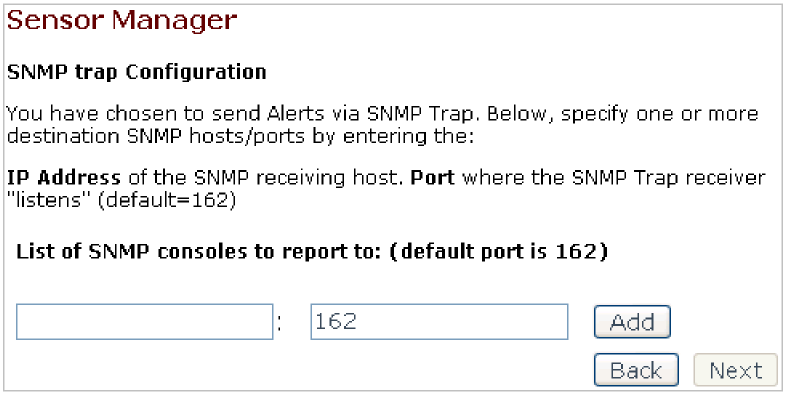
8. Click the **Next** button. If you checked:

- **Trap**, then go to Step 9
- **File**, then go to Step 10
- **Syslog**, then go to Step 11.

Otherwise, go to Step 12.

9. Receiving Alerts as SNMP traps.

The **SNMP trap Configuration** page displays (if you checked **Trap**).



Sensor Manager

SNMP trap Configuration

You have chosen to send Alerts via SNMP Trap. Below, specify one or more destination SNMP hosts/ports by entering the:

IP Address of the SNMP receiving host. **Port** where the SNMP Trap receiver "listens" (default=162)

List of SNMP consoles to report to: (default port is 162)

: 162

FIGURE: Sensor Manager

Specify the SNMP server **IP Address** (**not** the host name) of the SNMP receiving host, and the **port** number where the SNMP trap receiver "listens".

Note: The default port is `162`, not `80`.

- Optionally, click the **Add** button and specify an additional SNMP server IP Address (**not** the host name), and an additional port number of the target SNMP server where you want Alerts sent.
- When you're done, click the **Next** button.

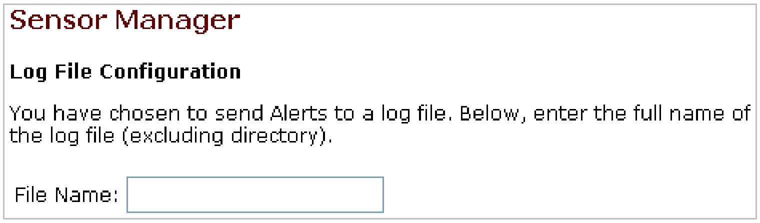
If you also checked:

- **File**, then go to Step 10
- **Syslog**, then go to Step 11.

Otherwise, go to Step 12.

10.Receiving Alerts as Log Files.

The **Log File Configuration** page displays (if you checked **File**).



Sensor Manager

Log File Configuration

You have chosen to send Alerts to a log file. Below, enter the full name of the log file (excluding directory).

File Name:

FIGURE: Sensor Manager

Do the following:

- Enter an Alert log file name in **File Name** field.

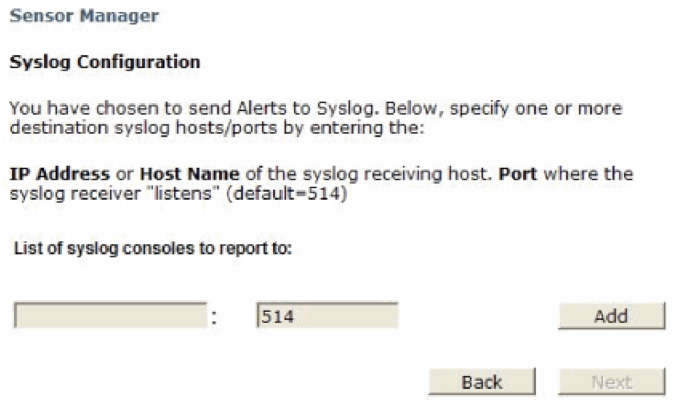
  Be sure to enter the full name of the log file (including the directory), and the log file's extension (e.g., `.txt`, `.rtf`, `.log`, etc.).

  The Alert log file is stored in the `Sensor_installation_directory\logs` directory, where `Sensor_installation_directory` is where the Sensor is installed.
- Click the **Next** button.

If you also checked **Syslog**, then go to Step 11. Otherwise, go to Step 12.

11.Receiving Alerts as Syslog messages.

The **Syslog File Configuration** page displays (if you checked **Syslog**). For a sample Syslog message, see the *DbProtect Administrator's Guide*.



Sensor Manager

Syslog Configuration

You have chosen to send Alerts to Syslog. Below, specify one or more destination syslog hosts/ports by entering the:

IP Address or **Host Name** of the syslog receiving host. **Port** where the syslog receiver "listens" (default=514)

List of syslog consoles to report to:

: 514

FIGURE: Sensor Manager

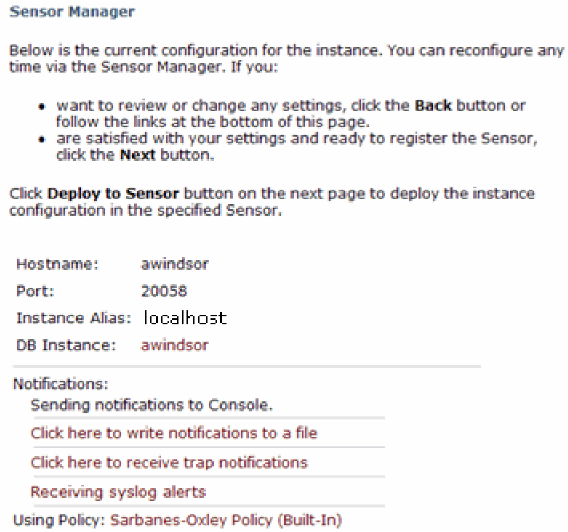
Specify the Syslog server IP Address, and the port number of the target Syslog server where you want Alerts sent.

Note: The default port is `514` (not `80`).

Caution! The Syslog port is a User Datagram Protocol (UDP) port, as opposed to Transmission Control Protocol (TCP).

- Optionally, click the **Add** button and specify an additional Syslog server IP Address, and an additional port number of the target Syslog server where you want Alerts sent.
- When you're done, click the **Next** button.

12. After you finish specifying the SNMP trap, and/or log file, and/or Syslog parameters, then the **Sensor Manager** summary page displays.



Sensor Manager

Below is the current configuration for the instance. You can reconfigure any time via the Sensor Manager. If you:

- want to review or change any settings, click the **Back** button or follow the links at the bottom of this page.
- are satisfied with your settings and ready to register the Sensor, click the **Next** button.

Click **Deploy to Sensor** button on the next page to deploy the instance configuration in the specified Sensor.

Hostname:	awindsor
Port:	20058
Instance Alias:	localhost
DB Instance:	awindsor

Notifications:

Sending notifications to Console.

Click here to write notifications to a file

Click here to receive trap notifications

Receiving syslog alerts

Using Policy: Sarbanes-Oxley Policy (Built-In)

FIGURE: Sensor Manager

If you:

- want to review or change any settings you can click the **Back** button or any link that displays on the page
- are satisfied with your settings and ready to deploy the configuration to the Sensor, click the **Next** button.

Note: You can reconfigure the Sensor any time via the **Sensor Manager**.

The second **Sensor Manager** page re-displays.

13. In the bottom, right corner of the page you can click the:

- **Deploy to Sensor** button to deploy this configured instance to the specified Sensor
- **Cancel** button to cancel the Sensor configuration.

Caution! All your configuration changes will be lost if you click the **Cancel** button.

FIGURE: **Cancel** and **Deploy to Sensor** buttons

Or you can click the:

- **Reconfigure Sensor** button to reconfigure the Sensor before deploying the instance configuration in the specified Sensor
- **Configure New Instance** button, if available (for a host-based Sensor, this button may be disabled if DbProtect Audit and Threat Management does **not** detect additional database instances for this server).

For more information, go back to Step 2.

Note: DbProtect audit and threat management may have limitations based on the type of Sensor, the nature of the activity, the target database, and the operating system.

Host-based Sensors detect both local and remote attacks. However, they detect only successfully executed commands. For example, a vulnerable database system may permit a certain type of attack, and that attack causes the host-based Sensor to generate an Alert. Importantly, a patched system generally rejects the same command, thus preventing a host-based Sensor from detecting an attempted breach.

For more information, see *DbProtect audit and threat management limitations (based on Sensor type, activity, target database, and operating system).*

Important: If you installed a host-based Sensor for Oracle to monitor Oracle databases on an Oracle RAC (regardless of host platform) you must appropriately configure the host-based Sensor. For more information, see *Appendix C: Installing and Configuring a Host-Based Sensor for Oracle to Monitor Oracle Databases on an Oracle RAC.*

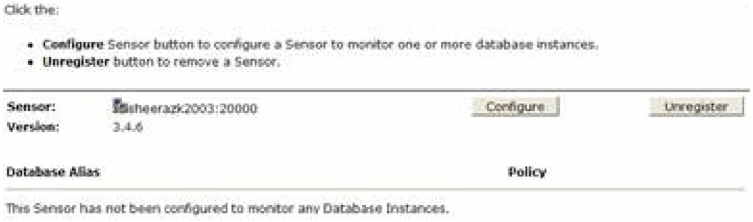
CONFIGURING A HOST-BASED SENSOR TO MONITOR SYBASE DATABASES AND DEPLOYING THE CONFIGURATION INFORMATION (WHEN SENSOR IS INSTALLED ON A SUPPORTED *NIX-BASED OPERATING SYSTEM)

To configure a host-based Sensor to monitor Sybase databases and deploy the configuration information (when Sensor is installed on a supported *nix-based operating system, i.e., Solaris or AIX):

1. Do one of the following to display the first **Sensor Manager** page:

- Click the **Sensors - Manage Sensor** workflow link on the **Home** page.
- Click the **Sensors** tab from anywhere on the page.

The first **Sensor Manager** page displays your registered Sensors.



Click the:

- **Configure** Sensor button to configure a Sensor to monitor one or more database instances.
- **Unregister** button to remove a Sensor.

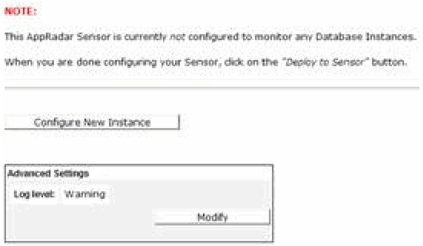
Sensor: sheerazk2003:20000
Version: 3.4.6

Database Alias	Policy
This Sensor has not been configured to monitor any Database Instances.	

FIGURE: Sensor Manager

2. Click the **Configure** button (if you are configuring a Sensor for the first time), or the **Reconfigure** button (if you are reconfiguring a Sensor).

The next **Sensor Manager** page displays.



NOTE:

This AppRadar Sensor is currently *not* configured to monitor any Database Instances.

When you are done configuring your Sensor, click on the *"Deploy to Sensor"* button.

Advanced Settings

Log level: Warning

FIGURE: Sensor Manager

This **Sensor Manager** page shows the:

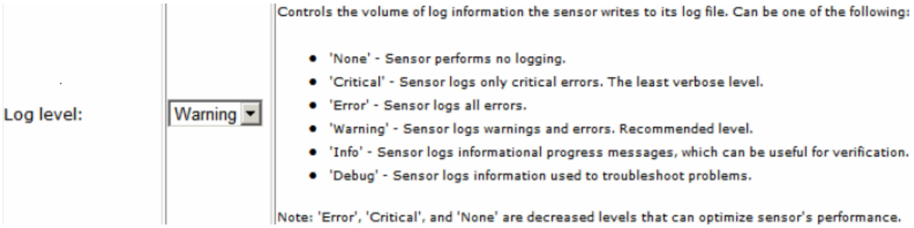
- **Alias** of any host server you have configured for your Sensor
- database **Type** of the instance where your Sensor is registered
- database instance **(DB Instance)** where your Sensor is registered
- **Policy** associated with the registered Sensor.

Note: The Console also displays whether the rules in your **Policy** are up-to-date or out-of-date. If a Policy is out-of-date, you can ASAP Update your Sensor with the latest security Rules (for more information, see *Performing an ASAP Update of Rules in your Sensors*), then use the **Policy Editor** to update Policies (deployed to your Sensors) with the new security Rules (for more information, see *Creating a Policy* and *Editing a Policy*).

When you're done, you can click the:

- **Modify** button in the **Advanced Settings** portion of the page to display the **Advanced Sensor Settings** page, which allows you to select the Sensor's logging level (see Step 4)
- **Configure New Instance** button to configure a new **Sybase database** for the Sensor (see Steps 5-16)
- **Reconfigure** button to modify the current configuration of an **Sybase database** for the Sensor (see Steps 6-16)
- **X** button to delete a configured Sensor monitoring an instance; for more information, see *Deleting configured Sensors*.

3. The **Advanced Sensor Settings** page allows you to modify the Sensor's **logging level** and/or modify the **inactivity duration**.



Log level: Warning

Controls the volume of log information the sensor writes to its log file. Can be one of the following:

- 'None' - Sensor performs no logging.
- 'Critical' - Sensor logs only critical errors. The least verbose level.
- 'Error' - Sensor logs all errors.
- 'Warning' - Sensor logs warnings and errors. Recommended level.
- 'Info' - Sensor logs informational progress messages, which can be useful for verification.
- 'Debug' - Sensor logs information used to troubleshoot problems.

Note: 'Error', 'Critical', and 'None' are decreased levels that can optimize sensor's performance.

FIGURE: **Advanced Sensor Settings** page

To modify the Sensor's logging level.

Use the **Log level:** drop-down to select the Sensor's logging level, which controls the volume of log information the Sensor outputs to its log file. You can select:

- **None.** Sensor performs no logging.
- **Critical.** Sensor logs only critical errors. The **least** verbose level.
- **Error.** Sensor logs **all** errors.
- **Warning.** Sensor logs warnings and errors. Recommended level.
- **Info.** Sensor logs informational progress messages, which can be useful for verification.
- **Debug.** Logs information used to troubleshoot Sensor problems at runtime.

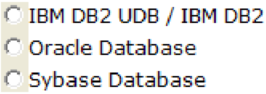
Note: **Error**, **Critical**, and **None** are all decreased logging levels which you can use to optimize Sensor performance.

When you're done, you can click the **Next** button to display the **Sensor Manager** page from Step 2. You can click the:

- **Configure New Instance** button to configure a new **Sybase database** for the Sensor (see Steps 5-16)
- **Reconfigure** button to modify the current configuration of a **Sybase database** for the Sensor (see Steps 6-16)
- **X** button to delete a configured Sensor monitoring an instance; for more information, see *Deleting configured Sensors*.

4. Configuring a new instance.

The **Sensor Manager** page prompts you to select a database platform for the host-based Sensor to monitor.



○ IBM DB2 UDB / IBM DB2

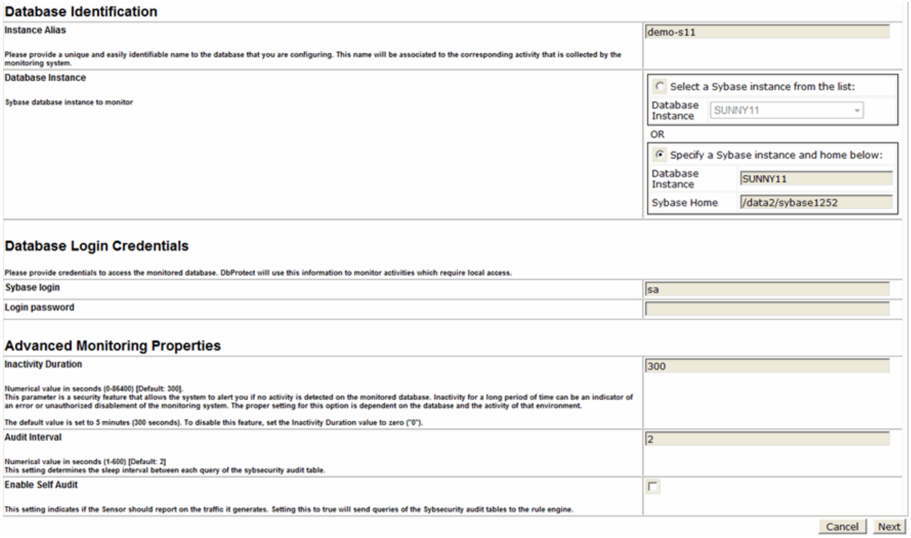
○ Oracle Database

○ Sybase Database

FIGURE: **Sensor Manager** page

- Select **Sybase Database**.
- Click the **Next** button.

The **Sensor Manager** page shown below allows you to configure/re-configure a Sensor for host-based **Sybase** (when the Sensor is installed on a *nix-based operating system).



Database Identification

Instance Alias: demo-s11

Please provide a unique and easily identifiable name to the database that you are configuring. This name will be associated to the corresponding activity that is collected by the monitoring system.

Database Instance

Sybase database instance to monitor

○ Select a Sybase instance from the list:

Database Instance: SUNNY11

OR

● Specify a Sybase instance and home below:

Database Instance: SUNNY11

Sybase Home: /data2/sybase1252

Database Login Credentials

Please provide credentials to access the monitored database. DbProtect will use this information to monitor activities which require local access.

Sybase login: sa

Login password:

Advanced Monitoring Properties

Inactivity Duration: 300

Numerical value in seconds (0-86400) [Default: 300].
This parameter is a security feature that allows the system to alert you if no activity is detected on the monitored database. Inactivity for a long period of time can be an indicator of an error or unauthorized disablement of the monitoring system. The proper setting for this option is dependent on the database and the activity of that environment.

The default value is set to 5 minutes (300 seconds). To disable this feature, set the Inactivity Duration value to zero ("0").

Audit Interval: 2

Numerical value in seconds (1-600) [Default: 2]
This setting determines the sleep interval between each query of the sybsecurity audit table.

Enable Self Audit: □

This setting indicates if the Sensor should report on the traffic it generates. Setting this to true will send queries of the Sybsecurity audit tables to the rule engine.

FIGURE: **Sensor Manager** page

This page consists of three portions. If you want to work with the:

- **Database Identification** portion of the page, see Step 5
- **Database Login Credentials** portion of the page, see Step 6
- **Advanced Monitoring Properties** portion of the page, see Step 7.

When you're done, go to Step 8.

5. In the **Database Identification** portion of the page:

- Enter a meaningful alias in the **Instance Alias:** field for the Sybase database you want the Sensor to monitor. DbProtect Audit and Threat Management uses this alias to identify the **Sybase database** from which Alerts are received.

Important: Your instance alias can only contain alphanumeric, underscore (_), period (`.`), and hyphen (`-`) characters, or spaces. Letters may be any mix of UPPER and/or lower case. **Acceptable** examples: `syb DB1`, `SYB.db1`, `Syb_DB1`, `SYB-DB1`, etc. **Unacceptable** examples: `SYB:DB1`, `SYB/DB1`, etc.

- The **Database Instance** buttons, fields, and drop-downs allow you to do the following:

  -Select **Select a Sybase instance from the list:**, and use the **Database Instance** drop-down to select a Sybase database host where a Sensor is installed

  -Select **Specify a Sybase instance and home below:** and manually enter the **Database Instance** name and the **Sybase Home**.

Note: **Sybase Home** refers to the home directory for Sybase, i.e., the place on the operating system where the Sybase database is installed.

6. The **Database Login Credentials** portion of the page allows you to enter a **Sybase login** and **Login password**, which DbProtect uses to monitor activity that requires local access.
7. In the **Advanced Monitoring Properties** portion of the page:

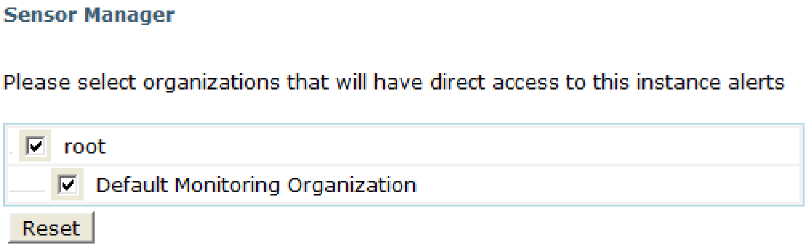
- **Inactivity Duration.** The **Inactivity Duration** is the amount of time (in seconds) that must elapse with no activity on a Sybase database or service before the Sensor generates an inactivity Alert. The default value is 5 minutes (`300` seconds). Valid values are `0` to `86400` seconds (i.e., 24 hours).

Note: Entering the value `0` (seconds) disables inactivity monitoring.

- **Audit Interval.** The **Audit Poll Interval** is a numerical value in seconds (`1`-`600`) that represents the interval at which the Sensor polls the Sybase Audit file to detect successful or failed login attempts. Default = `2` seconds.
- **Enable Self Audit.** Unchecked by default, the **Enable Self Audit** checkbox (if checked) instructs the Sensor to report on traffic that it (i.e., the Sensor itself) generates. Checking the **Enable Self Audit** checkbox will send queries of the Sybsecurity audit tables to the DbProtect rule engine.

8. Click the **Next** button.

The **Sensor Manager** page shown below allows you to select which Organizations can have direct access to Alerts generated on this Sybase instance. For more information on how Organizations work in DbProtect, see *DbProtect Organizations, Users, and User Roles*.



Sensor Manager

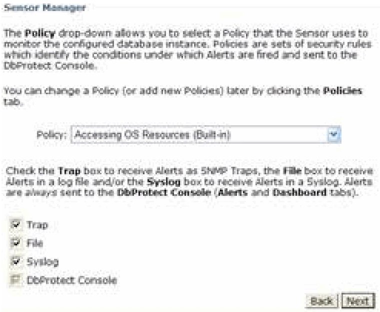
Please select organizations that will have direct access to this instance alerts

☑ root

☑ Default Monitoring Organization

FIGURE: Sensor Manager

9. The **Sensor Manager** page shown below allows you to select a Policy that the Sensor uses to monitor the configured Sybase database. Policies are sets of rules which identify the conditions under which Alerts are fired and sent to DbProtect Audit and Threat Management.



Sensor Manager

The **Policy** drop-down allows you to select a Policy that the Sensor uses to monitor the configured database instance. Policies are sets of security rules which identify the conditions under which Alerts are fired and sent to the DbProtect Console.

You can change a Policy (or add new Policies) later by clicking the **Policies** tab.

Policy: Accessing OS Resources (Built-in)

Check the **Trap** box to receive Alerts as SNMP Traps, the **File** box to receive Alerts in a log file and/or the **Syslog** box to receive Alerts in a Syslog. Alerts are always sent to the **DbProtect Console** (**Alerts** and **Dashboard** tabs).

☑ Trap

☑ File

☑ Syslog

☑ DbProtect Console

FIGURE: Sensor Manager

Use the **Policy:** drop-down to select a built-in or custom Policy the Sensor will use to monitor the configured Sybase database.

Note: Deploying a Policy via the **Policy Manger** allows you to deploy Policies to multiple Sybase databases simultaneously, which may (or may not) be monitored by the same Sensor. Additionally, you can change the Policies deployed (or deploy multiple additional Policies) any time by clicking the **Policies** tab; for more information, see *Deploying a Policy*.

10. The grayed-out **DbProtect Console** checkbox indicates Alerts are **always** sent to the DbProtect Console.

You can monitor these Alerts in real-time via the **Alert Manager** and the **Dashboard**; for more information, see *Monitoring, filtering, acknowledging, and archiving Alerts (via the Alert Manager)* and *Monitoring Alerts (via the Dashboard)* respectively. In addition, the **Report Manager** allows you to run **Detail Reports** and **Summary Reports** for Alerts.

Optionally, on this page you can check:

- **Trap** to receive Alerts also as SNMP traps
- **File** to receive Alerts also in a log file
- **Syslog** to receive Alerts also as Syslog messages.

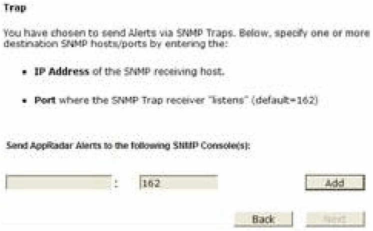
11. Click the **Next** button. If you checked:

- **Trap**, then go to Step 12
- **File**, then go to Step 13
- **Syslog**, then go to Step 14.

Otherwise, go to Step 15.

12.Receiving Alerts as SNMP traps.

The **SNMP trap Configuration** page displays (if you checked **Trap**).



Trap

You have chosen to send Alerts via SNMP Traps. Below, specify one or more destination SNMP hosts/ports by entering the:

- **IP Address** of the SNMP receiving host.
- **Port** where the SNMP Trap receiver "listens" (default=162)

Send AppRadar Alerts to the following SNMP Console(s):

: 162

FIGURE: **Sensor Manager**

Specify the SNMP server **IP Address** (**not** the host name) of the SNMP receiving host, and the **port** number where the SNMP trap receiver "listens".

Note: The default port is `162`, not `80`.

- Click the **Add** button.
- Click the **Next** button.

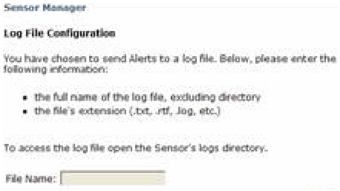
If you also checked:

- **File**, then go to Step 13
- **Syslog**, then go to Step 14.

Otherwise, go to Step 15.

13. Receiving Alerts as Log Files.

The **Log File Configuration** page displays (if you checked **File**).



Sensor Manager

Log File Configuration

You have chosen to send Alerts to a log file. Below, please enter the following information:

- the full name of the log file, excluding directory
- the file's extension (.txt, .rtf, .log, etc.)

To access the log file open the Sensor's logs directory.

File Name:

FIGURE: Sensor Manager

Do the following:

- Enter an Alert log file name in **File Name:** field.

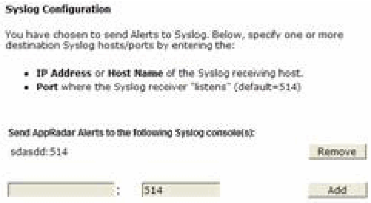
  Be sure to enter the full name of the log file (including the directory), and the log file's extension (e.g., `.txt`, `.rtf`, `.log`, etc.).

  The Alert log file is stored in the `Sensor_installation_directory\logs` directory, where `Sensor_installation_directory` is where the Sensor is installed.
- Click the **Next** button.

If you also checked **Syslog**, then go to Step 14. Otherwise, go to Step 15.

14. Receiving Alerts as Syslog messages.

The **Syslog File Configuration** page displays (if you checked **Syslog**). For a sample Syslog message, see the *DbProtect Administrator's Guide*.



Syslog Configuration

You have chosen to send Alerts to Syslog. Below, specify one or more destination Syslog hosts/ports by entering the:

- **IP Address** or **Host Name** of the Syslog receiving host.
- **Port** where the Syslog receiver "listens" (default=514)

Send AppRadar Alerts to the following Syslog console(s):

sdasdd:514

: 514

FIGURE: Sensor Manager

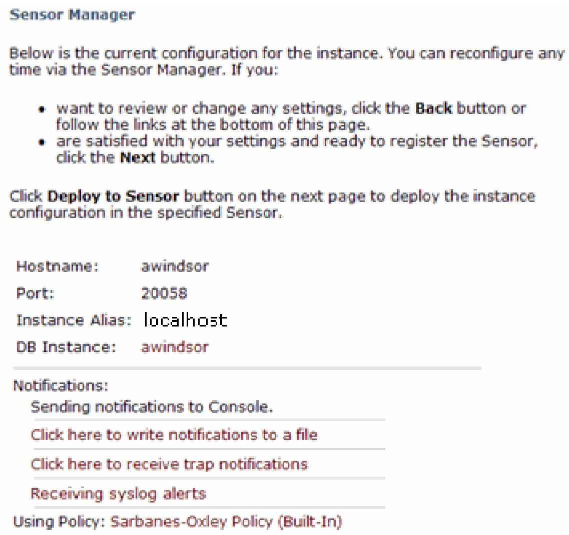
Specify the Syslog server IP Address (**not** the host name), and the port number of the target Syslog server where you want Alerts sent.

Note: The default port is `514` (not `80`).

Caution! The Syslog port is a User Datagram Protocol (UDP) port, as opposed to Transmission Control Protocol (TCP).

- Optionally, click the **Add** button and specify an additional Syslog server IP Address, and an additional port number of the target Syslog server where you want Alerts sent.
- When you're done, click the **Next** button.

15. After you finish specifying the SNMP trap, and/or log file, and/or Syslog parameters, then the **Sensor Manager** summary page displays.



Sensor Manager

Below is the current configuration for the instance. You can reconfigure any time via the Sensor Manager. If you:

- want to review or change any settings, click the **Back** button or follow the links at the bottom of this page.
- are satisfied with your settings and ready to register the Sensor, click the **Next** button.

Click **Deploy to Sensor** button on the next page to deploy the instance configuration in the specified Sensor.

Hostname:	awindsor
Port:	20058
Instance Alias:	localhost
DB Instance:	awindsor

Notifications:
Sending notifications to Console.
Click here to write notifications to a file
Click here to receive trap notifications
Receiving syslog alerts
Using Policy: Sarbanes-Oxley Policy (Built-In)

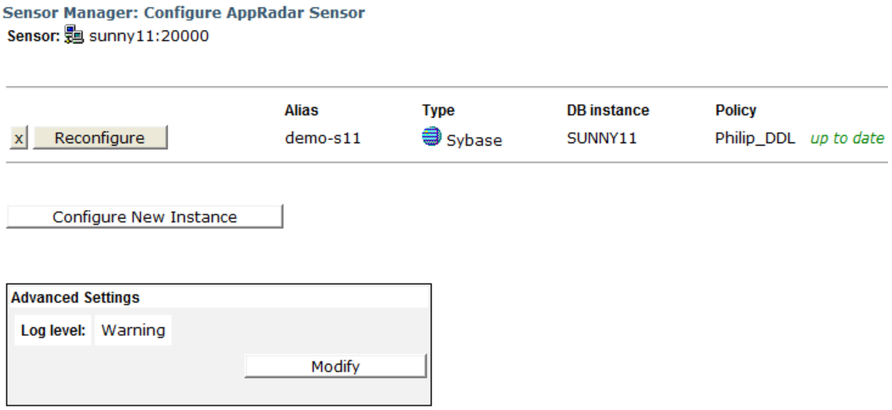
FIGURE: **Sensor Manager**

If you:

- want to review or change any settings you can click the **Back** button or any link that displays on the page
- are satisfied with your settings and ready to deploy the configuration to the Sensor, click the **Next** button.

Note: You can reconfigure the Sensor any time via the **Sensor Manager**.

The **Sensor Manager** page from Step 2 re-displays.



Sensor Manager: Configure AppRadar Sensor

Sensor: sunny11:20000

	Alias	Type	DB instance	Policy	
x Reconfigure	demo-s11	Sybase	SUNNY11	Philip_DDL	up to date

Advanced Settings

Log level: Warning

FIGURE: Sensor Manager

16. In the bottom, right corner of the page you can click the:

- **Deploy to Sensor** button to deploy this configured instance to the specified Sensor
- **Cancel** button to cancel the Sensor configuration.

Caution! All your configuration changes will be lost if you click the **Cancel** button.

FIGURE: **Cancel** and **Deploy to Sensor** buttons

Or you can click the:

- **Reconfigure Sensor** button to reconfigure the Sensor before deploying the instance configuration in the specified Sensor
- **Configure New Instance** button, if available (for a host-based Sensor, this button may be disabled if DbProtect Audit and Threat Management does **not** detect additional database instances for this server).

For more information, go back to Step 2.

CONFIGURING A HOST-BASED SENSOR TO MONITOR ORACLE SIDS AND SERVICES AND DEPLOYING THE CONFIGURATION INFORMATION (WHEN SENSOR IS INSTALLED ON WINDOWS)

In the case of host-based monitoring of Oracle on Microsoft Windows, the following conditions and warnings apply:

- Host-based Sensors monitoring Oracle on Windows use a hybrid of network-based and host-based architectures. These “hybrid Sensors” detect all attacks originating remotely, but only those local commands that are successfully executed.

  This does **not** apply to monitoring Oracle using a network-based Sensor, or using a host-based Sensor on any *nix platform (i.e., Solaris, AIX, HP-UX, or Red Hat Enterprise Linux) as these platforms follow standard network- and host-based audit and threat management guidelines.

  For more information, see *DbProtect audit and threat management limitations (based on Sensor type, activity, target database, and operating system)*.
- Database login names are always reported in Alerts as `/`, while logins are reported as `as sysdba`.
- The Rule **“Login attempt – successful”** only works (i.e., only fires an Alert) with local connections.
- When monitoring any Oracle instance on Windows, granting privileges via a local Oracle session may cause associated Alerts to contain only the first 25 characters of the SQL command. This is apparently due to a bug in Oracle. Application Security, Inc.'s security research team (Team SHATTER) is investigating.

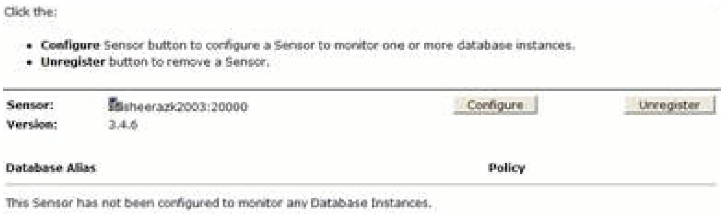
Important: If you installed a host-based Sensor for Oracle to monitor Oracle databases on an Oracle RAC (regardless of host platform) you **must** appropriately configure the host-based Sensor. For more information, see *Appendix C: Installing and Configuring a Host-Based Sensor for Oracle to Monitor Oracle Databases on an Oracle RAC.*

Important: If you installed a host-based Sensor for Oracle to monitor Oracle databases in an Oracle Fail Safe environment (Windows only) you **must** appropriately configure the host-based Sensor. For more information, see *Appendix B: Monitoring Oracle Databases in an Oracle Fail Safe Environment: Sensor and Cluster Configuration Steps.*

To configure a host-based Sensor to monitor Oracle SIDs and services and deploy the configuration information (when Sensor is installed on Windows):

1. Do one of the following to display the first **Sensor Manager** page:
   - Click the **Sensors - Manage Sensor** workflow link on the **Home** page.
   - Click the **Sensors** tab from anywhere on the page.

The first **Sensor Manager** page displays your registered Sensors.



Click the:

- **Configure** Sensor button to configure a Sensor to monitor one or more database instances.
- **Unregister** button to remove a Sensor.

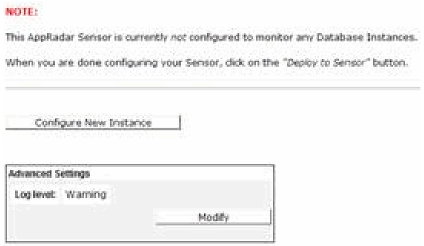
Sensor: sheerazk2003:20000
Version: 3.4.6

Database Alias	**Policy**
This Sensor has not been configured to monitor any Database Instances.	

FIGURE: Sensor Manager

2. Click the **Configure** button (if you are configuring a Sensor for the first time), or the **Reconfigure** button (if you are reconfiguring a Sensor).

The next **Sensor Manager** page displays.



NOTE:

This AppRadar Sensor is currently *not* configured to monitor any Database Instances.

When you are done configuring your Sensor, click on the *"Deploy to Sensor"* button.

Advanced Settings

Log level: Warning

This **Sensor Manager** page shows the:

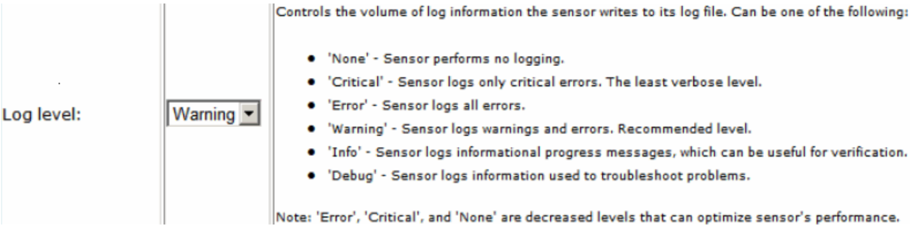
- **Alias** of any host server you have configured for your Sensor
- database **Type** of the instance where your Sensor is registered
- database instance **(DB Instance)** where your Sensor is registered
- **Policy** associated with the registered Sensor.

Note: The Console also displays whether the rules in your **Policy** are up-to-date or out-of-date. If a Policy is out-of-date, you can ASAP Update your Sensor with the latest security Rules (for more information, see *Performing an ASAP Update of Rules in your Sensors*), then use the **Policy Editor** to update Policies (deployed to your Sensors) with the new security Rules (for more information, see *Creating a Policy* and *Editing a Policy*).

When you’re done, you can click the:

- **Modify** button in the **Advanced Settings** portion of the page to display the **Advanced Sensor Settings** page, which allows you to select the Sensor's logging level (and go to Step 3)
- **Configure New Instance** button to configure a new **Oracle SID or service** for the Sensor (and go to Step 4)
- **Reconfigure** button to modify the current configuration of an **Oracle SID or service** for the Sensor (and go to Step 5)
- **X** button to delete a configured Sensor monitoring an instance; for more information, see *Deleting configured Sensors*.

3. The **Advanced Sensor Settings** page allows you to modify the Sensor's **logging level** and/or modify the **inactivity duration**.



Log level: Warning

Controls the volume of log information the sensor writes to its log file. Can be one of the following:

- 'None' - Sensor performs no logging.
- 'Critical' - Sensor logs only critical errors. The least verbose level.
- 'Error' - Sensor logs all errors.
- 'Warning' - Sensor logs warnings and errors. Recommended level.
- 'Info' - Sensor logs informational progress messages, which can be useful for verification.
- 'Debug' - Sensor logs information used to troubleshoot problems.

Note: 'Error', 'Critical', and 'None' are decreased levels that can optimize sensor's performance.

FIGURE: **Advanced Sensor Settings** page

To modify the Sensor's logging level.

Use the **Log level:** drop-down to select the Sensor's logging level, which controls the volume of log information the Sensor outputs to its log file. You can select:

- **None.** Sensor performs no logging.
- **Critical.** Sensor logs only critical errors. The **least** verbose level.
- **Error.** Sensor logs **all** errors.
- **Warning.** Sensor logs warnings and errors. Recommended level.
- **Info.** Sensor logs informational progress messages, which can be useful for verification.
- **Debug.** Logs information used to troubleshoot Sensor problems at runtime.

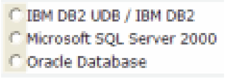
Note: **Error**, **Critical**, and **None** are all decreased logging levels which you can use to optimize Sensor performance.

When you’re done, you can click the **Next** button to display the **Sensor Manager** page from Step 2. You can click the:

- **Configure New Instance** button to configure a new **Oracle SID or service** for the Sensor (and go to Step 4)
- **Reconfigure** button to modify the current configuration of a **Oracle SID or service** for the Sensor (and go to Step 5)
- **X** button to delete a configured Sensor monitoring an instance; for more information, see *Deleting configured Sensors*.

4. Configuring a new instance.

The **Sensor Manager** page prompts you to select a database platform for the host-based Sensor to monitor.



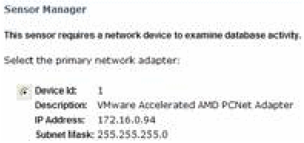
○ IBM DB2 UDB / IBM DB2
○ Microsoft SQL Server 2000
○ Oracle Database

FIGURE: **Sensor Manager** page

- Select **Oracle Database**.
- Click the **Next** button.

The next **Sensor Manager** page prompts you to specify a network device the Sensor will use to monitor traffic.

Note: If you are configuring a host-based Sensor for Oracle on Windows to monitor Oracle databases in an Oracle Fail Safe environment, you **must** select a network adapter that is associated with a real IP address (where the network traffic can sniff packets). Make sure this is **not** the cluster heartbeat card, because cluster heartbeat cards do not detect network traffic. For more information, see *Appendix B: Monitoring Oracle Databases in an Oracle Fail Safe Environment: Sensor and Cluster Configuration Steps*.



Sensor Manager

This sensor requires a network device to examine database activity.

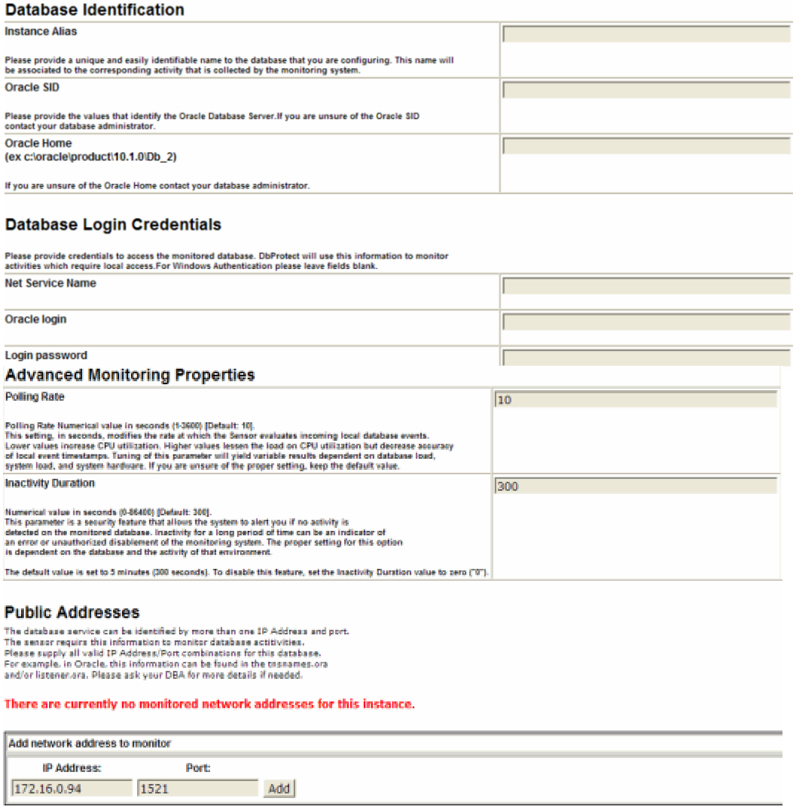
Select the primary network adapter:

● Device Id: 1
Description: VMware Accelerated AMD PCNet Adapter
IP Address: 172.16.0.94
Subnet Mask: 255.255.255.0

FIGURE: **Sensor Manager** page

- Click the **Next** button.

5. The **Sensor Manager** page shown below allows you to configure/re-configure a Sensor for host-based **Oracle** (when the Sensor is installed on Windows).



Database Identification

Instance Alias Please provide a unique and easily identifiable name to the database that you are configuring. This name will be associated to the corresponding activity that is collected by the monitoring system.	
Oracle SID Please provide the values that identify the Oracle Database Server.If you are unsure of the Oracle SID contact your database administrator.	
Oracle Home (ex c:\oracle\product\10.1.0\Db_2) If you are unsure of the Oracle Home contact your database administrator.	

Database Login Credentials

Please provide credentials to access the monitored database. DbProtect will use this information to monitor activities which require local access.For Windows Authentication please leave fields blank.

Net Service Name	
Oracle login	
Login password	

Advanced Monitoring Properties

Polling Rate Polling Rate Numerical value in seconds (1-3600) [Default: 10]. This setting, in seconds, modifies the rate at which the Sensor evaluates incoming local database events. Lower values increase CPU utilization. Higher values lessen the load on CPU utilization but decrease accuracy of local event timestamps. Tuning of this parameter will yield variable results dependent on database load, system load, and system hardware. If you are unsure of the proper setting, keep the default value.	10
Inactivity Duration Numerical value in seconds (0-86400) [Default: 300]. This parameter is a security feature that allows the system to alert you if no activity is detected on the monitored database. Inactivity for a long period of time can be an indicator of an error or unauthorized disablement of the monitoring system. The proper setting for this option is dependent on the database and the activity of that environment. The default value is set to 5 minutes (300 seconds). To disable this feature, set the Inactivity Duration value to zero ("0").	300

Public Addresses

The database service can be identified by more than one IP Address and port.
The sensor requirs this information to monitor database actitivities.
Please supply all valid IP Address/Port combinations for this database.
For example, in Oracle, this information can be found in the tnsnames.ora
and/or listener.ora. Please ask your DBA for more details if needed.

There are currently no monitored network addresses for this instance.

Add network address to monitor

IP Address:	Port:	
172.16.0.94	1521	Add

FIGURE: **Sensor Manager** page

This page consists of three portions. If you want to work with the:

- **Database Identification** portion of the page, see Step 6
- **Database Login Credentials** portion of the page, see Step 7
- **Advanced Monitoring Properties** portion of the page, see Step 8
- **Public Addresses** portion of the page, see Step 9.

When you're done, go to Step 10.

6. In the **Database Identification** portion of the page:

- Enter a meaningful Oracle SID alias in the **Instance Alias:** field, for the Oracle SID you want the Sensor to monitor. DbProtect Audit and Threat Management uses this alias to identify the Oracle SID from which Alerts are received.

Important: Your Oracle SID alias can only contain alphanumeric, underscore (_), period (.), and hyphen (-) characters, or spaces. **Acceptable** examples: `ORCL DB1`, `ORCL.DB1`, `ORCL_DB1`, `ORCL-DB1`, etc. **Unacceptable** examples: `ORCL:DB1`, `ORCL/DB1`, etc.

Caution! If you installed a host-based Sensor for Oracle to monitor Oracle databases on an Oracle RAC, make sure your **Instance Alias**: a.) is unique for each registered host-based Sensor for Oracle; b.) is easily identifiable for the database you are monitoring; c.) is easily identifies the node where the Sensor is installed (e.g., **Oracle RAC Node 1**, **Oracle RAC Node 2**, etc.). For more information, see ***Appendix C: Installing and Configuring a Host-Based Sensor for Oracle to Monitor Oracle Databases on an Oracle RAC***.

- The **Oracle SID:** fields allow you to do the following:

  -Select **Select an Oracle instance from the list of discovered SIDs:**, and use the **Oracle SID** drop-down to select an **Oracle SID** where a Sensor is installed (derived from the `oratab` file on the host)

  -Select **Specify Oracle SID and home below:** and manually enter the **Oracle SID** name and the **Oracle Home**.

Note: **Oracle Home** refers to the home directory for Oracle, i.e., the place on the operating system where the Oracle SID is installed. For example, `c:\oracle\product\10.1.0\Db_2`.

7. In the **Database Login Credentials** portion of the page:

- Enter the name of the **Net Service Name** (128 alphanumeric characters maximum, including spaces) for the Oracle SID or service you want to monitor. See your database administrator if you are unsure of this value.

Note: The **Oracle TNS Listener** is the server-based process that provides basic network connectivity for clients, application servers, and other databases to an Oracle database. A Listener can provide network connectivity to one or many SIDs and services.

- Enter the **Oracle login** and **Login password** for your Oracle SID or service -- if you plan to use Filters.

Note: For Windows authentication, leave these fields blank. The user ID defaults to the "SYS" user.

- When you are finished configuring DbProtect Audit and Threat Management and defining all Rules, you can re-configure your Sensors **without** an Oracle SID or service user name and password, and then re-deploy the Sensors.

Note: To enhance security, the user name/password pair that you enter is stored in encrypted form on the Sensor.

8. In the **Advanced Monitoring Properties** portion of the page:

- **Modify the Sensor's Polling Rate.** The **Polling Rate** (in milliseconds) is how often the Sensor polls for incoming database events and adjusts the rate interval. Lower values yield the best accuracy but increase CPU utilization. Higher values lessen the load on CPU utilization, but also diminish accuracy (in other words, some events may not be detected). Modifying this value yields variable results, depending on your database and system load and system hardware. Default = `10` milliseconds.
- **Modify the Sensor's inactivity duration.** The **Inactivity Duration** is the amount of time (in seconds) that must elapse with no activity on an Oracle SID or service before the Sensor generates an inactivity Alert. The default value is 5 minutes (`300` seconds). Valid values are `0` to `86400` seconds (i.e., 24 hours).

Note: Entering the value `0` (seconds) disables inactivity monitoring.

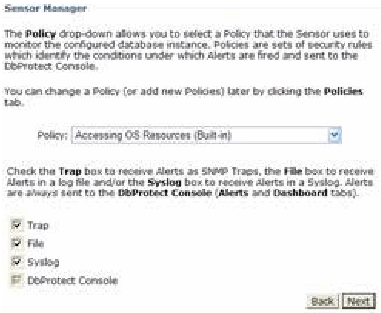
9. In the **Public Addresses** portion of the page:

- Enter the **IP Address:** and **Port:** of the network interface to the remotely-monitored Oracle SID or service.

Note: If you are configuring a host-based Sensor for Oracle on Windows to monitor Oracle databases in an Oracle Fail Safe environment, you **must** configure the network adapter for the cluster's virtual IP address. If this address is not already populated in the **IP Address:** field, then you **must** enter it manually. For more information, see *Appendix B: Monitoring Oracle Databases in an Oracle Fail Safe Environment: Sensor and Cluster Configuration Steps*.

- Click the **Add** button.
- Click the **Next** button.

10. The **Sensor Manager** page shown below allows you to select a Policy that the Sensor uses to monitor the configured Oracle SID or service. Policies are sets of rules which identify the conditions under which Alerts are fired and sent to DbProtect Audit and Threat Management.



Sensor Manager

The **Policy** drop-down allows you to select a Policy that the Sensor uses to monitor the configured database instance. Policies are sets of security rules which identify the conditions under which Alerts are fired and sent to the DbProtect Console.

You can change a Policy (or add new Policies) later by clicking the **Policies** tab.

Policy: Accessing OS Resources (Built-in)

Check the **Trap** box to receive Alerts as SNMP Traps, the **File** box to receive Alerts in a log file and/or the **Syslog** box to receive Alerts in a Syslog. Alerts are always sent to the **DbProtect Console** (**Alerts** and **Dashboard** tabs).

☑ Trap

☑ File

☑ Syslog

☐ DbProtect Console

FIGURE: Sensor Manager

Use the **Policy:** drop-down to select a built-in or custom Policy the Sensor will use to monitor the configured Oracle SID or service.

Note: Deploying a Policy via the **Policy Manger** allows you to deploy Policies to multiple Oracle SIDs or services simultaneously, which may (or may not) be monitored by the same Sensor. Additionally, you can change the Policies deployed (or deploy multiple additional Policies) any time by clicking the **Policies** tab; for more information, see *Deploying a Policy*.

Caution! If you installed a host-based Sensor for Oracle to monitor Oracle databases on an Oracle RAC, you must deploy the exact same Policy for each host-based Sensor for Oracle (otherwise, you may get inconsistent results for the Alerts you are expecting to see). For more information, see ***Appendix C: Installing and Configuring a Host-Based Sensor for Oracle to Monitor Oracle Databases on an Oracle RAC*** and ***Deploying a Policy***.

11. The grayed-out **DbProtect Console** checkbox indicates Alerts are **always** sent to the DbProtect Console.

You can monitor these Alerts in real-time via the **Alert Manager** and the **Dashboard**; for more information, see *Monitoring, filtering, acknowledging, and archiving Alerts (via the Alert Manager)* and *Monitoring Alerts (via the Dashboard)* respectively. In addition, the **Report Manager** allows you to run **Detail Reports** and **Summary Reports** for Alerts.

Optionally, on this page you can check:

- **Trap** to receive Alerts also as SNMP traps
- **File** to receive Alerts also in a log file
- **Syslog** to receive Alerts also as Syslog messages.

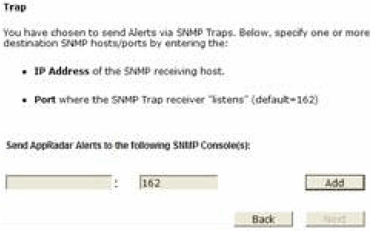
12. Click the **Next** button. If you checked:

- **Trap**, then go to Step 13
- **File**, then go to Step 14
- **Syslog**, then go to Step 15.

Otherwise, go to Step 16.

13. Receiving Alerts as SNMP traps.

The **SNMP trap Configuration** page displays (if you checked **Trap**).



Trap

You have chosen to send Alerts via SNMP Traps. Below, specify one or more destination SNMP hosts/ports by entering the:

- **IP Address** of the SNMP receiving host.
- **Port** where the SNMP Trap receiver "listens" (default=162)

Send AppRadar Alerts to the following SNMP Console(s):

: 162

FIGURE: Sensor Manager

Specify the SNMP server **IP Address** (**not** the host name) of the SNMP receiving host, and the **port** number where the SNMP trap receiver "listens".

Note: The default port is `162`, not `80`.

- Click the **Add** button.
- Click the **Next** button.

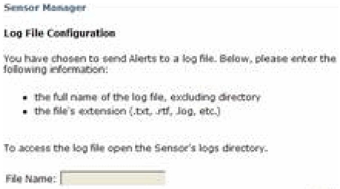
If you also checked:

- **File**, then go to Step 14
- **Syslog**, then go to Step 15.

Otherwise, go to Step 16.

14. Receiving Alerts as Log Files.

The **Log File Configuration** page displays (if you checked **File**).



Sensor Manager

Log File Configuration

You have chosen to send Alerts to a log file. Below, please enter the following information:

- the full name of the log file, excluding directory
- the file's extension (.txt, .rtf, .log, etc.)

To access the log file open the Sensor's logs directory.

File Name:

FIGURE: Sensor Manager

Do the following:

- Enter an Alert log file name in **File Name:** field.

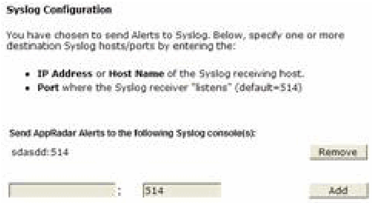
  Be sure to enter the full name of the log file (including the directory), and the log file's extension (e.g., `.txt`, `.rtf`, `.log`, etc.).

  The Alert log file is stored in the `Sensor_installation_directory\logs` directory, where `Sensor_installation_directory` is where the Sensor is installed.
- Click the **Next** button.

If you also checked **Syslog**, then go to Step 15. Otherwise, go to Step 16.

15.Receiving Alerts as Syslog messages.

The **Syslog File Configuration** page displays (if you checked **Syslog**). For a sample Syslog message, see the *DbProtect Administrator's Guide*.



Syslog Configuration

You have chosen to send Alerts to Syslog. Below, specify one or more destination Syslog hosts/ports by entering the:

- **IP Address** or **Host Name** of the Syslog receiving host.
- **Port** where the Syslog receiver "listens" (default=514)

Send AppRadar Alerts to the following Syslog console(s):

sdasdd:514

FIGURE: Sensor Manager

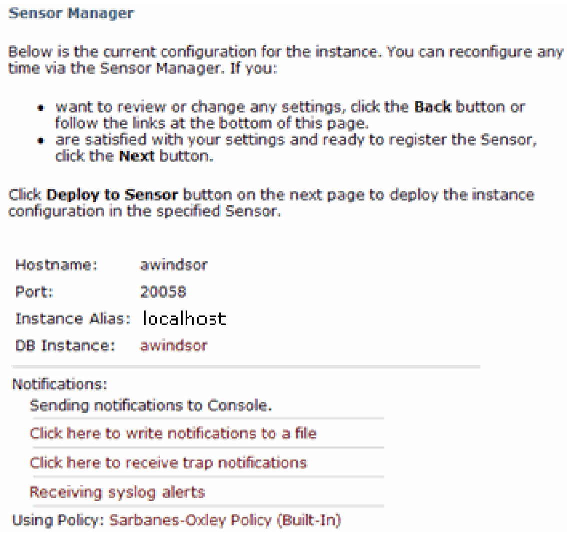
Specify the Syslog server IP Address (**not** the host name), and the port number of the target Syslog server where you want Alerts sent.

Note: The default port is `514` (not `80`).

Caution! The Syslog port is a User Datagram Protocol (UDP) port, as opposed to Transmission Control Protocol (TCP).

- Optionally, click the **Add** button and specify an additional Syslog server IP Address, and an additional port number of the target Syslog server where you want Alerts sent.
- When you're done, click the **Next** button.

16. After you finish specifying the SNMP trap, and/or log file, and/or Syslog parameters, then the **Sensor Manager** summary page displays.



Sensor Manager

Below is the current configuration for the instance. You can reconfigure any time via the Sensor Manager. If you:

- want to review or change any settings, click the **Back** button or follow the links at the bottom of this page.
- are satisfied with your settings and ready to register the Sensor, click the **Next** button.

Click **Deploy to Sensor** button on the next page to deploy the instance configuration in the specified Sensor.

Hostname: awindsor
Port: 20058
Instance Alias: localhost
DB Instance: awindsor

Notifications:
Sending notifications to Console.
Click here to write notifications to a file
Click here to receive trap notifications
Receiving syslog alerts
Using Policy: Sarbanes-Oxley Policy (Built-In)

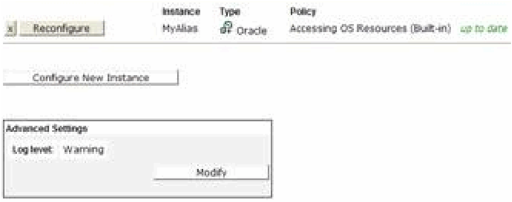
FIGURE: Sensor Manager

If you:

- want to review or change any settings you can click the **Back** button or any link that displays on the page
- are satisfied with your settings and ready to deploy the configuration to the Sensor, click the **Next** button.

Note: You can reconfigure the Sensor any time via the **Sensor Manager**.

The **Sensor Manager** page from Step 2 re-displays.



Instance	Type	Policy	
MyAlias	Oracle	Accessing OS Resources (Built-in)	up to date

Advanced Settings

Log level: Warning

FIGURE: Sensor Manager

17. In the bottom, right corner of the page you can click the:

- **Deploy to Sensor** button to deploy this configured instance to the specified Sensor
- **Cancel** button to cancel the Sensor configuration.

Caution! All your configuration changes will be lost if you click the **Cancel** button.

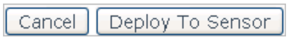


FIGURE: **Cancel** and **Deploy to Sensor** buttons

Or you can click the:

- **Reconfigure Sensor** button to reconfigure the Sensor before deploying the instance configuration in the specified Sensor
- **Configure New Instance** button, if available (for a host-based Sensor, this button may be disabled if DbProtect Audit and Threat Management does **not** detect additional database instances for this server).

For more information, go back to Step 2.

CONFIGURING A HOST-BASED SENSOR TO MONITOR ORACLE SIDS AND SERVICES AND DEPLOYING THE CONFIGURATION INFORMATION (WHEN SENSOR IS INSTALLED ON A *NIX-BASED OPERATING SYSTEM)

Note: DbProtect audit and threat management may have limitations based on the type of Sensor, the nature of the activity, the target database, and the operating system.

Host-based Sensors detect both local and remote attacks. However, they detect only successfully executed commands. For example, a vulnerable database system may permit a certain type of attack, and that attack causes the host-based Sensor to generate an Alert. Importantly, a patched system generally rejects the same command, thus preventing a host-based Sensor from detecting an attempted breach.

For more information, see *DbProtect audit and threat management limitations (based on Sensor type, activity, target database, and operating system).*

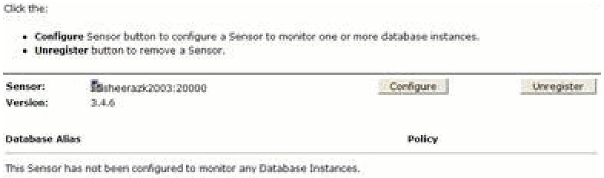
Important: If you installed a host-based Sensor for Oracle to monitor Oracle databases on an Oracle RAC (regardless of host platform) you must appropriately configure the host-based Sensor. For more information, see *Appendix C: Installing and Configuring a Host-Based Sensor for Oracle to Monitor Oracle Databases on an Oracle RAC.*

To configure a host-based Sensor to monitor Oracle SIDs and services and deploy the configuration information (when Sensor is installed on a *nix-based operating system, i.e., Solaris, AIX, HP-UX, or Red Hat Enterprise Linux):

1. Do one of the following to display the first **Sensor Manager** page:

- Click the **Sensors - Manage Sensor** workflow link on the **Home** page.
- Click the **Sensors** tab from anywhere on the page.

The first **Sensor Manager** page displays your registered Sensors.



Click the:

- **Configure** Sensor button to configure a Sensor to monitor one or more database instances.
- **Unregister** button to remove a Sensor.

Sensor: sheerazk2003:20000

Version: 3.4.6

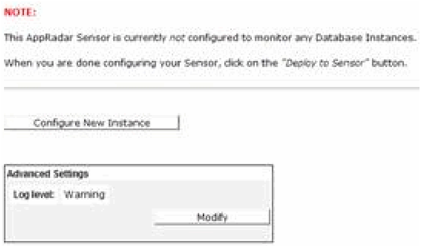
Database Alias	Policy

This Sensor has not been configured to monitor any Database Instances.

FIGURE: Sensor Manager

2. Click the **Configure** button (if you are configuring a Sensor for the first time), or the **Reconfigure** button (if you are reconfiguring a Sensor).

The next **Sensor Manager** page displays.



NOTE:

This AppRadar Sensor is currently *not* configured to monitor any Database Instances.

When you are done configuring your Sensor, click on the *"Deploy to Sensor"* button.

FIGURE: Sensor Manager

This **Sensor Manager** page shows the:

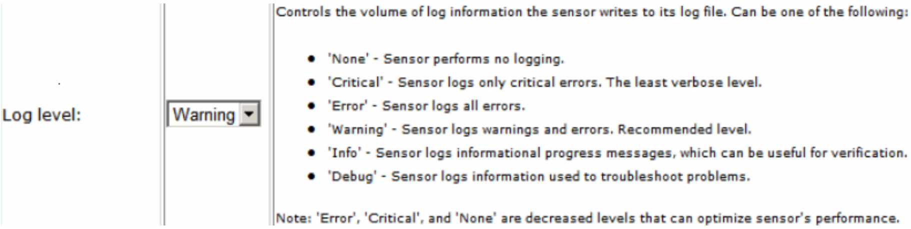
- **Alias** of any host server you have configured for your Sensor
- database **Type** of the instance where your Sensor is registered
- database instance **(DB Instance)** where your Sensor is registered
- **Policy** associated with the registered Sensor.

Note: The Console also displays whether the rules in your **Policy** are up-to-date or out-of-date. If a Policy is out-of-date, you can ASAP Update your Sensor with the latest security Rules (for more information, see *Performing an ASAP Update of Rules in your Sensors*), then use the **Policy Editor** to update Policies (deployed to your Sensors) with the new security Rules (for more information, see *Creating a Policy* and *Editing a Policy*).

When you’re done, you can click the:

- **Modify** button in the **Advanced Settings** portion of the page to display the **Advanced Sensor Settings** page, which allows you to select the Sensor's logging level (see Step 4)
- **Configure New Instance** button to configure a new **Oracle SID or service** for the Sensor (see Steps 5-16)
- **Reconfigure** button to modify the current configuration of an **Oracle SID or service** for the Sensor (see Steps 6-16)
- **X** button to delete a configured Sensor monitoring an instance; for more information, see *Deleting configured Sensors*.

3. The **Advanced Sensor Settings** page allows you to modify the Sensor's **logging level** and/or modify the **inactivity duration**.



Log level: Warning ▾

Controls the volume of log information the sensor writes to its log file. Can be one of the following:

- 'None' - Sensor performs no logging.
- 'Critical' - Sensor logs only critical errors. The least verbose level.
- 'Error' - Sensor logs all errors.
- 'Warning' - Sensor logs warnings and errors. Recommended level.
- 'Info' - Sensor logs informational progress messages, which can be useful for verification.
- 'Debug' - Sensor logs information used to troubleshoot problems.

Note: 'Error', 'Critical', and 'None' are decreased levels that can optimize sensor's performance.

FIGURE: **Advanced Sensor Settings** page

To modify the Sensor's logging level.

Use the **Log level:** drop-down to select the Sensor's logging level, which controls the volume of log information the Sensor outputs to its log file. You can select:

- **None.** Sensor performs no logging.
- **Critical.** Sensor logs only critical errors. The **least** verbose level.
- **Error.** Sensor logs **all** errors.
- **Warning.** Sensor logs warnings and errors. Recommended level.
- **Info.** Sensor logs informational progress messages, which can be useful for verification.
- **Debug.** Logs information used to troubleshoot Sensor problems at runtime.

Note: **Error**, **Critical**, and **None** are all decreased logging levels which you can use to optimize Sensor performance.

When you’re done, you can click the **Next** button to display the **Sensor Manager** page from Step 2. You can click the:

- **Configure New Instance** button to configure a new **Oracle SID or service** for the Sensor (see Steps 5-16)
- **Reconfigure** button to modify the current configuration of a **Oracle SID or service** for the Sensor (see Steps 6-16)
- **X** button to delete a configured Sensor monitoring an instance; for more information, see *Deleting configured Sensors*.

4. **Configuring a new instance.**

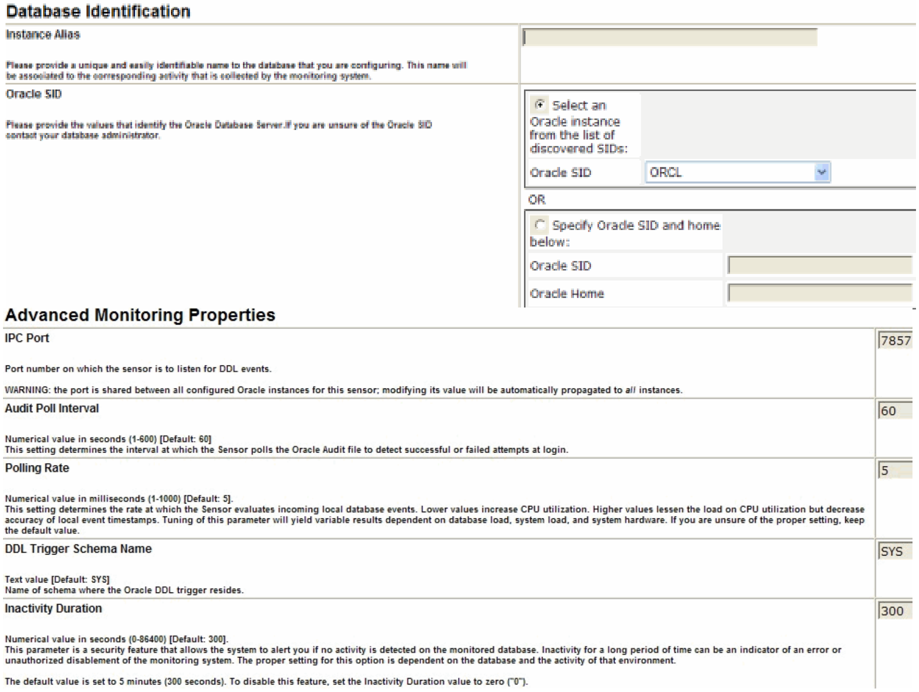
The **Sensor Manager** page prompts you to select a database platform for the host-based Sensor to monitor.

○ IBM DB2 UDB / IBM DB2
○ Oracle Database

FIGURE: **Sensor Manager** page

- Select **Oracle Database**.
- Click the **Next** button.

The **Sensor Manager** page shown below allows you to configure/re-configure a Sensor for host-based **Oracle** (when the Sensor is installed on a *nix-based operating system).



Database Identification

Instance Alias

Please provide a unique and easily identifiable name to the database that you are configuring. This name will be associated to the corresponding activity that is collected by the monitoring system.

Oracle SID

Please provide the values that identify the Oracle Database Server.If you are unsure of the Oracle SID contact your database administrator.

● Select an Oracle instance from the list of discovered SIDs:

Oracle SID: ORCL

OR

○ Specify Oracle SID and home below:

Oracle SID

Oracle Home

Advanced Monitoring Properties

IPC Port: 7857

Port number on which the sensor is to listen for DDL events.

WARNING: the port is shared between all configured Oracle instances for this sensor; modifying its value will be automatically propagated to *all* instances.

Audit Poll Interval: 60

Numerical value in seconds (1-600) [Default: 60]
This setting determines the interval at which the Sensor polls the Oracle Audit file to detect successful or failed attempts at login.

Polling Rate: 5

Numerical value in milliseconds (1-1000) [Default: 5].
This setting determines the rate at which the Sensor evaluates incoming local database events. Lower values increase CPU utilization. Higher values lessen the load on CPU utilization but decrease accuracy of local event timestamps. Tuning of this parameter will yield variable results dependent on database load, system load, and system hardware. If you are unsure of the proper setting, keep the default value.

DDL Trigger Schema Name: SYS

Text value [Default: SYS]
Name of schema where the Oracle DDL trigger resides.

Inactivity Duration: 300

Numerical value in seconds (0-86400) [Default: 300].
This parameter is a security feature that allows the system to alert you if no activity is detected on the monitored database. Inactivity for a long period of time can be an indicator of an error or unauthorized disablement of the monitoring system. The proper setting for this option is dependent on the database and the activity of that environment.

The default value is set to 5 minutes (300 seconds). To disable this feature, set the Inactivity Duration value to zero ("0").

FIGURE: **Sensor Manager** page

This page consists of three portions. If you want to work with the:

- **Database Identification** portion of the page, see Step 5
- **Advanced Monitoring Properties** portion of the page, see Step 6

When you're done, go to Step 7.

5. In the **Database Identification** portion of the page:

- Enter a meaningful Oracle SID alias in the **Instance Alias:** field, for the Oracle SID you want the Sensor to monitor. DbProtect Audit and Threat Management uses this alias to identify the Oracle SID from which Alerts are received.

Important: Your Oracle SID alias can only contain alphanumeric, underscore (_), period (.), and hyphen (-) characters, or spaces. **Acceptable** examples: `ORCL DB1`, `ORCL.DB1`, `ORCL_DB1`, `ORCL-DB1`, etc. **Unacceptable** examples: `ORCL:DB1`, `ORCL/DB1`, etc.

Caution! If you installed a host-based Sensor for Oracle to monitor Oracle databases on an Oracle RAC, make sure your **Instance Alias**: a.) is unique for each registered host-based Sensor for Oracle; b.) is easily identifiable for the database you are monitoring; c.) is easily identifies the node where the Sensor is installed (e.g., **Oracle RAC Node 1**, **Oracle RAC Node 2**, etc.). For more information, see ***Appendix C: Installing and Configuring a Host-Based Sensor for Oracle to Monitor Oracle Databases on an Oracle RAC***.

- The **Oracle SID:** fields allow you to do the following:

  -Select **Select an Oracle instance from the list of discovered SIDs:**, and use the **Oracle SID** drop-down to select an **Oracle SID** where a Sensor is installed (derived from the `oratab` file on the host)

  -Select **Specify Oracle SID and home below:** and manually enter the **Oracle SID** name and the **Oracle Home**.

Note: Oracle Home refers to the home directory for Oracle, i.e., the place on the operating system where the Oracle SID is installed. For example, `/export/home/oracle/OraHome32`. Also, in some installations of Oracle, there may be missing or extraneous configuration entries in the `oratab` file (typically found in the `/var/opt/oracle` or `/etc/oratab`). If this is the case on your server, AppSecInc recommends you manually specify the Oracle Home and Oracle SID.

6. In the **Advanced Monitoring Properties** portion of the page:

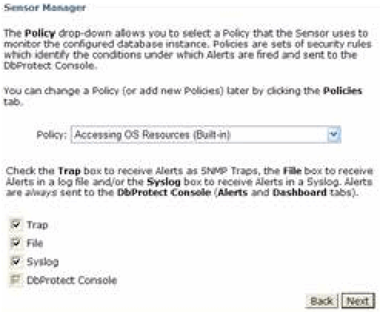
- **IPC Port.** The **IPC Port** is where the Sensor "listens" for Alerts that pertain to Data Definition Language (DDL) changes. Typically, you should not have to change this port number from its default setting of port `7777`.
- **Audit Poll Interval.** The **Audit Poll Interval** is a numerical value in seconds (`1-600`) that represents the interval at which the Sensor polls the Oracle Audit file to detect successful or failed login attempts. Default = `60` milliseconds.
- **Polling Rate.** The **Polling Rate** (in milliseconds) is how often the Sensor polls for incoming database events and adjusts the rate interval. Lower values yield the best accuracy but increase CPU utilization. Higher values lessen the load on CPU utilization, but also diminish accuracy (in other words, some events may not be detected). Modifying this value yields variable results, depending on your database and system load and system hardware. Default = `5` milliseconds.
- **DDL Trigger Schema Name.** The **DDL Trigger Schema Name** is the name of the schema where the DDL trigger resides. You can modify this value. The default value is `SYS`. For more information on working with DDL triggers, see *Appendix E: Working with Oracle DDL Triggers* in the *DbProtect Installation Guide*.

- **Inactivity Duration.** The **Inactivity Duration** is the amount of time (in seconds) that must elapse with no activity on an Oracle SID or service before the Sensor generates an inactivity Alert. The default value is 5 minutes (`300` seconds). Valid values are `0` to `86400` seconds (i.e., 24 hours).

Note: Entering the value `0` (seconds) disables inactivity monitoring.

7. Click the **Next** button.

The **Sensor Manager** page shown below allows you to select a Policy that the Sensor uses to monitor the configured Oracle SID or service. Policies are sets of rules which identify the conditions under which Alerts are fired and sent to DbProtect Audit and Threat Management.



Sensor Manager

The **Policy** drop-down allows you to select a Policy that the Sensor uses to monitor the configured database instance. Policies are sets of security rules which identify the conditions under which Alerts are fired and sent to the DbProtect Console.

You can change a Policy (or add new Policies) later by clicking the **Policies** tab.

Policy: Accessing OS Resources (Built-in)

Check the **Trap** box to receive Alerts as SNMP Traps, the **File** box to receive Alerts in a log file and/or the **Syslog** box to receive Alerts in a Syslog. Alerts are always sent to the **DbProtect Console** (**Alerts** and **Dashboard** tabs).

☑ Trap
☑ File
☑ Syslog
☑ DbProtect Console

FIGURE: Sensor Manager

Use the **Policy:** drop-down to select a built-in or custom Policy the Sensor will use to monitor the configured Oracle SID or service.

Note: Deploying a Policy via the **Policy Manger** allows you to deploy Policies to multiple Oracle SIDs or services simultaneously, which may (or may not) be monitored by the same Sensor. Additionally, you can change the Policies deployed (or deploy multiple additional Policies) any time by clicking the **Policies** tab; for more information, see *Deploying a Policy*.

Caution! If you installed a host-based Sensor for Oracle to monitor Oracle databases on an Oracle RAC, you must deploy the exact same Policy for each host-based Sensor for Oracle (otherwise, you may get inconsistent results for the Alerts you are expecting to see). For more information, see ***Appendix C: Installing and Configuring a Host-Based Sensor for Oracle to Monitor Oracle Databases on an Oracle RAC*** and ***Deploying a Policy***.

8. The grayed-out **DbProtect Console** checkbox indicates Alerts are **always** sent to the DbProtect Console.

You can monitor these Alerts in real-time via the **Alert Manager** and the **Dashboard**; for more information, see *Monitoring, filtering, acknowledging, and archiving Alerts (via the Alert Manager)* and *Monitoring Alerts (via the Dashboard)* respectively. In addition, the **Report Manager** allows you to run **Detail Reports** and **Summary Reports** for Alerts.

Optionally, on this page you can check:

- **Trap** to receive Alerts also as SNMP traps
- **File** to receive Alerts also in a log file
- **Syslog** to receive Alerts also as Syslog messages.

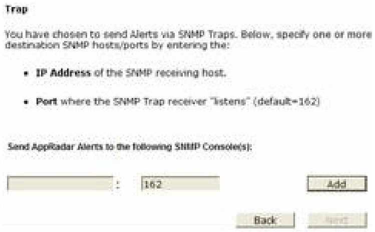
9. Click the **Next** button. If you checked:

- **Trap**, then go to Step 10
- **File**, then go to Step 11
- **Syslog**, then go to Step 12.

Otherwise, go to Step 13.

10.Receiving Alerts as SNMP traps.

The **SNMP trap Configuration** page displays (if you checked **Trap**).



Trap

You have chosen to send Alerts via SNMP Traps. Below, specify one or more destination SNMP hosts/ports by entering the:

- **IP Address** of the SNMP receiving host.
- **Port** where the SNMP Trap receiver "listens" (default=162)

Send AppRadar Alerts to the following SNMP Console(s):

: 162

FIGURE: Sensor Manager

Specify the SNMP server **IP Address** (**not** the host name) of the SNMP receiving host, and the **port** number where the SNMP trap receiver "listens".

Note: The default port is `162`, not `80`.

- Click the **Add** button.
- Click the **Next** button.

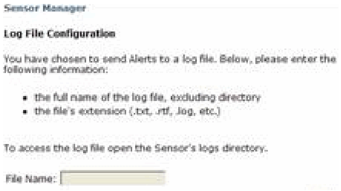
If you also checked:

- **File**, then go to Step 11
- **Syslog**, then go to Step 12.

Otherwise, go to Step 13.

11. Receiving Alerts as Log Files.

The **Log File Configuration** page displays (if you checked **File**).



Sensor Manager

Log File Configuration

You have chosen to send Alerts to a log file. Below, please enter the following information:

- the full name of the log file, excluding directory
- the file's extension (.txt, .rtf, .log, etc.)

To access the log file open the Sensor's logs directory.

File Name:

FIGURE: Sensor Manager

Do the following:

- Enter an Alert log file name in **File Name:** field.

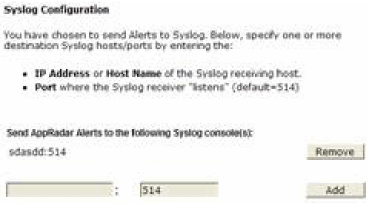
  Be sure to enter the full name of the log file (including the directory), and the log file's extension (e.g., `.txt`, `.rtf`, `.log`, etc.).

  The Alert log file is stored in the `Sensor_installation_directory\logs` directory, where `Sensor_installation_directory` is where the Sensor is installed.
- Click the **Next** button.

If you also checked **Syslog**, then go to Step 12. Otherwise, go to Step 13.

12. Receiving Alerts as Syslog messages.

The **Syslog File Configuration** page displays (if you checked **Syslog**). For a sample Syslog message, see the *DbProtect Administrator's Guide*.



Syslog Configuration

You have chosen to send Alerts to Syslog. Below, specify one or more destination Syslog hosts/ports by entering the:

- **IP Address** or **Host Name** of the Syslog receiving host.
- **Port** where the Syslog receiver "listens" (default=514)

Send AppRadar Alerts to the following Syslog console(s):

sdasdd:514

FIGURE: Sensor Manager

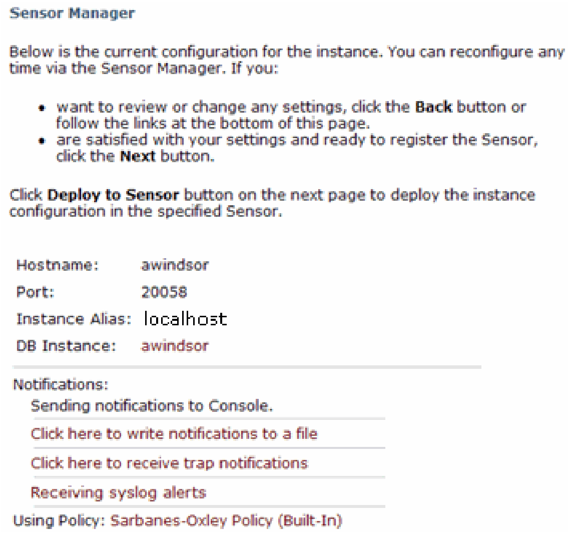
Specify the Syslog server IP Address (**not** the host name), and the port number of the target Syslog server where you want Alerts sent.

Note: The default port is `514` (not `80`).

Caution! The Syslog port is a User Datagram Protocol (UDP) port, as opposed to Transmission Control Protocol (TCP).

- Optionally, click the **Add** button and specify an additional Syslog server IP Address, and an additional port number of the target Syslog server where you want Alerts sent.
- When you're done, click the **Next** button.

13. After you finish specifying the SNMP trap, and/or log file, and/or Syslog parameters, then the **Sensor Manager** summary page displays.



Sensor Manager

Below is the current configuration for the instance. You can reconfigure any time via the Sensor Manager. If you:

- want to review or change any settings, click the **Back** button or follow the links at the bottom of this page.
- are satisfied with your settings and ready to register the Sensor, click the **Next** button.

Click **Deploy to Sensor** button on the next page to deploy the instance configuration in the specified Sensor.

Hostname:	awindsor
Port:	20058
Instance Alias:	localhost
DB Instance:	awindsor

Notifications:

Sending notifications to Console.

Click here to write notifications to a file

Click here to receive trap notifications

Receiving syslog alerts

Using Policy: Sarbanes-Oxley Policy (Built-In)

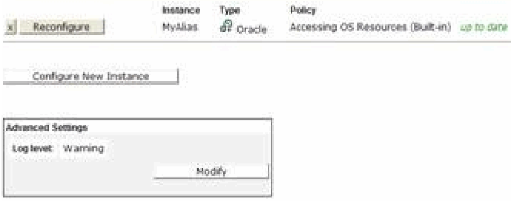
FIGURE: Sensor Manager

If you:

- want to review or change any settings you can click the **Back** button or any link that displays on the page
- are satisfied with your settings and ready to deploy the configuration to the Sensor, click the **Next** button.

Note: You can reconfigure the Sensor any time via the **Sensor Manager**.

The **Sensor Manager** page from Step 2 re-displays.



	Instance	Type	Policy	
x Reconfigure	MyAlias	Oracle	Accessing OS Resources (Built-in)	up to date

Advanced Settings

Log level: Warning

FIGURE: Sensor Manager

14. In the bottom, right corner of the page you can click the:

- **Deploy to Sensor** button to deploy this configured instance to the specified Sensor
- **Cancel** button to cancel the Sensor configuration.

Caution! All your configuration changes will be lost if you click the **Cancel** button.

FIGURE: **Cancel** and **Deploy to Sensor** buttons

Or you can click the:

- **Reconfigure Sensor** button to reconfigure the Sensor before deploying the instance configuration in the specified Sensor
- **Configure New Instance** button, if available (for a host-based Sensor, this button may be disabled if DbProtect Audit and Threat Management does **not** detect additional database instances for this server).

For more information, go back to Step 2.

CONFIGURING A NETWORK-BASED SENSOR TO MONITOR A SYBASE DATABASE SERVER AND DEPLOYING THE CONFIGURATION INFORMATION (WHEN SENSOR IS INSTALLED ON WINDOWS)

Note: DbProtect audit and threat management may have limitations based on the type of Sensor, the nature of the activity, the target database, and the operating system.

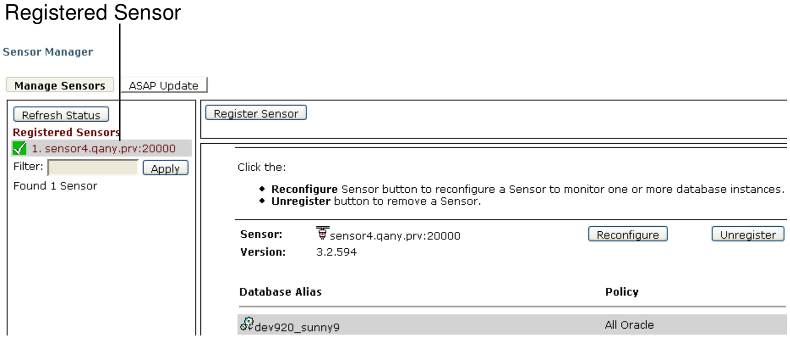
Network-based Sensors fire Alerts for all remote connections, e.g., from a web server communicating to its remote back-end database. However, they do not detect activity originating from the database host.

For more information, see *DbProtect audit and threat management limitations (based on Sensor type, activity, target database, and operating system).*

To configure a network-based Sensor to monitor a Sybase database server and deploying the configuration information (when Sensor is installed on Windows):

1. Do one of the following:
   - Click the **Sensors - Manage Sensor** workflow link on the **Home** page.
   - Click the **Sensors** tab from anywhere on the page.

The first **Sensor Manager** page displays your already-registered Sensors.



✓ 1. sensor4.qany.prv:20000

Filter:

Found 1 Sensor

Click the:

- **Reconfigure** Sensor button to reconfigure a Sensor to monitor one or more database instances.
- **Unregister** button to remove a Sensor.

Sensor: sensor4.qany.prv:20000
Version: 3.2.594

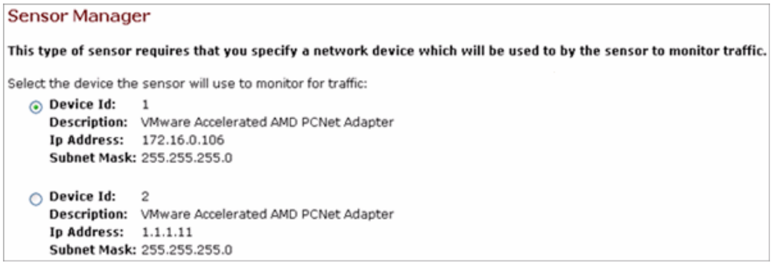
Database Alias	**Policy**
dev920_sunny9	All Oracle

FIGURE: Sensor Manager

If you have not registered *any* Sensors, then the first **Sensor Manager** page displays a message.

2. Click the **Configure** button (if you are configuring a Sensor for the first time), or the **Reconfigure** button (if you are reconfiguring a Sensor).

If you are configuring a new network-based Sensor, the next **Sensor Manager** page prompts you to specify a network device the Sensor will use to monitor traffic. If you have already configured the Sensor, go to Step 4.



Sensor Manager

This type of sensor requires that you specify a network device which will be used to by the sensor to monitor traffic.

Select the device the sensor will use to monitor for traffic:

● **Device Id:** 1
Description: VMware Accelerated AMD PCNet Adapter
Ip Address: 172.16.0.106
Subnet Mask: 255.255.255.0

○ **Device Id:** 2
Description: VMware Accelerated AMD PCNet Adapter
Ip Address: 1.1.1.11
Subnet Mask: 255.255.255.0

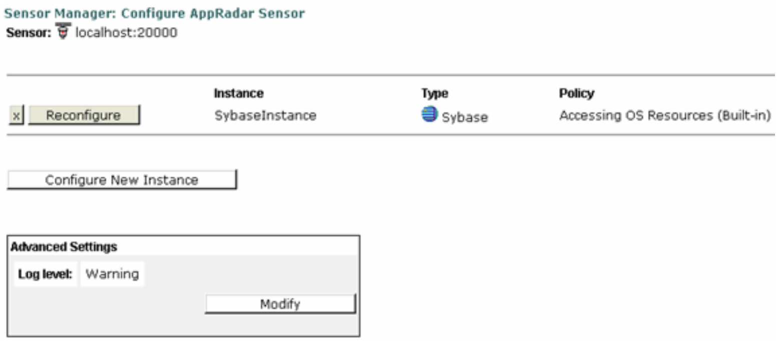
FIGURE: Sensor Manager

3. Select which network device the Sensor should use to monitor traffic. In addition to the **name** of the device, you should also know the **host IP address** each device is configured to use, and the **subnet mask** of the network device. For example:

- **Device ID:** The number of the NIC (Network Interface Card) in the Sensor server. If the server only has one NIC, then the Device ID is `1`. If there are multiple NICs on the server machine, they are listed as `Device ID: 1`, `Device ID: 2`, etc.
- **Description:** The make and model of the NIC, e.g., `3com 905B`
- **Host IP Address:** The host IP address of the NIC, e.g., `192.168.1.5`
- **Subnet Mask:** The address of your organization's subnet, e.g., `255.255.255.0`.

4. The **Sensor Manager** page shows the:

- **Alias** of any host server you have configured for your Sensor
- database **Type** of the instance where your Sensor is registered
- database instance **(DB Instance)** where your Sensor is registered
- **Policy** associated with the registered Sensor.



Sensor Manager: Configure AppRadar Sensor

Sensor: localhost:20000

	Instance	Type	Policy
☒ Reconfigure	SybaseInstance	Sybase	Accessing OS Resources (Built-in)

Advanced Settings

Log level: Warning

FIGURE: Sensor Manager

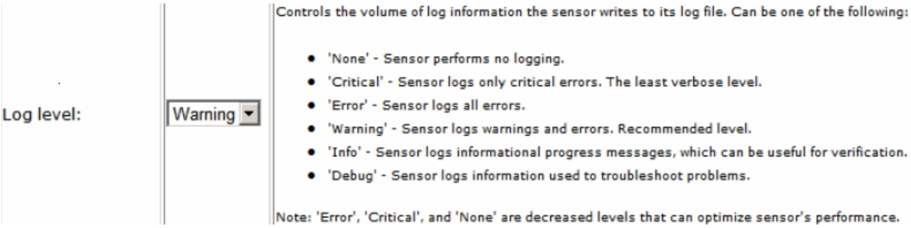
Note: The Console also displays whether the rules in your **Policy** are up-to-date or out-of-date. If a Policy is out-of-date, you can ASAP Update your Sensor with the latest security Rules (for more information, see *Performing an ASAP Update of Rules in your Sensors*), then use the **Policy Editor** to update Policies (deployed to your Sensors) with the new security Rules (for more information, see *Creating a Policy* and *Editing a Policy*).

5. You can click the:

- **Modify** button in the **Advanced Settings** portion of the page to display the **Advanced Sensor Settings** page, which allows you to select the Sensor's logging level (see Steps 6-7)
- **Configure New Instance** button to configure a new **Sybase database server** for the Sensor (see Steps 8-19)

- **Reconfigure** button to modify the current configuration of an **Sybase database server** for the Sensor (see Steps 8-19)
- **X** button to delete a configured Sensor monitoring an instance; for more information, see *Deleting configured Sensors*.

6. The **Advanced Sensor Settings** page allows you to modify the Sensor's **logging level**.



Log level: Warning

Controls the volume of log information the sensor writes to its log file. Can be one of the following:

- 'None' - Sensor performs no logging.
- 'Critical' - Sensor logs only critical errors. The least verbose level.
- 'Error' - Sensor logs all errors.
- 'Warning' - Sensor logs warnings and errors. Recommended level.
- 'Info' - Sensor logs informational progress messages, which can be useful for verification.
- 'Debug' - Sensor logs information used to troubleshoot problems.

Note: 'Error', 'Critical', and 'None' are decreased levels that can optimize sensor's performance.

FIGURE: **Advanced Sensor Settings** page

To modify the Sensor's logging level:

Use the **Log level:** drop-down to select the Sensor's logging level, which controls the volume of log information the Sensor outputs to its log file. You can select:

- **None.** Sensor performs no logging.
- **Critical.** Sensor logs only critical errors. The **least** verbose level.
- **Error.** Sensor logs **all** errors.
- **Warning.** Sensor logs warnings and errors. Recommended level.
- **Info.** Sensor logs informational progress messages, which can be useful for verification.
- **Debug.** Logs information used to troubleshoot Sensor problems at runtime.

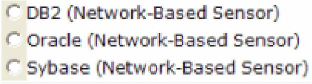
Note: **Error**, **Critical**, and **None** are all decreased logging levels which you can use to optimize Sensor performance.

7. When you're done, you can click the **Next** button to re-display the second **Sensor Manager** page (see Step 4), then click the:

- **Configure New Instance** button to configure a new **Sybase database server** for the Sensor (see Steps 8-19)
- **Reconfigure** button to modify the current configuration of a **Sybase database server** for the Sensor (see Steps 8-19).

8. Click the **Next** button.

The next **Sensor Manager** page displays, prompting you to select a database platform for the network-based Sensor to monitor.

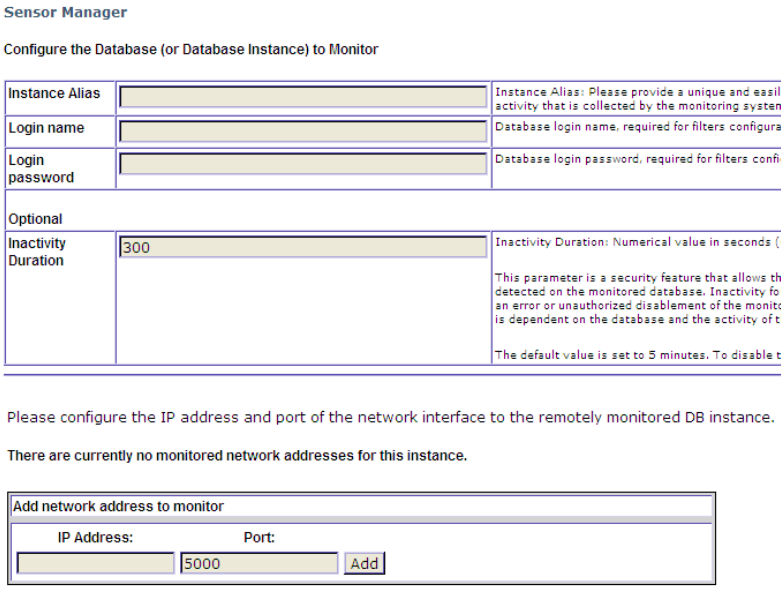


○ DB2 (Network-Based Sensor)
○ Oracle (Network-Based Sensor)
○ Sybase (Network-Based Sensor)

FIGURE: Sensor Manager

9. Select **Sybase (Network-Based Sensor)** and click the **Next** button.

The next **Sensor Manager** page displays.



Sensor Manager

Configure the Database (or Database Instance) to Monitor

Instance Alias		Instance Alias: Please provide a unique and easil activity that is collected by the monitoring systen
Login name		Database login name, required for filters configura
Login password		Database login password, required for filters confi

Optional

Inactivity Duration	300	Inactivity Duration: Numerical value in seconds (This parameter is a security feature that allows th detected on the monitored database. Inactivity fo an error or unauthorized disablement of the monit is dependent on the database and the activity of t The default value is set to 5 minutes. To disable t

Please configure the IP address and port of the network interface to the remotely monitored DB instance.

There are currently no monitored network addresses for this instance.

Add network address to monitor

IP Address: Port: 5000 Add

FIGURE: Sensor Manager

10. Do the following:

- Enter a meaningful instance alias (e.g., `SYBASE_DB1`) in the **Instance Alias** field, for the Sybase database server you want the Sensor to monitor (DbProtect Audit and Threat Management uses this alias to identify the databases from which Alerts are received).
- Enter your Sybase database server **Login Name** and **Login Password** if you plan to use Filters.

  When you are finished configuring DbProtect Audit and Threat Management and defining all Rules, you can re-configure your Sensors **without** a Sybase database server user name and password, and then re-deploy the Sensors.

Note: To enhance security, the user name/password pair that you enter is stored in encrypted form on the Sensor.

- Optionally, in the **Optional** portion of the page, you can modify the value in the **Inactivity duration** field. The "inactivity duration" is the amount of time (in seconds) that must elapse with no activity on a Sybase database server before the Sensor generates an inactivity Alert. The default value is 5 minutes (`300` seconds). Valid values are `0` to `86400` seconds (i.e., 24 hours).

Note: Entering the value `0` (seconds) disables inactivity monitoring.

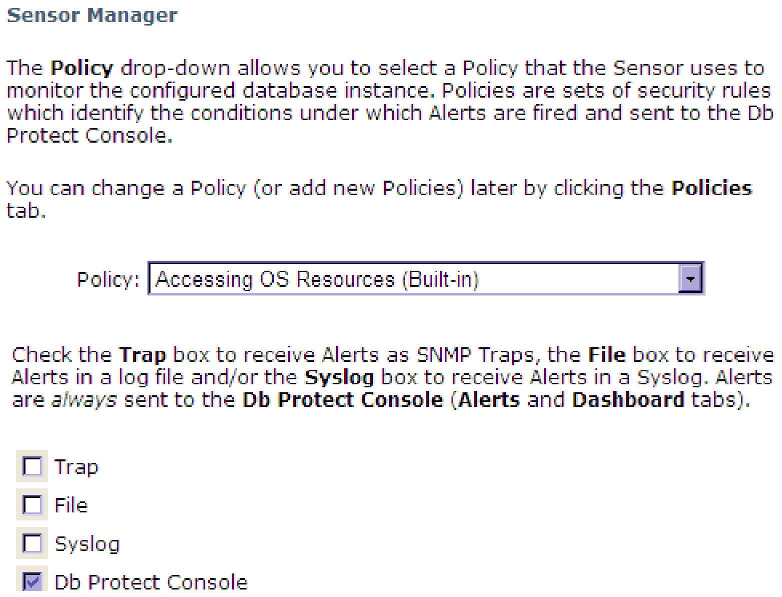
- Enter the **IP Address:** and **Port:** of the network interface to the remotely-monitored Sybase database server.
- Click the **Add** button.

A given host machine can accommodate (and, subsequently, a Sensor can monitor) multiple SIDs, servers, and services, including:

- **DB2 database servers**; for more information, see *Configuring a network-based Sensor to monitor a DB2 database server and deploying the configuration information (when Sensor is installed on Windows)*)
- **Oracle SIDS and services**; for more information, see *Configuring a network-based Sensor to monitor Oracle SIDs and services and deploying the configuration information (when Sensor is installed on Windows)*.

11. When you're done specifying the databases on the host machine that you want the Sensor to monitor, click the **Next** button.

The next **Sensor Manager** page displays.



Sensor Manager

The **Policy** drop-down allows you to select a Policy that the Sensor uses to monitor the configured database instance. Policies are sets of security rules which identify the conditions under which Alerts are fired and sent to the Db Protect Console.

You can change a Policy (or add new Policies) later by clicking the **Policies** tab.

Policy: Accessing OS Resources (Built-in)

Check the **Trap** box to receive Alerts as SNMP Traps, the **File** box to receive Alerts in a log file and/or the **Syslog** box to receive Alerts in a Syslog. Alerts are *always* sent to the **Db Protect Console** (**Alerts** and **Dashboard** tabs).

☐ Trap
☐ File
☐ Syslog
☑ Db Protect Console

FIGURE: Sensor Manager

12. Use the **Policy** drop-down to select a built-in or custom Policy that the Sensor will use to monitor the configured database. Policies are sets of security Rules which identify the conditions under which Alerts are fired and sent to DbProtect Audit and Threat Management. Different Sensors and databases may require different Policies, since intrusion risk and data sensitivity will vary between database installations.

Note: You can change the Policy associated with a configured database instance (or deploy multiple additional Policies to a configured database instance) any time by clicking the **Policies** tab; for more information, see *Deploying a Policy*.

13. The grayed-out **DbProtect Console** checkbox indicates Alerts are **always** sent to the DbProtect Console.

You can monitor these Alerts in real-time via the **Alert Manager** and the **Dashboard**; for more information, see *Monitoring, filtering, acknowledging, and archiving Alerts (via the Alert Manager)* and *Monitoring Alerts (via the Dashboard)*, respectively. In addition, the **Report Manager** allows you to run **Detail Reports** and **Summary Reports** for Alerts. For more information, see *Reports*.

Optionally, on this page you can check the:

- **Trap** checkbox to receive Alerts also as SNMP traps
- **File** checkbox to receive Alerts also in a log file
- **Syslog** checkbox to receive Alerts as Syslog messages.

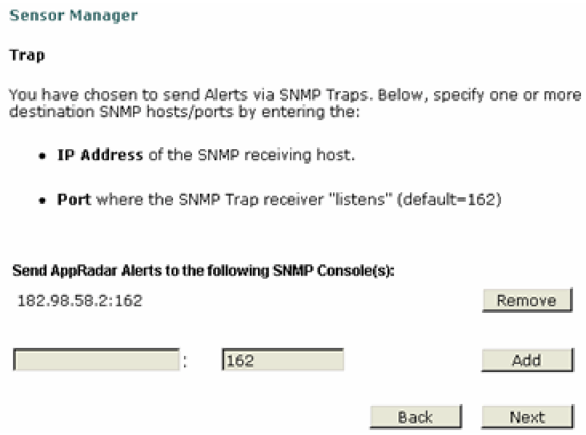
14. Click the **Next** button. If you checked the:

- **Trap** checkbox, then go to Step 15
- **File** checkbox, then go to Step 16
- **Syslog** checkbox, then go to Step 17.

Otherwise, go to Step 18.

15.Receiving Alerts as SNMP traps.

The **SNMP trap Configuration** page displays (if you clicked the **Trap** checkbox in Step 13).



Sensor Manager

Trap

You have chosen to send Alerts via SNMP Traps. Below, specify one or more destination SNMP hosts/ports by entering the:

- **IP Address** of the SNMP receiving host.
- **Port** where the SNMP Trap receiver "listens" (default=162)

Send AppRadar Alerts to the following SNMP Console(s):

182.98.58.2:162

: 162

FIGURE: **Sensor Manager**

Specify the SNMP server **IP Address** (**not** the host name) of the SNMP receiving host, and the **port** number where the SNMP trap receiver "listens".

Note: The default port is `162`, not `80`.

- Click the **Add** button.
- Click the **Next** button.

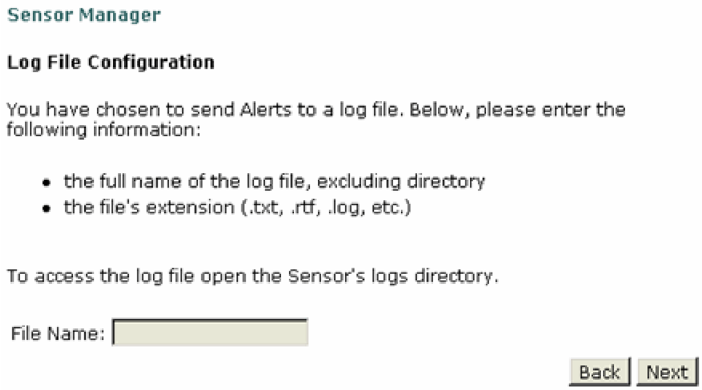
If you also checked the:

- **File** checkbox in Step 13, then go to Step 16
- **Syslog** checkbox in Step 13, then go to Step 17.

Otherwise, go to Step 18.

16.Receiving Alerts as Log Files.

The **Log File Configuration** page displays (if you clicked the **File** checkbox in Step 13).



Sensor Manager

Log File Configuration

You have chosen to send Alerts to a log file. Below, please enter the following information:

- the full name of the log file, excluding directory
- the file's extension (.txt, .rtf, .log, etc.)

To access the log file open the Sensor's logs directory.

File Name:

FIGURE: Sensor Manager

Do the following:

- Enter an Alert log file name in **File Name** field.

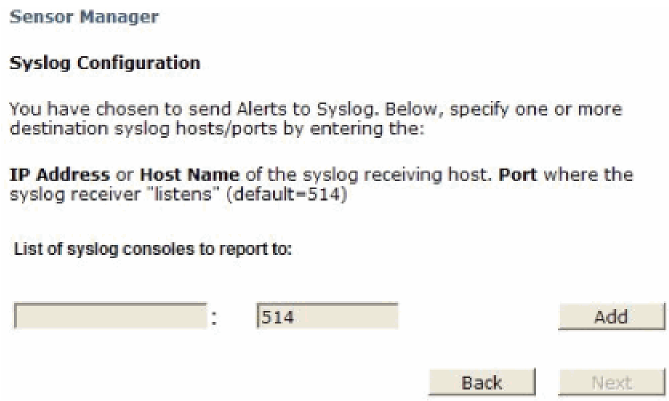
  Be sure to enter the full name of the log file (including the directory), and the log file’s extension (e.g., `.txt`, `.rtf`, `.log`, etc.).

  The Alert log file is stored in the `Sensor_installation_directory\logs` directory, where `Sensor_installation_directory` is where the Sensor is installed.
- Click the **Next** button.

If you also checked the **Syslog** checkbox in Step 13, then go to Step 17. Otherwise, go to Step 18.

17. Receiving Alerts as Syslog messages.

The **Syslog File Configuration** page displays (if you clicked the **Syslog** checkbox in Step 13). For a sample Syslog message, see the *DbProtect Administrator’s Guide*.



Sensor Manager

Syslog Configuration

You have chosen to send Alerts to Syslog. Below, specify one or more destination syslog hosts/ports by entering the:

IP Address or **Host Name** of the syslog receiving host. **Port** where the syslog receiver "listens" (default=514)

List of syslog consoles to report to:

FIGURE: Sensor Manager

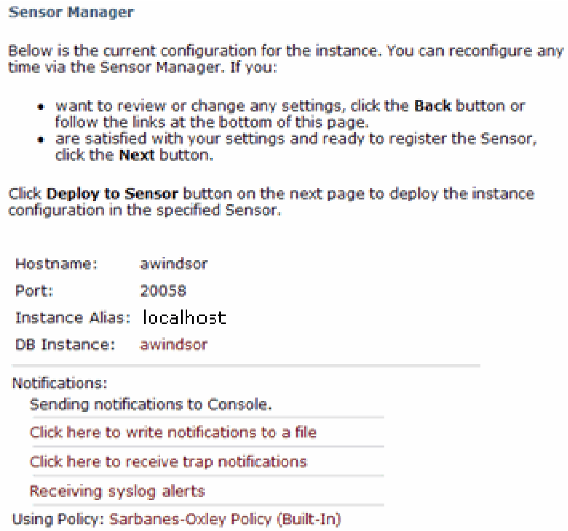
Specify the Syslog server IP Address (**not** the host name), and the port number of the target Syslog server where you want Alerts sent.

Note: The default port is `514` (not `80`).

Caution! The Syslog port is a User Datagram Protocol (UDP) port, as opposed to Transmission Control Protocol (TCP).

- Click the **Add** button.
- Click the **Next** button.

18. After you finish specifying the SNMP trap, and/or log file, and/or Syslog parameters (depending on which checkboxes, if any, you selected), then the **Sensor Manager** summary page displays.



Sensor Manager

Below is the current configuration for the instance. You can reconfigure any time via the Sensor Manager. If you:

- want to review or change any settings, click the **Back** button or follow the links at the bottom of this page.
- are satisfied with your settings and ready to register the Sensor, click the **Next** button.

Click **Deploy to Sensor** button on the next page to deploy the instance configuration in the specified Sensor.

Hostname:	awindsor
Port:	20058
Instance Alias:	localhost
DB Instance:	awindsor

Notifications:
Sending notifications to Console.
Click here to write notifications to a file
Click here to receive trap notifications
Receiving syslog alerts
Using Policy: Sarbanes-Oxley Policy (Built-In)

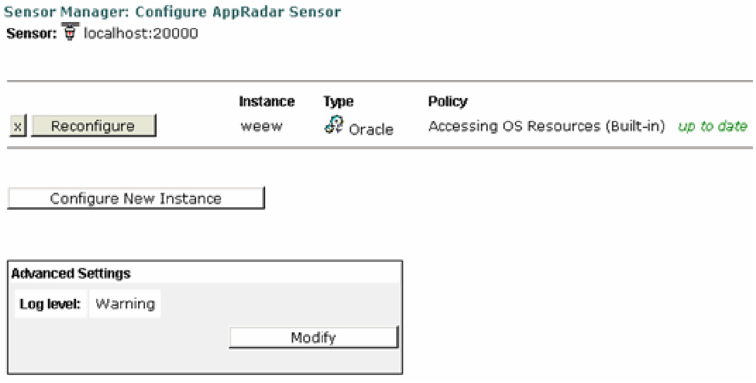
FIGURE: Sensor Manager

If you:

- want to review or change any settings you can click the **Back** button or any link that displays on the page
- are satisfied with your settings and ready to deploy the configuration to the Sensor, click the **Next** button.

Note: You can reconfigure the Sensor any time via the Sensor Manager.

19. The first **Sensor Manager** page re-displays.



Sensor Manager: Configure AppRadar Sensor

Sensor: localhost:20000

	Instance	Type	Policy
	weew	Oracle	Accessing OS Resources (Built-in) *up to date*

Advanced Settings

Log level: Warning

FIGURE: Sensor Manager

You can click the:

- **Reconfigure** button to reconfigure the Sensor before deploying the configuration to the specified Sensor
- **Cancel** button to cancel the configuration
- **Deploy to Sensor** button to deploy this configuration to the specified Sensor

Important: You **must** click the **Deploy to Sensor** button to make your modifications permanent.

- **Configure New Instance** button to configure a new database.

CONFIGURING A NETWORK-BASED SENSOR TO MONITOR A DB2 DATABASE SERVER AND DEPLOYING THE CONFIGURATION INFORMATION (WHEN SENSOR IS INSTALLED ON WINDOWS)

Note: DbProtect audit and threat management may have limitations based on the type of Sensor, the nature of the activity, the target database, and the operating system.

Network-based Sensors fire Alerts for all remote connections, e.g., from a web server communicating to its remote back-end database. However, they do not detect activity originating from the database host.

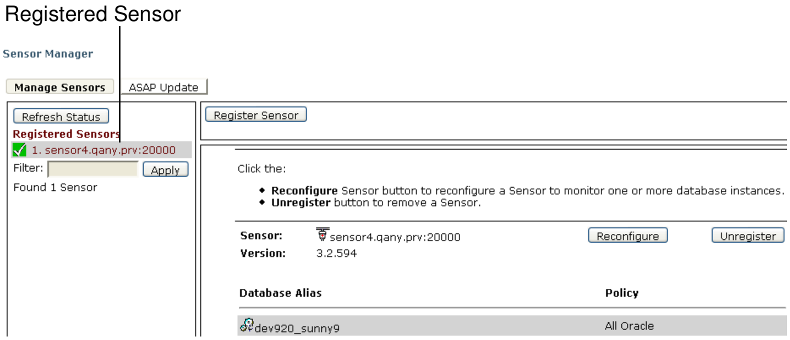
For more information, see *DbProtect audit and threat management limitations (based on Sensor type, activity, target database, and operating system).*

To configure a network-based Sensor to monitor a DB2 database server and deploy the configuration information (when Sensor is installed on Windows):

1. Do one of the following to display the first **Sensor Manager** page:

- Click the **Sensors - Manage Sensor** workflow link on the **Home** page.
- Click the **Sensors** tab from anywhere on the page.

The first **Sensor Manager** page displays your already-registered Sensors.



Click the:

- **Reconfigure** Sensor button to reconfigure a Sensor to monitor one or more database instances.
- **Unregister** button to remove a Sensor.

Sensor: sensor4.qany.prv:20000
Version: 3.2.594

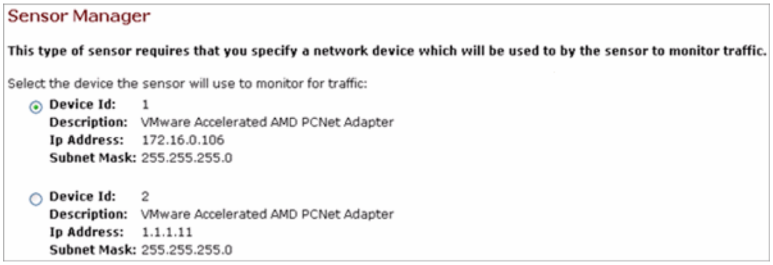
Database Alias	Policy
dev920_sunny9	All Oracle

FIGURE: Sensor Manager

If you have not registered *any* Sensors, then the first **Sensor Manager** page displays a message.

2. Click the **Configure** button (if you are configuring a Sensor for the first time), or the **Reconfigure** button (if you are reconfiguring a Sensor).

If you are configuring a new network-based Sensor, the next **Sensor Manager** page prompts you to specify a network device the Sensor will use to monitor traffic. If you have already configured the Sensor, go to Step 4.



Sensor Manager

This type of sensor requires that you specify a network device which will be used to by the sensor to monitor traffic.

Select the device the sensor will use to monitor for traffic:

◉ **Device Id:** 1
Description: VMware Accelerated AMD PCNet Adapter
Ip Address: 172.16.0.106
Subnet Mask: 255.255.255.0

○ **Device Id:** 2
Description: VMware Accelerated AMD PCNet Adapter
Ip Address: 1.1.1.11
Subnet Mask: 255.255.255.0

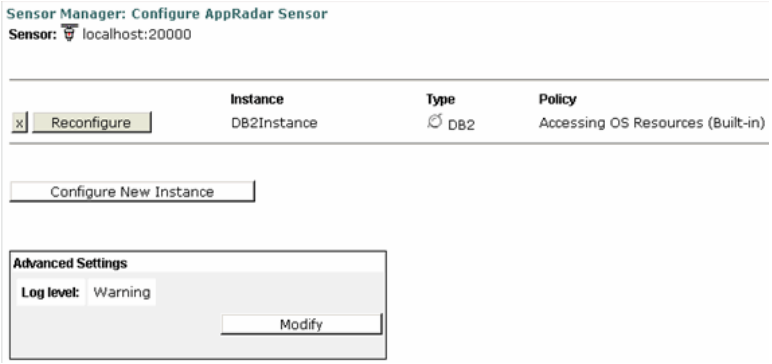
FIGURE: Sensor Manager

3. Select which network device the Sensor should use to monitor traffic. In addition to the **name** of the device, you should also know the **host IP address** each device is configured to use, and the **subnet mask** of the network device. For example:

   - Device ID: The number of the NIC (Network Interface Card) in the Sensor server. If the server only has one NIC, then the Device ID is `1`. If there are multiple NICs on the server machine, they are listed as `Device ID: 1`, `Device ID: 2`, etc.
   - **Description:** The make and model of the NIC, e.g., `3com 905B`
   - **Host IP Address:** The host IP address of the NIC, e.g., `192.168.1.5`
   - **Subnet Mask:** The address of your organization's subnet, e.g., `255.255.255.0`

4. The **Sensor Manager** page shows the:

- **Alias** of any host server you have configured for your Sensor
- database **Type** of the instance where your Sensor is registered
- database instance **(DB Instance)** where your Sensor is registered
- **Policy** associated with the registered Sensor.



Sensor Manager: Configure AppRadar Sensor

Sensor: localhost:20000

	Instance	Type	Policy
x Reconfigure	DB2Instance	DB2	Accessing OS Resources (Built-in)

Configure New Instance

Advanced Settings

Log level: Warning

Modify

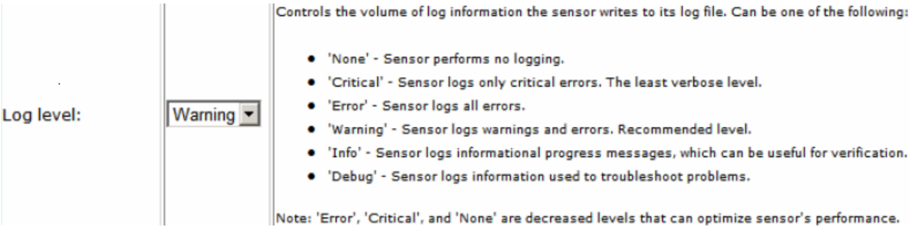
FIGURE: Sensor Manager

Note: The Console also displays whether the rules in your **Policy** are up-to-date or out-of-date. If a Policy is out-of-date, you can ASAP Update your Sensor with the latest security Rules (for more information, see *Performing an ASAP Update of Rules in your Sensors*), then use the **Policy Editor** to update Policies (deployed to your Sensors) with the new security Rules (for more information, see *Creating a Policy* and *Editing a Policy*).

5. You can click the:

- **Modify** button in the **Advanced Settings** portion of the page to display the **Advanced Sensor Settings** page, which allows you to select the Sensor's logging level (see Steps 6-7)
- **Configure New Instance** button to configure a new **DB2 database server** for the Sensor (see Steps 8-19)
- **Reconfigure** button to modify the current configuration of a **DB2 server** for the Sensor (see Steps 8-19)
- **X** button to delete a configured Sensor monitoring an instance; for more information, see *Deleting configured Sensors.*

6. The **Advanced Sensor Settings** page allows you to modify the Sensor's **logging level**.



Log level: Warning ▾

Controls the volume of log information the sensor writes to its log file. Can be one of the following:

- 'None' - Sensor performs no logging.
- 'Critical' - Sensor logs only critical errors. The least verbose level.
- 'Error' - Sensor logs all errors.
- 'Warning' - Sensor logs warnings and errors. Recommended level.
- 'Info' - Sensor logs informational progress messages, which can be useful for verification.
- 'Debug' - Sensor logs information used to troubleshoot problems.

Note: 'Error', 'Critical', and 'None' are decreased levels that can optimize sensor's performance.

FIGURE: **Advanced Sensor Settings** page

To modify the Sensor's logging level:

Use the **Log level:** drop-down to select the Sensor's logging level, which controls the volume of log information the Sensor outputs to its log file. You can select:

- **None.** Sensor performs no logging.
- **Critical.** Sensor logs only critical errors. The **least** verbose level.
- **Error.** Sensor logs **all** errors.
- **Warning.** Sensor logs warnings and errors. Recommended level.
- **Info.** Sensor logs informational progress messages, which can be useful for verification.
- **Debug.** Logs information used to troubleshoot Sensor problems at runtime.

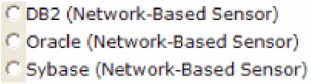
Note: **Error**, **Critical**, and **None** are all decreased logging levels which you can use to optimize Sensor performance.

7. When you're done, you can click the **Next** button to re-display the second **Sensor Manager** page (see Step 4), then click the:

- **Configure New Instance** button to configure a new **DB2 database server** for the Sensor (see Steps 8-19)
- **Reconfigure** button to modify the current configuration of a **DB2 database server** for the Sensor (see Steps 8-19).

8. Click the **Next** button.

The next **Sensor Manager** page displays, prompting you to select a database platform for the network-based Sensor to monitor.

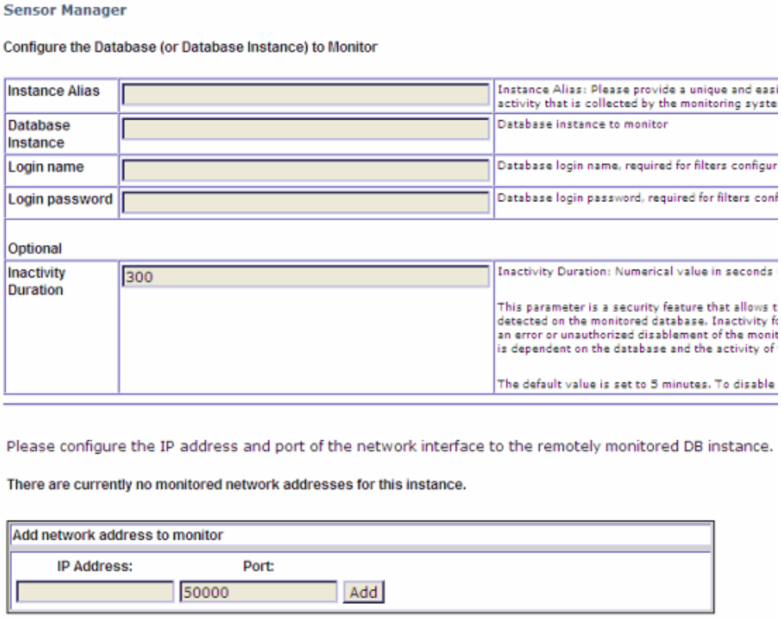


○ DB2 (Network-Based Sensor)
○ Oracle (Network-Based Sensor)
○ Sybase (Network-Based Sensor)

FIGURE: **Sensor Manager**

9. Select **DB2 (Network-Based Sensor)** and click the **Next** button.

The next **Sensor Manager** page displays.



Sensor Manager

Configure the Database (or Database Instance) to Monitor

Instance Alias		Instance Alias: Please provide a unique and easi activity that is collected by the monitoring syste
Database Instance		Database instance to monitor
Login name		Database login name, required for filters configur
Login password		Database login password, required for filters conf
Optional		
Inactivity Duration	300	Inactivity Duration: Numerical value in seconds This parameter is a security feature that allows t detected on the monitored database. Inactivity fo an error or unauthorized disablement of the monit is dependent on the database and the activity of The default value is set to 5 minutes. To disable

Please configure the IP address and port of the network interface to the remotely monitored DB instance.

There are currently no monitored network addresses for this instance.

Add network address to monitor

IP Address:	Port:	
	50000	Add

FIGURE: Sensor Manager

10. Do the following:

- Enter a meaningful instance alias (e.g., `DB2_EAGLE`) in the **Instance Alias** field, for the DB2 database server you want the Sensor to monitor (DbProtect Audit and Threat Management uses this alias to identify the databases from which Alerts are received).
- Enter the DB2 database server you want to monitor in the **Database instance** field.
- Enter your DB2 database server **Login Name** and **Login Password** if you plan to use Filters.

  When you are finished configuring DbProtect Audit and Threat Management and defining all Rules, you can re-configure your Sensors **without** a DB2 database server user name and password, and then re-deploy the Sensors.

Note: To enhance security, the user name/password pair that you enter is stored in encrypted form on the Sensor.

Optionally, in the **Optional** portion of the page, you can modify the value in the **Inactivity duration** field. The “inactivity duration” is the amount of time (in seconds) that must elapse with no activity on a DB2 database server before the Sensor generates an inactivity Alert. The default value is 5 minutes (`300` seconds). Valid values are `0` to `86400` seconds (i.e., 24 hours).

Note: Entering the value `0` (seconds) disables inactivity monitoring.

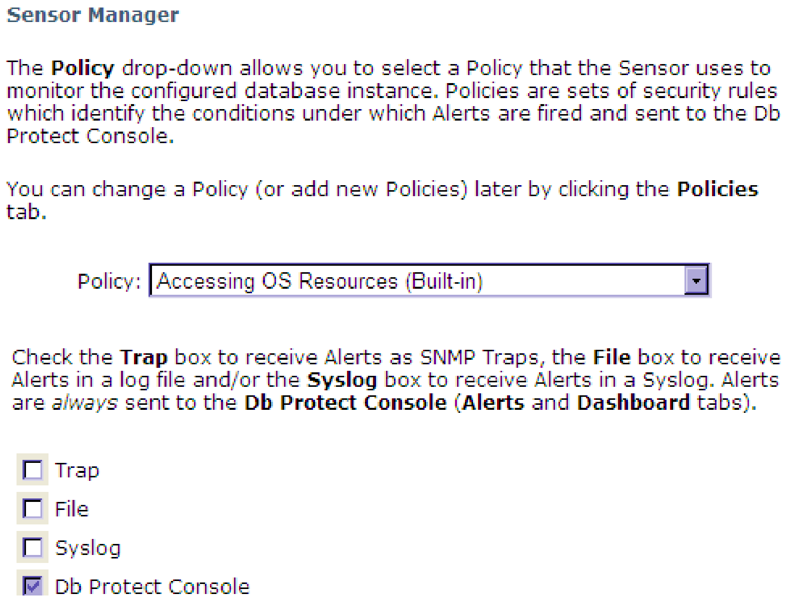
- Enter the **IP Address:** and **Port:** of the network interface to the remotely-monitored DB2 database server.
- Click the **Add** button.

A given host machine can accommodate (and, subsequently, a Sensor can monitor) multiple SIDs, servers, and services, including:

- **Sybase database servers**; for more information, see *Configuring a network-based Sensor to monitor a Sybase database server and deploying the configuration information (when Sensor is installed on Windows)*)
- **Oracle SIDS and services**; for more information, see *Configuring a network-based Sensor to monitor Oracle SIDs and services and deploying the configuration information (when Sensor is installed on Windows)*.

11. When you're done specifying the databases on the host machine that you want the Sensor to monitor, click the **Next** button.

The next **Sensor Manager** page displays.



Sensor Manager

The **Policy** drop-down allows you to select a Policy that the Sensor uses to monitor the configured database instance. Policies are sets of security rules which identify the conditions under which Alerts are fired and sent to the Db Protect Console.

You can change a Policy (or add new Policies) later by clicking the **Policies** tab.

Policy: Accessing OS Resources (Built-in)

Check the **Trap** box to receive Alerts as SNMP Traps, the **File** box to receive Alerts in a log file and/or the **Syslog** box to receive Alerts in a Syslog. Alerts are *always* sent to the **Db Protect Console** (**Alerts** and **Dashboard** tabs).

☐ Trap
☐ File
☐ Syslog
☑ Db Protect Console

FIGURE: Sensor Manager

12. Use the **Policy** drop-down to select a built-in or custom Policy the Sensor will use to monitor the configured database. Policies are sets of security Rules which identify the conditions under which Alerts are fired and sent to DbProtect Audit and Threat Management. Different Sensors and databases may require different Policies, since intrusion risk and data sensitivity will vary between database installations.

Note: You can change the Policy associated with a configured database instance (or deploy multiple additional Policies to a configured database instance) any time by clicking the **Policies** tab; for more information, see *Deploying a Policy*.

13. The grayed-out **DbProtect Console** checkbox indicates Alerts are **always** sent to the DbProtect Console.

You can monitor these Alerts in real-time via the **Alert Manager** and the **Dashboard**; for more information, see *Monitoring, filtering, acknowledging, and archiving Alerts (via the Alert Manager)* and *Monitoring Alerts (via the Dashboard)*, respectively. In addition, the **Report Manager** allows you to run **Detail Reports** and **Summary Reports** for Alerts. For more information, see *Reports*.

Optionally, on this page you can check the:

- **Trap** checkbox to receive Alerts also as SNMP traps
- **File** checkbox to receive Alerts also in a log file
- **Syslog** checkbox to receive Alerts as Syslog messages.

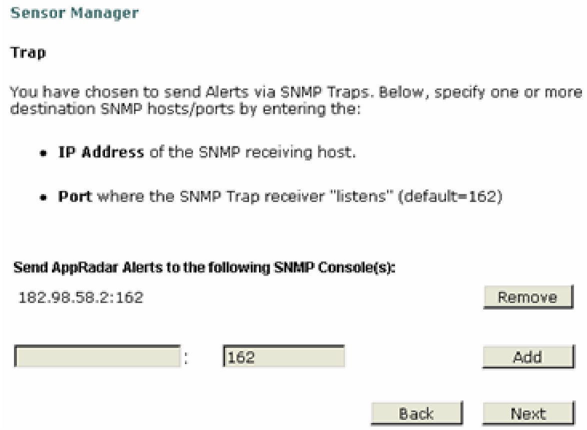
14. Click the **Next** button. If you checked the:

- **Trap** checkbox, then go to Step 15
- **File** checkbox, then go to Step 16
- **Syslog** checkbox, then go to Step 17.

Otherwise, go to Step 18.

15. Receiving Alerts as SNMP traps.

The **SNMP trap Configuration** page displays (if you clicked the **Trap** checkbox in Step 13).



Sensor Manager

Trap

You have chosen to send Alerts via SNMP Traps. Below, specify one or more destination SNMP hosts/ports by entering the:

- **IP Address** of the SNMP receiving host.
- **Port** where the SNMP Trap receiver "listens" (default=162)

Send AppRadar Alerts to the following SNMP Console(s):

182.98.58.2:162

: 162

FIGURE: Sensor Manager

Specify the SNMP server **IP Address** (**not** the host name) of the SNMP receiving host, and the **port** number where the SNMP trap receiver "listens".

Note: The default port is `162`, not `80`.

- Click the **Add** button.
- Click the **Next** button.

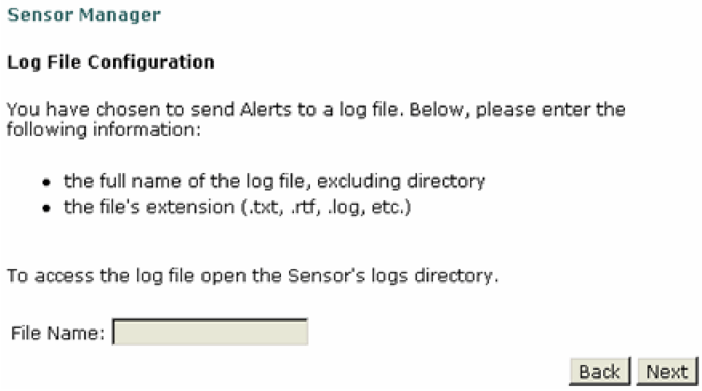
If you also checked the:

- **File** checkbox in Step 13, then go to Step 16
- **Syslog** checkbox in Step 13, then go to Step 17.

Otherwise, go to Step 18.

16.Receiving Alerts as Log Files.

The **Log File Configuration** page displays (if you clicked the **File** checkbox in Step 13).



Sensor Manager

Log File Configuration

You have chosen to send Alerts to a log file. Below, please enter the following information:

- the full name of the log file, excluding directory
- the file's extension (.txt, .rtf, .log, etc.)

To access the log file open the Sensor's logs directory.

File Name:

FIGURE: Sensor Manager

Do the following:

- Enter an Alert log file name in **File Name** field.

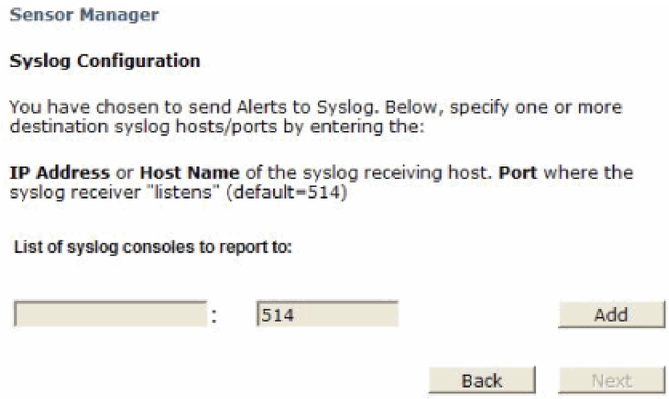
  Be sure to enter the full name of the log file (including the directory), and the log file's extension (e.g., `.txt`, `.rtf`, `.log`, etc.).

  The Alert log file is stored in the `Sensor_installation_directory\logs` directory, where `Sensor_installation_directory` is where the Sensor is installed.
- Click the **Next** button.

If you also checked the **Syslog** checkbox in Step 13, then go to Step 17. Otherwise, go to Step 18.

17. Receiving Alerts as Syslog messages.

The **Syslog File Configuration** page displays (if you clicked the **Syslog** checkbox in Step 13). For a sample Syslog message, see the *DbProtect Administrator's Guide*.



Sensor Manager

Syslog Configuration

You have chosen to send Alerts to Syslog. Below, specify one or more destination syslog hosts/ports by entering the:

IP Address or **Host Name** of the syslog receiving host. **Port** where the syslog receiver "listens" (default=514)

List of syslog consoles to report to:

: 514

FIGURE: Sensor Manager

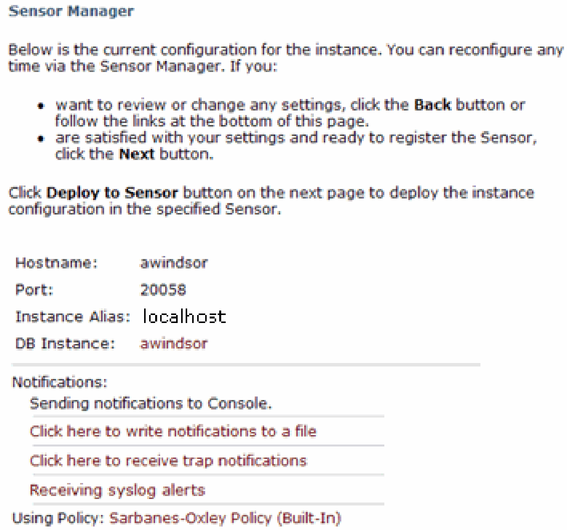
Specify the Syslog server IP Address (**not** the host name), and the port number of the target Syslog server where you want Alerts sent.

Note: The default port is `514` (not `80`).

Caution! The Syslog port is a User Datagram Protocol (UDP) port, as opposed to Transmission Control Protocol (TCP).

- Click the **Add** button.
- Click the **Next** button.

After you finish specifying the SNMP trap, and/or log file, and/or Syslog parameters (depending on which checkboxes, if any, you selected), then the **Sensor Manager** summary page displays.



Sensor Manager

Below is the current configuration for the instance. You can reconfigure any time via the Sensor Manager. If you:

- want to review or change any settings, click the **Back** button or follow the links at the bottom of this page.
- are satisfied with your settings and ready to register the Sensor, click the **Next** button.

Click **Deploy to Sensor** button on the next page to deploy the instance configuration in the specified Sensor.

Hostname:	awindsor
Port:	20058
Instance Alias:	localhost
DB Instance:	awindsor

Notifications:
Sending notifications to Console.
Click here to write notifications to a file
Click here to receive trap notifications
Receiving syslog alerts
Using Policy: Sarbanes-Oxley Policy (Built-In)

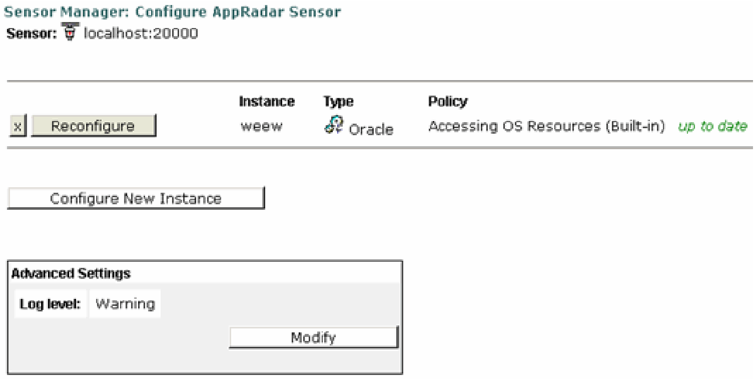
FIGURE: Sensor Manager

If you:

- want to review or change any settings you can click the **Back** button or any link that displays on the page
- are satisfied with your settings and ready to deploy the configuration to the Sensor, click the **Next** button.

Note: You can reconfigure the Sensor any time via the Sensor Manager.

18. The first **Sensor Manager** page re-displays.



Sensor Manager: Configure AppRadar Sensor

Sensor: localhost:20000

	Instance	Type	Policy
	weew	Oracle	Accessing OS Resources (Built-in) *up to date*

Advanced Settings

Log level: Warning

FIGURE: **Sensor Manager**

You can click the:

- **Reconfigure** button to reconfigure the Sensor before deploying the configuration to the specified Sensor
- **Cancel** button to cancel the configuration
- **Deploy to Sensor** button to deploy this configuration to the specified Sensor

Important: You **must** click the **Deploy to Sensor** button to make your modifications permanent.

- **Configure New Instance** button to configure a new database.

CONFIGURING A NETWORK-BASED SENSOR TO MONITOR ORACLE SIDS AND SERVICES AND DEPLOYING THE CONFIGURATION INFORMATION (WHEN SENSOR IS INSTALLED ON WINDOWS)

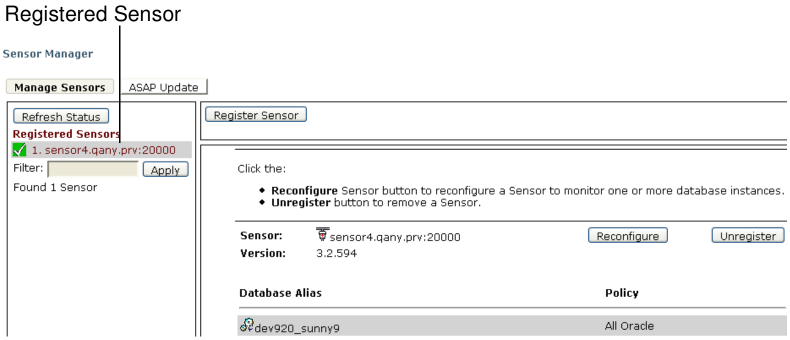
Note: DbProtect Audit and Threat Management may have limitations based on the type of Sensor, the nature of the activity, the target database, and the operating system. Network-based Sensors fire Alerts for all remote connections, e.g., from a web server communicating to its remote back-end database. However, they do **not** detect activity originating from the database host. For more information, see *DbProtect audit and threat management limitations (based on Sensor type, activity, target database, and operating system)*.

To configure a network-based Sensor to monitor Oracle SIDs and services and deploy the configuration information (when Sensor is installed on Windows):

1. Do one of the following to display the first **Sensor Manager** page:

- Click the **Sensors - Manage Sensor** workflow link on the **Home** page.
- Click the **Sensors** tab from anywhere on the page.

The first **Sensor Manager** page displays your already-registered Sensors.



Registered Sensor

Registered Sensors

✓ 1. sensor4.qany.prv:20000

Filter:

Found 1 Sensor

Click the:

- **Reconfigure** Sensor button to reconfigure a Sensor to monitor one or more database instances.
- **Unregister** button to remove a Sensor.

Sensor: sensor4.qany.prv:20000

Version: 3.2.594

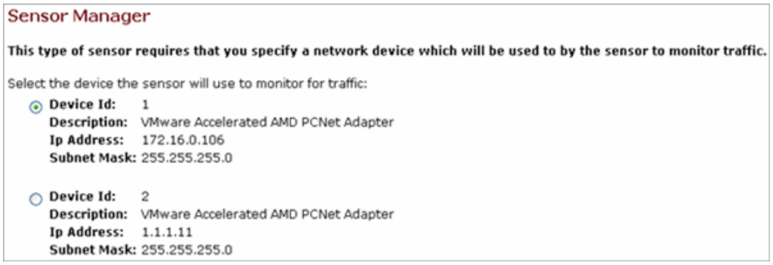
Database Alias	Policy
dev920_sunny9	All Oracle

FIGURE: Sensor Manager

If you have not registered *any* Sensors, then the first **Sensor Manager** page displays a message.

2. Click the **Configure** button (if you are configuring a Sensor for the first time), or the **Reconfigure** button (if you are reconfiguring a Sensor).

If you are configuring a new network-based Sensor, the next **Sensor Manager** page prompts you to specify a network device the Sensor will use to monitor traffic. If you have already configured the Sensor, go to Step 4.



Sensor Manager

This type of sensor requires that you specify a network device which will be used to by the sensor to monitor traffic.

Select the device the sensor will use to monitor for traffic:

● **Device Id:** 1
Description: VMware Accelerated AMD PCNet Adapter
Ip Address: 172.16.0.106
Subnet Mask: 255.255.255.0

○ **Device Id:** 2
Description: VMware Accelerated AMD PCNet Adapter
Ip Address: 1.1.1.11
Subnet Mask: 255.255.255.0

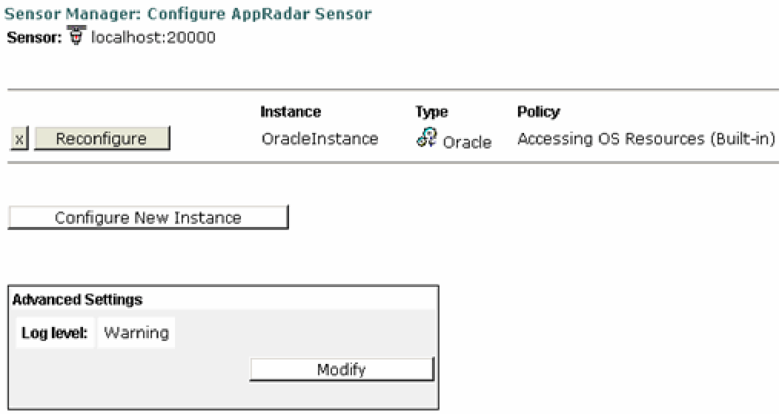
FIGURE: Sensor Manager

3. Select which network device the Sensor should use to monitor traffic. In addition to the **name** of the device, you should also know the **host IP address** each device is configured to use, and the **subnet mask** of the network device. For example:

   - **Device ID:** The number of the NIC (Network Interface Card) in the Sensor server. If the server only has one NIC, then the Device ID is `1`. If there are multiple NICs on the server machine, they are listed as `Device ID: 1`, `Device ID: 2`, etc.
   - **Description:** The make and model of the NIC, e.g., `3com 905B`
   - **Host IP Address:** The host IP address of the NIC, e.g., `192.168.1.5`
   - **Subnet Mask:** The address of your organization's subnet, e.g., `255.255.255.0`.

4. The **Sensor Manager** page shows the:

- **Alias** of any host server you have configured for your Sensor
- database **Type** of the instance where your Sensor is registered
- database instance **(DB Instance)** where your Sensor is registered
- **Policy** associated with the registered Sensor.



Sensor Manager: Configure AppRadar Sensor

Sensor: localhost:20000

	Instance	Type	Policy
x Reconfigure	OracleInstance	Oracle	Accessing OS Resources (Built-in)

Advanced Settings

Log level: Warning

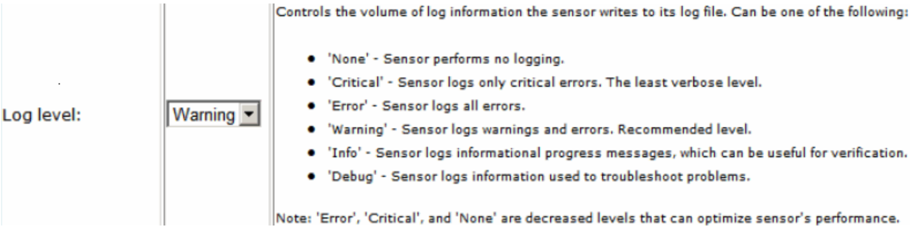
FIGURE: Sensor Manager

Note: The Console also displays whether the rules in your **Policy** are up-to-date or out-of-date. If a Policy is out-of-date, you can ASAP Update your Sensor with the latest security Rules (for more information, see *Performing an ASAP Update of Rules in your Sensors*), then use the **Policy Editor** to update Policies (deployed to your Sensors) with the new security Rules (for more information, see *Creating a Policy* and *Editing a Policy*).

5. You can click the:

- **Modify** button in the **Advanced Settings** portion of the page to display the **Advanced Sensor Settings** page, which allows you to select the Sensor's logging level (see Steps 6-7)
- **Configure New Instance** button to configure a new **Oracle SID or service** for the Sensor (see Steps 8-19)
- **Reconfigure** button to modify the current configuration of an **Oracle SID or service** for the Sensor (see Steps 8-19)
- **X** button to delete a configured Sensor monitoring an instance; for more information, see *Deleting configured Sensors*.

6. The **Advanced Sensor Settings** page allows you to modify the Sensor's **logging level**.



Log level: Warning ▾

Controls the volume of log information the sensor writes to its log file. Can be one of the following:

- 'None' - Sensor performs no logging.
- 'Critical' - Sensor logs only critical errors. The least verbose level.
- 'Error' - Sensor logs all errors.
- 'Warning' - Sensor logs warnings and errors. Recommended level.
- 'Info' - Sensor logs informational progress messages, which can be useful for verification.
- 'Debug' - Sensor logs information used to troubleshoot problems.

Note: 'Error', 'Critical', and 'None' are decreased levels that can optimize sensor's performance.

FIGURE: **Advanced Sensor Settings** page

To modify the Sensor's logging level:

Use the **Log level:** drop-down to select the Sensor's logging level, which controls the volume of log information the Sensor outputs to its log file. You can select:

- **None.** Sensor performs no logging.
- **Critical.** Sensor logs only critical errors. The **least** verbose level.
- **Error.** Sensor logs **all** errors.
- **Warning.** Sensor logs warnings and errors. Recommended level.
- **Info.** Sensor logs informational progress messages, which can be useful for verification.
- **Debug.** Logs information used to troubleshoot Sensor problems at runtime.

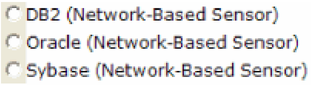
Note: **Error**, **Critical**, and **None** are all decreased logging levels which you can use to optimize Sensor performance.

7. When you're done, you can click the **Next** button to re-display the second **Sensor Manager** page (see Step 4), then click the:

- **Configure New Instance** button to configure a new **Oracle SID or service** for the Sensor (see Steps 8-19)
- **Reconfigure** button to modify the current configuration of an **Oracle SID or service** for the Sensor (see Steps 8-19).

8. Click the **Next** button.

The next **Sensor Manager** page displays, prompting you to select a database platform for the network-based Sensor to monitor.

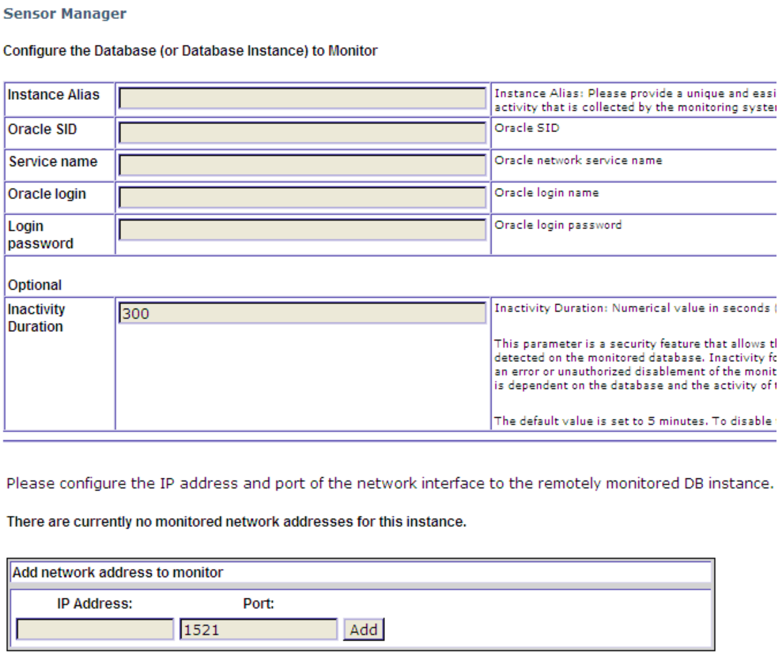


○ DB2 (Network-Based Sensor)
○ Oracle (Network-Based Sensor)
○ Sybase (Network-Based Sensor)

FIGURE: **Sensor Manager**

9. Select **Oracle (Network-Based Sensor)** and click the **Next** button.

The next **Sensor Manager** page displays.



Sensor Manager

Configure the Database (or Database Instance) to Monitor

Instance Alias		Instance Alias: Please provide a unique and easi activity that is collected by the monitoring syste
Oracle SID		Oracle SID
Service name		Oracle network service name
Oracle login		Oracle login name
Login password		Oracle login password
Optional		
Inactivity Duration	300	Inactivity Duration: Numerical value in seconds This parameter is a security feature that allows t detected on the monitored database. Inactivity f an error or unauthorized disablement of the monit is dependent on the database and the activity of The default value is set to 5 minutes. To disable

Please configure the IP address and port of the network interface to the remotely monitored DB instance.

There are currently no monitored network addresses for this instance.

Add network address to monitor

IP Address:	Port:	
	1521	Add

FIGURE: Sensor Manager

10. Do the following:

- Enter a meaningful instance alias (e.g., `ORCL_EAGLE`) in the **Instance Alias** field, for the Oracle SID or service you want the Sensor to monitor (DbProtect Audit and Threat Management uses this alias to identify the databases from which Alerts are received).
- Enter the name of the **Oracle SID** and **Service Name** (128 alphanumeric characters maximum, including spaces) for the Oracle SID or service you want to monitor. See your database administrator if you are unsure of these values.

Note: The Oracle TNS Listener is the server-based process that provides basic network connectivity for clients, application servers, and other databases to an Oracle database. A Listener can provide network connectivity to one or many SIDs and services.

- Enter the **Oracle login** and **Login password** for your Oracle SID or service -- if you plan to use Filters.

  When you are finished configuring DbProtect Audit and Threat Management and defining all Rules, you can re-configure your Sensors **without** an Oracle SID or service user name and password, and then re-deploy the Sensors.

Note: To enhance security, the user name/password pair that you enter is stored in encrypted form on the Sensor.

Important: If you are using network-based Sensors for Oracle on Windows for Audit and Threat Management, and you want to use Filters, then you **must** enter an Oracle user name and password in this step. The user name/password pair is **not** used to monitor your database. The pair is only used by the Audit Filter Wizard to collect object information from the database. For more information, see *Working with the Audit Filter Wizard*.

- Optionally, in the **Optional** portion of the page, you can modify the value in the **Inactivity duration** field. The "inactivity duration" is the amount of time (in seconds) that must elapse with no activity on the Oracle SID or service before the Sensor generates an inactivity Alert. The default value is 5 minutes (`300` seconds). Valid values are `0` to `86400` seconds (i.e., 24 hours).

Note: Entering the value `0` (seconds) disables inactivity monitoring.

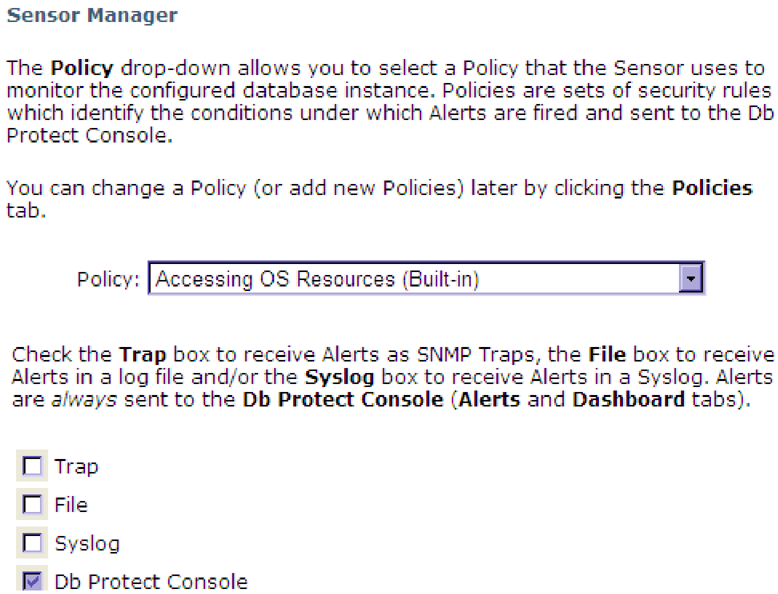
- Enter the **IP Address:** and **Port:** of the network interface to the remotely-monitored Oracle SID or service.
- Click the **Add** button.

A given host machine can accommodate (and, subsequently, a Sensor can monitor) multiple SIDs, servers, and services, including:

- **Sybase database servers**; for more information, see *Configuring a network-based Sensor to monitor a Sybase database server and deploying the configuration information (when Sensor is installed on Windows)*)
- **DB2 database servers**; for more information, see *Configuring a network-based Sensor to monitor a DB2 database server and deploying the configuration information (when Sensor is installed on Windows)*.

11. When you're done specifying the databases on the host machine that you want the Sensor to monitor, click the **Next** button.

The next **Sensor Manager** page displays.



Sensor Manager

The **Policy** drop-down allows you to select a Policy that the Sensor uses to monitor the configured database instance. Policies are sets of security rules which identify the conditions under which Alerts are fired and sent to the Db Protect Console.

You can change a Policy (or add new Policies) later by clicking the **Policies** tab.

Policy: Accessing OS Resources (Built-in)

Check the **Trap** box to receive Alerts as SNMP Traps, the **File** box to receive Alerts in a log file and/or the **Syslog** box to receive Alerts in a Syslog. Alerts are *always* sent to the **Db Protect Console** (**Alerts** and **Dashboard** tabs).

☐ Trap
☐ File
☐ Syslog
☑ Db Protect Console

FIGURE: Sensor Manager

12. Use the **Policy** drop-down to select a built-in or custom Policy that the Sensor will use to monitor the configured database. Policies are sets of security Rules which identify the conditions under which Alerts are fired and sent to DbProtect Audit and Threat Management. Different Sensors and databases may require different Policies, since intrusion risk and data sensitivity will vary between database installations.

Note: You can change the Policy associated with a configured database instance (or deploy multiple additional Policies to a configured database instance) any time by clicking the **Policies** tab; for more information, see *Deploying a Policy*.

13. The grayed-out **DbProtect Console** checkbox indicates Alerts are **always** sent to the DbProtect Console.

You can monitor these Alerts in real-time via the **Alert Manager** and the **Dashboard**; for more information, see *Monitoring, filtering, acknowledging, and archiving Alerts (via the Alert Manager)* and *Monitoring Alerts (via the Dashboard)*, respectively. In addition, the **Report Manager** allows you to run **Detail Reports** and **Summary Reports** for Alerts. For more information, see *Reports*.

Optionally, on this page you can check the:

- **Trap** checkbox to receive Alerts also as SNMP traps
- **File** checkbox to receive Alerts also in a log file
- **Syslog** checkbox to receive Alerts as Syslog messages.

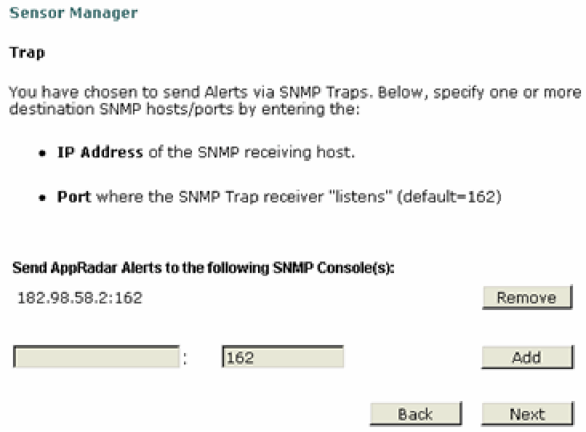
14. Click the **Next** button. If you checked the:

- **Trap** checkbox, then go to Step 15
- **File** checkbox, then go to Step 16
- **Syslog** checkbox, then go to Step 17.

Otherwise, go to Step 18.

15.Receiving Alerts as SNMP traps.

The **SNMP trap Configuration** page displays (if you clicked the **Trap** checkbox in Step 13).



Sensor Manager

Trap

You have chosen to send Alerts via SNMP Traps. Below, specify one or more destination SNMP hosts/ports by entering the:

- **IP Address** of the SNMP receiving host.
- **Port** where the SNMP Trap receiver "listens" (default=162)

Send AppRadar Alerts to the following SNMP Console(s):

182.98.58.2:162

: 162

FIGURE: Sensor Manager

Specify the SNMP server **IP Address** (**not** the host name) of the SNMP receiving host, and the **port** number where the SNMP trap receiver "listens".

Note: The default port is `162`, not `80`.

- Click the **Add** button.
- Click the **Next** button.

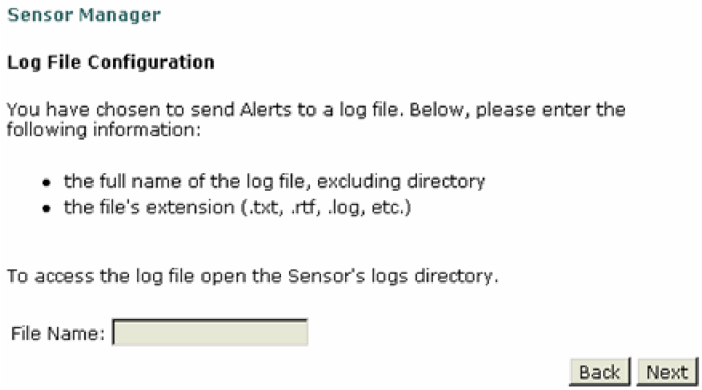
If you also checked the:

- **File** checkbox in Step 13, then go to Step 16
- **Syslog** checkbox in Step 13, then go to Step 17.

Otherwise, go to Step 18.

16.Receiving Alerts as Log Files.

The **Log File Configuration** page displays (if you clicked the **File** checkbox in Step 13).



Sensor Manager

Log File Configuration

You have chosen to send Alerts to a log file. Below, please enter the following information:

- the full name of the log file, excluding directory
- the file's extension (.txt, .rtf, .log, etc.)

To access the log file open the Sensor's logs directory.

File Name:

FIGURE: Sensor Manager

Do the following:

- Enter an Alert log file name in **File Name** field.

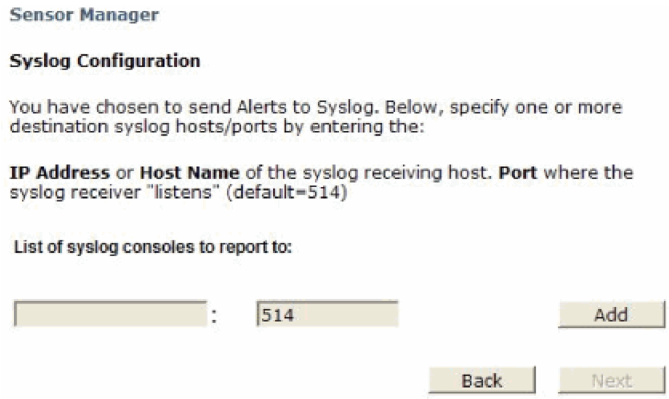
  Be sure to enter the full name of the log file (including the directory), and the log file's extension (e.g., `.txt`, `.rtf`, `.log`, etc.).

  The Alert log file is stored in the `Sensor_installation_directory\logs` directory, where `Sensor_installation_directory` is where the Sensor is installed.
- Click the **Next** button.

If you also checked the **Syslog** checkbox in Step 13, then go to Step 17. Otherwise, go to Step 18.

17. Receiving Alerts as Syslog messages.

The **Syslog File Configuration** page displays (if you clicked the **Syslog** checkbox in Step 13). For a sample Syslog message, see the *DbProtect Administrator's Guide*.



Sensor Manager

Syslog Configuration

You have chosen to send Alerts to Syslog. Below, specify one or more destination syslog hosts/ports by entering the:

IP Address or **Host Name** of the syslog receiving host. **Port** where the syslog receiver "listens" (default=514)

List of syslog consoles to report to:

: 514

FIGURE: Sensor Manager

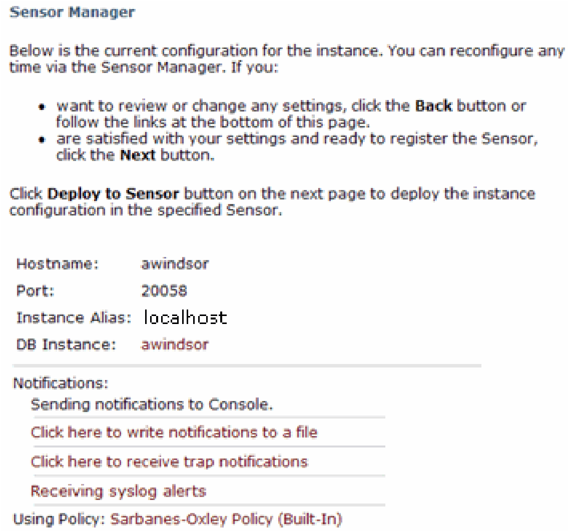
Specify the Syslog server IP Address (**not** the host name), and the port number of the target Syslog server where you want Alerts sent.

Note: The default port is `514` (not `80`).

Caution! The Syslog port is a User Datagram Protocol (UDP) port, as opposed to Transmission Control Protocol (TCP).

- Click the **Add** button.
- Click the **Next** button.

18. After you finish specifying the SNMP trap, and/or log file, and/or Syslog parameters (depending on which checkboxes, if any, you selected), then the **Sensor Manager** summary page displays.



Sensor Manager

Below is the current configuration for the instance. You can reconfigure any time via the Sensor Manager. If you:

- want to review or change any settings, click the **Back** button or follow the links at the bottom of this page.
- are satisfied with your settings and ready to register the Sensor, click the **Next** button.

Click **Deploy to Sensor** button on the next page to deploy the instance configuration in the specified Sensor.

Hostname:	awindsor
Port:	20058
Instance Alias:	localhost
DB Instance:	awindsor

Notifications:

Sending notifications to Console.

Click here to write notifications to a file

Click here to receive trap notifications

Receiving syslog alerts

Using Policy: Sarbanes-Oxley Policy (Built-In)

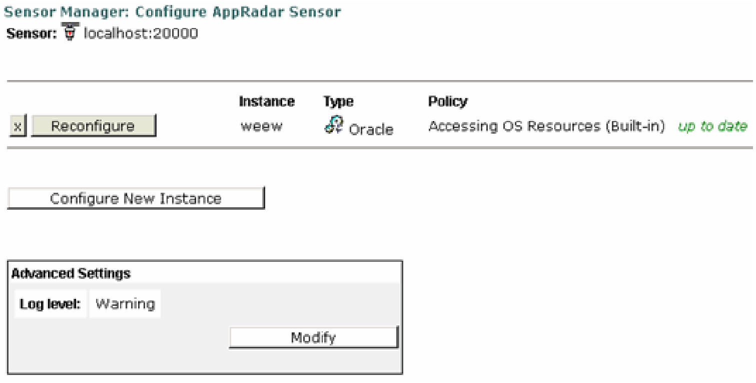
FIGURE: Sensor Manager

If you:

- want to review or change any settings you can click the **Back** button or any link that displays on the page
- are satisfied with your settings and ready to deploy the configuration to the Sensor, click the **Next** button.

Note: You can reconfigure the Sensor any time via the Sensor Manager.

19. The first **Sensor Manager** page re-displays.



Sensor Manager: Configure AppRadar Sensor

Sensor: localhost:20000

	Instance	Type	Policy
x Reconfigure	weew	Oracle	Accessing OS Resources (Built-in) *up to date*

Advanced Settings

Log level: Warning

FIGURE: Sensor Manager

You can click the:

- **Reconfigure** button to reconfigure the Sensor before deploying the configuration to the specified Sensor
- **Cancel** button to cancel the configuration
- **Deploy to Sensor** button to deploy this configuration to the specified Sensor

Important: You **must** click the **Deploy to Sensor** button to make your modifications permanent.

- **Configure New Instance** button to configure a new database.

Deleting configured Sensors

You can **delete** Sensors configured for:

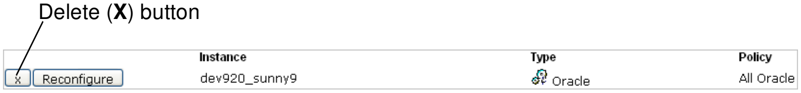
- SQL Server instances (host-based only)
- Oracle SIDs or services (host-based or network-based)
- DB2 database servers (host-based or network-based)
- Sybase database servers (network-based only).

To delete a configured host- or network-based Sensor:

1. Display the **Sensor Manager** to view your configured Sensors, and determine which one you want to delete.

2. From the **Sensor Manager** page, click the **X** button next to the configured Sensor you want to delete.

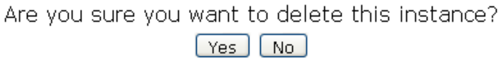
Delete (**X**) button



	Instance	Type	Policy
X Reconfigure	dev920_sunny9	Oracle	All Oracle

FIGURE: Sensor Manager

A confirmation page prompts you to confirm that you are *sure* you want to delete the configured Sensor.



Are you sure you want to delete this instance?

FIGURE: Confirm delete page

3. If you are *sure* you want to delete the configured Sensor, click the **Yes** button.

Your configured Sensor is deleted.

Performing an ASAP Update of Rules in your Sensors

Prior to the release of Console Management Server version 4.1 and Sensor version 3.9 (both released as part of DbProtect 2009.1R4), if you wanted to update a Sensor with the latest security Rules, you had to manually upgrade both your Console and your Sensor.

However, starting with Console Management Server version 4.1, the **Sensor Manager** page allows you to perform an ASAP Update of security Rules in your host- or network-based Sensors, as long as:

- the **Console Management Server** is at least **version 4.1**
- the **Sensor** is at least **version 3.9**

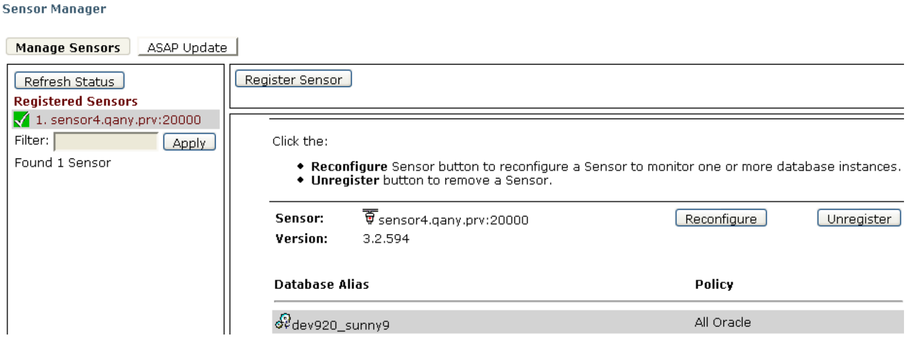
Note: For more information on DbProtect component versioning, see the *DbProtect Version Compatibility Matrix, and Determining the Current Version of Installed DbProtect Applications* in the *DbProtect Installation Guide* or the *DbProtect Administrator's Guide.*

- the **Sensor** is **registered** (for more information, see *Registering a Sensor*)
- the Sensor does **not** already contain the latest available security Rules from the Application Security, Inc. security Rules **knowledgebase**.

After you ASAP Update your Sensor with the latest available security Rules, you can use the **Policy Editor** to update Policies (deployed to your Sensors) with the new security Rules; for more information, see *Policies*.

To perform an ASAP Update of your ASAP Updateable Sensors with the latest available security Rules:

1. Do one of the following to display the first **Sensor Manager** page:
   - Click the **Sensors - Manage Sensor** workflow link on the **Home** page.
   - Click the **Sensors** tab from anywhere on the page.



Sensor Manager

Registered Sensors

✓ 1. sensor4.qany.prv:20000

Filter:

Found 1 Sensor

Click the:

- **Reconfigure** Sensor button to reconfigure a Sensor to monitor one or more database instances.
- **Unregister** button to remove a Sensor.

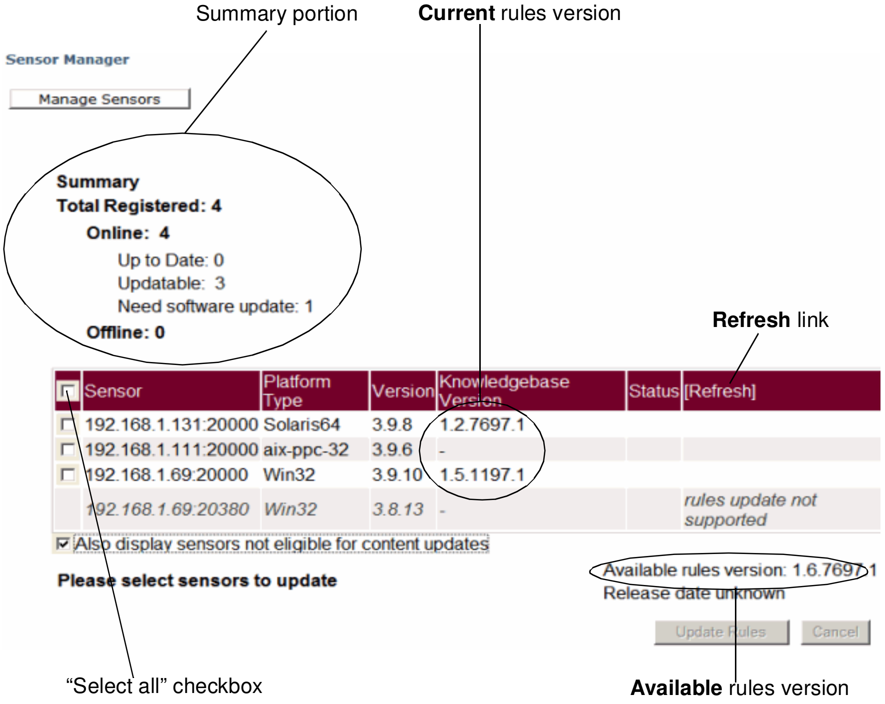
Sensor: sensor4.qany.prv:20000

Version: 3.2.594

Database Alias	Policy
dev920_sunny9	All Oracle

FIGURE: Sensor Manager

2. Click the **ASAP Update** button to display the security Rule ASAP Update page of the **Sensor Manager**.



Summary
Total Registered: 4
Online: 4
Up to Date: 0
Updatable: 3
Need software update: 1
Offline: 0

☐	Sensor	Platform Type	Version	Knowledgebase Version	Status	[Refresh]
☐	192.168.1.131:20000	Solaris64	3.9.8	1.2.7697.1		
☐	192.168.1.111:20000	aix-ppc-32	3.9.6	-		
☐	192.168.1.69:20000	Win32	3.9.10	1.5.1197.1		
	192.168.1.69:20380	*Win32*	*3.8.13*	-		*rules update not supported*

☑ Also display sensors not eligible for content updates

Please select sensors to update

Available rules version: 1.6.7697.1
Release date unknown

FIGURE: **Sensor Manager** (security Rule ASAP Update page)

The **summary portion** of the page displays information about your registered Sensors. Specifically, this portion of the page lists the number of:

- **Total Registered:** Sensors -- both ASAP Updateable and non-ASAP Updateable; for more information, see *Registering a Sensor*
- **Online:** registered Sensors, including how many Sensors:

  -are **Up to Date:** with the latest available security Rules

  -are **Updateable:** (i.e., you should ASAP Update these Sensors with the latest security Rules, following the steps described in this topic)

  -**Need software update:** (i.e., you need to upgrade your Sensor to at least version 3.9 in order to ASAP Update them; for more information on upgrading your Sensors, see the *DbProtect Administrator's Guide*)
- registered Sensors that are currently **Offline:**

The **lower portion** of the **Sensor Manager's** security Rule ASAP Update page displays **security Rule ASAP Update** information about your registered Sensors. Specifically, this portion of the page consists of the following columns:

- **Sensor.** The name of each registered **Sensor** that is ASAP Updateable with the latest available security Rules. You should ASAP Update these Sensors with the latest security Rules, following the steps described in this topic.

Hint: You can check the **Also display Sensors not eligible for content updates** checkbox if you want to display Sensors that are non-ASAP Updateable, because: a.) they already contain up-to-date security Rules, or b.) they are too old (pre-version 3.9). Non-ASAP Updateable Sensors display in *italics*, are grayed-out, and do **not** contain checkboxes (i.e., you cannot select these Sensors for an ASAP Update).

- **Platform Type.** The operating system **platform** the Sensor (that is ASAP Updateable with the latest available security Rules) is installed on (e.g., **Win32**).
- **Version.** The **version** of the registered Sensor that is ASAP Updateable with the latest available security Rules; for more information on DbProtect component versions, see *DbProtect Version Compatibility Matrix, and Determining the Current Version of Installed DbProtect Applications* in the *DbProtect Administrator's Guide* or the *DbProtect Installation Guide*.

Note: Again, Sensors older than version 3.9 do **not** allow you to perform an ASAP Update of the latest available security Rules. Application Security Inc. recommends you upgrade your Sensors to at least version 3.9 in order to take advantage of this important functionality. For more information on upgrading your Sensors, see the *DbProtect Administrator's Guide*.

- **Knowledgebase Version**. The version of Application Security, Inc.'s security Rules **knowledgebase** used by the registered Sensor. You should compare this version number to the **Available rules version** number (in the lower-right portion of the page) to determine whether your Sensor (assuming it's version 3.9 or greater) can and should be ASAP Updated with the latest available security Rules.

Note: If the **Knowledgebase Version** column displays a dash (-), this means the corresponding registered Sensor contains security Rules that are so outdated they aren't even versioned. In this case, Application Security, Inc. **strongly** recommends you ASAP Update the Sensor (assuming it's ASAP Updateable, i.e., your registered Sensor is at least version 3.9).

- **Status.** The real-time ASAP Update **status** of your registered Sensor (that is ASAP Updateable with the latest available security Rules).
- **Refresh.** The current state of the Sensor, e.g., **Online**, **Offline**, etc. You can click the **Refresh** link to refresh the current state of the Sensor.

Note: If a Sensor is up-to-date with the latest security Rules (i.e., if you check the **Also display Sensors not eligible for content updates** checkbox), then the **Refresh** column reads: *latest known rules version.*

- **Knowledgebase Version**. The version of Application Security, Inc.'s security Rules **knowledgebase** containing security Rules.

3. Check one or more Sensors that contain ASAP Updateable security Rules.

Hint: You can check the "select all" checkbox in the upper-left corner of the lower portion of the page to select all Sensors that are ASAP Updateable with the latest available security Rules.

4. Click the **Update Rules** button. DbProtect Audit and Threat Management updates all ASAP Updateable Sensors (selected in Step 3) with the latest available security Rules. The **Status** column provides a real-time ASAP Update status.

Note: You can click the **Cancel** button to cancel the ASAP Update of a Sensor. If the **Status** column indicates an ASAP Update is **Pending**, the ASAP Update is cancelled completely. However, if the **Status** column indicates an ASAP Update is **In Progress**, DbProtect completes its update of the Sensor that is being ASAP Updated, and then cancels the ASAP Update of all queued Sensors.

Hint: If you ASAP Update **some** -- but not **all** -- of your ASAP Updateable Sensors with the latest available security Rules, you **must** click the **Reset** button before you select and ASAP Update additional Sensors.

Important: Once you have ASAP Updated a Sensor with the latest available security Rules, you may have to re-configure your Sensor, and re-deploy the configuration information to the Sensor, in order for the new security Rules to take effect on the database instances you are monitoring; for more information, see *Configuring a Sensor and deploying the configuration information*.

5. Click the **Manage Sensors** button to return to the main **Sensor Manager** page *any time* (in other words, you do not have to wait until the ASAP Update of your security Rules is completed). However, your ASAP Updateable Sensor(s) **may** appear offline until the ASAP Update is completed.

Monitoring the "health" of your Sensors (via the Sensor Manager)

You can monitor the "health" of your registered Sensors via the **Sensor Manager** and the **Dashboard**. If you're not receiving Alerts, it **could** be because your registered Sensor is "unhealthy". A "healthy" Sensor is:

- **"up and running"** on the database SID or instance where it is registered
- **actively collecting/interpreting data and firing Alerts** to DbProtect Audit and Threat Management in accordance with its deployed Policies.

Hint: If you have trouble establishing a connection between the Console and a Sensor installed on Microsoft Windows 2008 (i.e., a host-based Sensor for Oracle on Windows, a host-based Sensor for DB2 on Windows, a host-based Sensor for Microsoft SQL Server on Windows, or any network-based Sensor), make sure IPV6 support is **not** enabled on the network adapter, and that your Microsoft Windows Firewall is disabled.

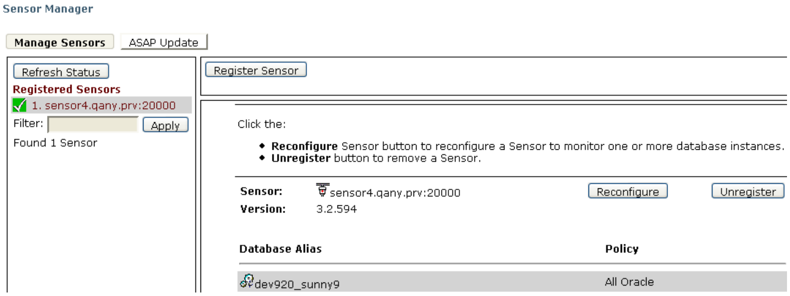
For more information, see the *DbProtect Administrator's Guide*.

To monitor the "health" of your Sensors via the **Sensor Manager**:

1. Do one of the following to display the first **Sensor Manager** page:

- Click the **Sensors - Manage Sensor** workflow link on the **Home** page.
- Click the **Sensors** tab from anywhere on the page.

The first **Sensor Manager** page displays your registered Sensors.



✓ 1. sensor4.qany.prv:20000

Filter: Apply

Found 1 Sensor

Click the:

- **Reconfigure** Sensor button to reconfigure a Sensor to monitor one or more database instances.
- **Unregister** button to remove a Sensor.

Sensor: sensor4.qany.prv:20000

Version: 3.2.594

Database Alias	Policy
dev920_sunny9	All Oracle

FIGURE: Sensor Manager

If the color-coded icon next to your registered Sensor is:

- **green**, then the Sensor is "healthy"
- **red**, then the Sensor is "unhealthy"; for more information, see the *Monitoring the Health of Your Sensors* of the *DbProtect Administrator's Guide*.

Hint: Click the **Refresh Status** button to view the most current state of your Sensors' "health".

Unregistering a Sensor

When you **unregister a Sensor**, the Sensor stops sending messages and Alerts. Unregistration returns the Sensor to its original, unconfigured installation state -- but it is not removed. (For more information on removing Sensors, see *Manually removing a Sensor*.)

Important: For information on installing and uninstalling Sensors, including Sensors in a SQL Server cluster, see the *DbProtect Installation Guide*.

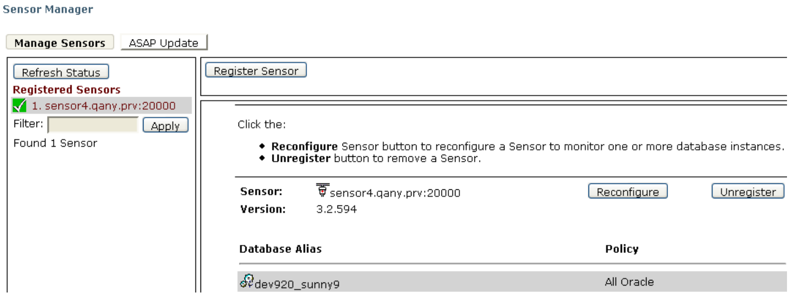
Note: An unregistered Sensor continues to log events to a notification file (`appradar_app.txt` located in the Sensor's log directory), but **only** whether the Sensor is "up" or "down".

To unregister a Sensor:

1. Do one of the following to display the first **Sensor Manager** page:

- Click the **Manage Sensors** workflow link on the **Home** page.
- Click the **Sensors** tab from anywhere on the page.

The first **Sensor Manager** page displays your registered Sensors.



Click the:

- **Reconfigure** Sensor button to reconfigure a Sensor to monitor one or more database instances.
- **Unregister** button to remove a Sensor.

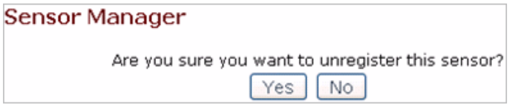
Sensor: sensor4.qany.prv:20000
Version: 3.2.594

Database Alias	Policy
dev920_sunny9	All Oracle

FIGURE: Sensor Manager

2. Highlight a registered Sensor, and click the **Unregister** button.

A page displays, prompting you to confirm the unregistration.



Are you sure you want to unregister this sensor?

FIGURE: Unregistration confirmation

3. Click the **Yes** button.

DbProtect Audit and Threat Management unregisters your Sensor.

If unregistration is unsuccessful, DbProtect Audit and Threat Management prompts you to let it attempt a forced unregistration. If the forced unregistration of the Sensor fails, you may have to remove the Sensor manually; for more information, see *Manually removing a Sensor*.

Manually removing a Sensor

You can manually remove a Sensor in the rare event a Sensor does not respond to an unregistration request; for more information, see *Unregistering a Sensor*.

Important: For information on installing and uninstalling Sensors, including Sensors in a SQL Server cluster, see the *DbProtect Installation Guide*.

To manually remove a Sensor:

1. Run the `force_unregister.bat` for Windows-based Sensors, or `force_unregister` on Sensors on Unix and Linux platforms, on the Sensor's host computer.

   Default locations:

   - for Windows-based Sensors, `force_unregister.bat` is located by default in `<Sensor Install Directory>\AppSecInc\Sensor\utils`
   - for Unix- and Linux-based Sensors, `force_unregister` is located by default in `<Sensor Install Directory>/ASIappradar/sensor/util`

Your Sensor is unregistered.

Note: You can register the Sensor again, if necessary; for more information, see *Registering a Sensor*.

Alerts

This chapter consists of the following topics:

- *What is an Alert?*
- *Monitoring Alerts via the DbProtect Audit and Threat Management UI*
- *Monitoring Alerts as SNMP traps, the log file, or Syslog*
- *Acknowledging and archiving Alerts*
- *"Password Guessing" and "Password Scripted Attack" Alerts*
- *Alert aggregation*
- *If you get two Alerts with the same title*
- *Warning about missing "Application Name" in Alerts from host-based Sensor for Oracle 9i on *nix platforms*
- *Limitations in Alerts generated by host-based Sensors for Oracle on Windows*
- *Limitations in Alerts generated by host-based Sensors for Oracle on any *nix platform*
- *Limitations in Alerts generated by host-based Sensors for DB2 on any supported platform*
- *Understanding the Alert Manager*
- *Monitoring, filtering, acknowledging, and archiving Alerts (via the Alert Manager).*

What is an Alert?

A **security Alert** is a notification of a monitored security event on the database host or network. DbProtect Audit and Threat Management fires an Alert when the criterion for security Rule in the associated Policy is met (unless an Exception or Filter prevents the Alert from firing). The level of a security Alert is either **High**, **Medium**, or **Low**. For more information, see *Policies*.

An **Informational Alert** (also known as an audit) is a record of standard database activity. The level of an Informational Alert can be **Info-1**, **Info-2**, **Info-3**, or **Info-4**.

Caution! The **Alert Manager** only displays security Alerts. It does **not** display Informational Alerts.

Note: DbProtect audit and threat management may have limitations based on the type of Sensor, the nature of the activity, the target database, and the operating system. For more information, see *DbProtect audit and threat management limitations (based on Sensor type, activity, target database, and operating system).*

Important: Prior to the release of Console Management Server version 4.1 and Sensor version 3.9 (both released as part of DbProtect 2009.1R4), if you wanted to update the security Rules in a Sensor, you had to manually upgrade both your Console and your Sensor.

However, starting with Console Management Server version 4.1, the **Sensor Manager** page allows you to perform an ASAP Update of security Rules in your host- or network-based Sensors, as long as the Console Management Server is at least version 4.1, the Sensor is at least version 3.9, and the Sensor is registered (for more information, see *Registering a Sensor*).

After you ASAP Update your Sensor with the latest security Rules, you can use the **Policy Editor** to update Policies (deployed to your Sensors) with these new security Rules; for more information, see *Policies*.

Monitoring Alerts via the DbProtect Audit and Threat Management UI

The DbProtect Audit and Threat Management UI provides the following two ways to monitor your real-time Alerts:

- **Dashboard.** Provides a graphical quantitative summary of Alerts. Designed for operations personnel, you can quickly and easily identify issues using visual cues. The **Dashboard** automatically refreshes itself every 30 seconds to update the display of new, real-time Alerts. This value is customizable. For more information, see *Monitoring Alerts (via the Dashboard)*.
- **Alert Manager.** Displays real-time Alerts, color-coded for easy identification of risk level. Sorting, grouping, and criteria matching features allow you to Filter views of incoming Alerts. For more information, see *Monitoring, filtering, acknowledging, and archiving Alerts (via the Alert Manager)*.

In addition, the **Report Manager** allows you to create **Detail** and **Summary** Reports for Alerts received by DbProtect Audit and Threat Management, and can be generated and filtered by search criteria. Reports provide information about the Alerts produced in your enterprise, as well as the details that make up those Alerts. For more information, see *Reports*.

Monitoring Alerts as SNMP traps, the log file, or Syslog

Optionally, you can also send Alerts to:

- **SNMP Trap Receiver.** Sensors can fire Alerts as SNMP traps.
- **Log File.** Sensors can write Alerts to a log file.
- **Syslog.** Sensors can write Alerts as Syslog messages. Syslog messages sent out by the Sensors are in **ArcSight CEF**, a standard format for logging security alert messages. These messages can be sent **remotely** over the UDP network protocol or **locally** to a Syslog daemon on the same machine as the Sensor. For more information, see the *DbProtect Administrator's Guide*.

All three methods are specified during Sensor configuration; for more information, see *Configuring a Sensor and deploying the configuration information*.

Acknowledging and archiving Alerts

You can acknowledge and archive Alerts via the **Alert Manager** to ensure proper operational handling of security and audit events. For more information, see *Monitoring, filtering, acknowledging, and archiving Alerts (via the Alert Manager)*.

Note: If you want to back up your Alerts and physically remove them from the DbProtect Audit and Threat Management system, see the *DbProtect Administrator's Guide*.

"Password Guessing" and "Password Scripted Attack" Alerts

The generation of "Password Guessing" and "Password Scripted Attack" Alerts occur on a "per minute" basis. Within any given one minute time interval, there must be at least:

- 10 failed logins to trigger a "Password Guessing" Alert
- 100 failed logins to trigger a "Password Scripted Attack" Alert.

The **Alert Manager** will not display more than one **yellow (medium)** and one **red (high)** Alert per minute for "Password Guessing" and "Password Scripted Attack" Alerts.

Alert aggregation

DbProtect Audit and Threat Management aggregates every:

- 10 **blue (low)** Alerts as one **yellow (medium)** Alert
- 100 **blue (low)** Alerts as one **red (high)** Alert.

Note: Application Security, Inc. implemented this feature because the generation of hundreds of blue (low) Alerts per minute triggered a massive generation of yellow and red Alerts.

If you get two Alerts with the same title

If you are monitoring an Oracle database and you get two Alerts with same Rule Title -- one with all correct information, the one missing information (e.g., login/username, network user, client application name), you should disable the `sql_trace` parameter. You can do so by doing one of the following:

- log on to Oracle as `sys` and run `"alter system set sql_trace=false scope=both`
- update the `init` file.

Warning about missing "Application Name" in Alerts from host-based Sensor for Oracle 9i on *nix platforms

If you have a host-based Sensor installed to monitor an Oracle 9i database on any *nix platform (i.e., Solaris, AIX, HP-UX, and Red Hat Enterprise Linux), the "Application Name" will **not** display in your Alerts. This is because Oracle 9 does not provide a mechanism for the DDL trigger to retrieve the "Application Name" (or "module").

However, this functionality is available in Oracle 10g and greater. Subsequently, DDL Alerts in these Oracle releases now display the "Application Name".

Limitations in Alerts generated by host-based Sensors for Oracle on Windows

If you have a host-based Sensor installed to monitor an Oracle database on Windows:

- Database login names are always reported in Alerts as `/`, while logins are reported as: `as sysdba`.
- The Rule "Login attempt – successful" only works (i.e., only fires an Alert) with local connections.

For more information, see *Configuring a host-based Sensor to monitor Oracle SIDs and services and deploying the configuration information (when Sensor is installed on Windows).*

Limitations in Alerts generated by host-based Sensors for Oracle on any *nix platform

If you have a host-based Sensor installed to monitor an Oracle 9i or 10g database on any *nix platform (i.e., Solaris, AIX, HP-UX, and Red Hat Enterprise Linux), all DDL statements reported via the DDL trigger have **significant restrictions** with respect to the amount of SQL text the trigger can retrieve. In nearly all cases these restrictions are limited to:

- the DDL command (i.e., `DROP`, `CREATE`, etc.)
- the DDL object type (`TABLE`, `VIEW`, `INDEX`, etc.)
- the object name itself.

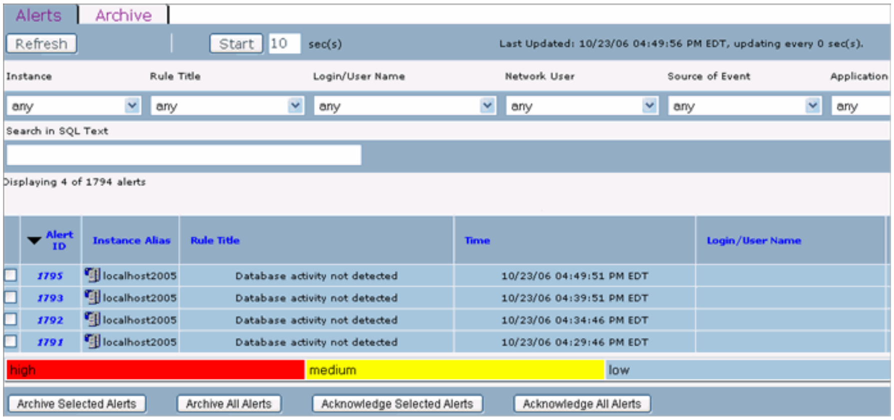
This restriction applies to all DDL statements in Oracle 9i on the Red Hat Enterprise Linux platform and for the `CREATE`, `DROP`, `ASSOCIATE` and `DISASSOCIATE STATISTICS` commands for the other *nix platforms, as well as all platforms running Oracle 10g.

Limitations in Alerts generated by host-based Sensors for DB2 on any supported platform

If you have a host-based Sensor installed to monitor a DB2 on any supported platform (i.e., Red Hat Enterprise Linux, Solaris, AIX, and Microsoft Windows), DB2 will truncate SQL text in Alerts if the SQL text is longer than the size of the pipe used by DB2's event monitor. This limitation is typically 4KB, but may be larger depending on the specific DB2 implementation.

Understanding the Alert Manager

The **Alert Manager** is shown below (partial).



10 sec(s)

Last Updated: 10/23/06 04:49:56 PM EDT, updating every 0 sec(s).

Instance	Rule Title	Login/User Name	Network User	Source of Event	Application
any	any	any	any	any	any

Search in SQL Text

Displaying 4 of 1794 alerts

	Alert ID	Instance Alias	Rule Title	Time	Login/User Name
□	1795	localhost2005	Database activity not detected	10/23/06 04:49:51 PM EDT	
□	1793	localhost2005	Database activity not detected	10/23/06 04:39:51 PM EDT	
□	1792	localhost2005	Database activity not detected	10/23/06 04:34:46 PM EDT	
□	1791	localhost2005	Database activity not detected	10/23/06 04:29:46 PM EDT	

FIGURE: Alert Manager

The **Alert Manager** allows you to monitor your security Alerts, i.e., notifications of monitored security events on the database host or network.

Note: The **Alert Manager** only displays security Alerts. It does **not** display Informational Alerts.

Specifically, the **Alert Manager** allows you to use the:

- **Alerts/Archive tabs** portion of the **Alert Manager** to display the **Archived Alerts** page and view or delete your archived Alerts
- **Alert display tools** portion of the **Alert Manager** to view/sort Alerts, filter Alerts, edit the Alert notification rate, and edit the number of Alerts that display on the **Alert Manager**
- **Acknowledge/Archive buttons** portion of the **Alert Manager** to acknowledge and archive your Alerts
- **Alerts** portion of the **Alert Manager** to view your Alert detail.

For more information, see *Monitoring, filtering, acknowledging, and archiving Alerts (via the Alert Manager)*.

Monitoring, filtering, acknowledging, and archiving Alerts (via the Alert Manager)

DbProtect Audit and Threat Management receives Alerts from your registered Sensors. The **Alert Manager** allows you to monitor your real-time Alerts. You can view, sort, Filter, acknowledge, archive, and delete them on this page.

The **Alert Manager** also allows you to change the Alert notification rate (default rate = 10 seconds), and the number of Alerts that display on the page (default number = 10 Alerts). The auto refresh feature is **not** turned on by default. To turn on the auto refresh feature, you must click the **Start** button. For more information, see Step 6, below.

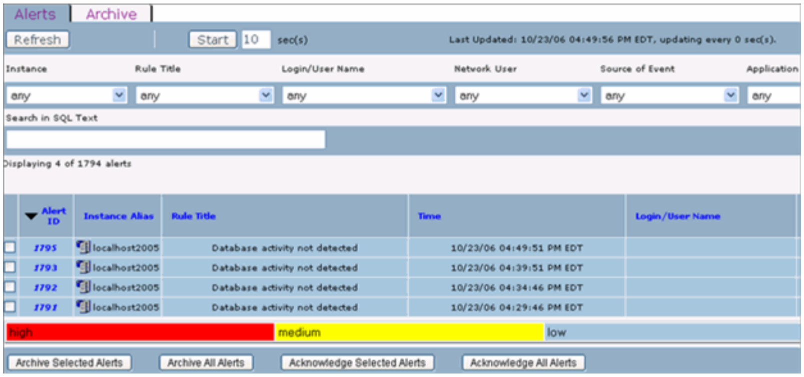
Caution! When you have not used DbProtect Audit and Threat Management for a while, your Session normally times out. However, on certain pages, it does **not**. Specifically, Audit and Threat Management does **not** time out on the **Alert Manager**, the **Dashboard**, and the **ASAP Update** portion of the **Sensor Manager**.

To monitor Alerts (via the **Alert Manager**):

1. Do one of the following to display the **Alert Manager**:

- Click the **Alerts - Security Monitoring** workflow link on the **Home** page.
- Click the **Alerts** tab from anywhere on the page.

The **Alerts** section displays by default. You can click the **Archive** tab at the top of the page to display the Archive portion of the **Alert Manager**.



10 sec(s)

Last Updated: 10/23/06 04:49:56 PM EDT, updating every 0 sec(s).

Instance	Rule Title	Login/User Name	Network User	Source of Event	Application
any	any	any	any	any	any

Search in SQL Text

Displaying 4 of 1794 alerts

	Alert ID	Instance Alias	Rule Title	Time	Login/User Name
□	1795	localhost2005	Database activity not detected	10/23/06 04:49:51 PM EDT	
□	1793	localhost2005	Database activity not detected	10/23/06 04:39:51 PM EDT	
□	1792	localhost2005	Database activity not detected	10/23/06 04:34:46 PM EDT	
□	1791	localhost2005	Database activity not detected	10/23/06 04:29:46 PM EDT	

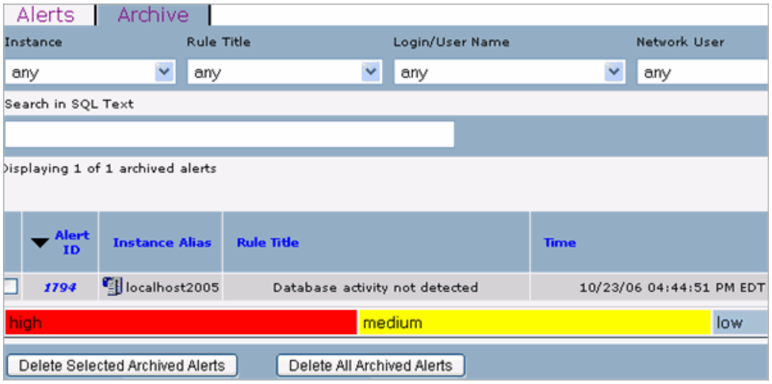
FIGURE: Alert Manager

2. Your **Alert Manager** options follow. If you want to:

- view or delete your archived Alerts, go to Step 3
- view or sort your Alerts, go to Step 4
- filter your Alerts, go to Step 5
- edit the Alert notification rate, go to Step 6
- acknowledge and archive your Alerts, go to Step 7
- view Alert detail, go to Step 8.

3. View or delete your archived Alerts.

You can click the **Archive** tab (in the **Alerts/Archive tabs** portion of the **Alert Manager**) to display the **Archived Alerts** page and view your archived Alerts.



Instance	Rule Title	Login/User Name	Network User
any	any	any	any

Search in SQL Text

)isplaying 1 of 1 archived alerts

	Alert ID	Instance Alias	Rule Title	Time
□	1794	localhost2005	Database activity not detected	10/23/06 04:44:51 PM EDT

high	medium	low

FIGURE: **Alert Manager** (**Archived Alerts** page)

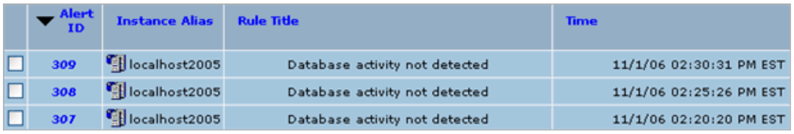
You can delete:

- **selected** archived Alerts by checking one or more archived Alerts, then clicking the **Delete Selected Archived Alerts** button
- **all** archived Alerts by clicking the **Delete All Archived Alerts** button.

4. View your Alerts.

The **Alerts** portion of the **Alert Manager** page displays your real-time Alerts, color-coded by risk level, i.e., **High** (red), **Medium** (yellow), **Low** (blue), and **Acknowledged** (gray).

Important: To view the Alert detail, click any **Alert ID** to display an Alert detail pop up, then go to Step 9.



	Alert ID	Instance Alias	Rule Title	Time
□	309	localhost2005	Database activity not detected	11/1/06 02:30:31 PM EST
□	308	localhost2005	Database activity not detected	11/1/06 02:25:26 PM EST
□	307	localhost2005	Database activity not detected	11/1/06 02:20:20 PM EST

FIGURE: **Alert Manager** (**Alerts** portion)

Note: Risk levels are derived from built-in Rules. These Rules define the Policy deployed to an instance monitored by a Sensor, and determine when Alerts are fired. For more information, see *What is a Policy?* and *What do the risk levels mean?*

Caution! If you get two Alerts with the same rule title -- one containing correct information, and another one containing missing information (e.g., missing login/username, network user, and client application name), you may need to disable `sql_trace`. For more information, see ***If you get two Alerts with the same title***.

Sort your Alerts.

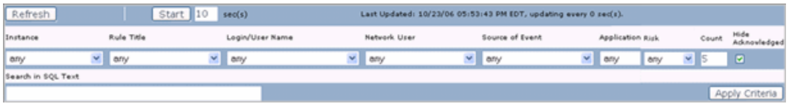
You can sort your Alerts by clicking any of the following column links (on the header row of the **Alert** portion of the page):

- **Alert ID** (default)
- **Instance Name**
- **Rule Title**
- **Time**
- **Login/User Name**
- **Network User**
- **Source of Attack**
- **Client Application Name**.

For example, if you want to sort your Alerts from latest-to-oldest, click the **Time** column link. Also note, you can sort your Alerts in ascending or descending order.

5. Filter your Alerts.

When you have a lot of Alerts, sometimes it's difficult and time-consuming to see the most important ones. The **Alert display tools** allow you to filter your Alerts.



Start 10 sec(s)

Last Updated: 10/23/06 05:53:43 PM EDT, updating every 0 sec(s).

Instance	Rule Title	Login/User Name	Network User	Source of Event	Application	Risk	Count	Hide Acknowledged
any	any	any	any	any	any	any	5	☑

Search in SQL Text

FIGURE: **Alert Manager** (Alert display tools)

You can filter your Alerts by:

- **Filter drop-downs.** The Alert filter drop-downs are:

  -**Instance**

  -**Rule Title**

  -**Login/User Name**

  -**Network User**

  -**Source of Attack**

  -**Application**

  -**Risk Level**.

  Use these drop-downs to filter your Alert data, then click the **Apply Criteria** button to display Alerts that match your filter criteria.

- **Filtering SQL text.** Enter valid SQL text in the **Search in SQL text** field, then click the **Apply Criteria** button (only for filtering host-based SQL Server Alerts).

  For example, if you want to Filter Alerts with the SQL text `Select`, enter `Select` in the **Search in SQL Text** field, then click the **Apply Criteria** button to display all Alerts with the SQL text `Select`.
- **Acknowledged Alerts only.** Uncheck the **Hide Acknowledged** checkbox (checked by default), then click the **Apply Criteria** button to display acknowledged Alerts in addition to unacknowledged Alerts.
- **Specify an Alert count.** You can enter the exact number of Alerts that you want to display in the **Count** field, then click the **Apply Criteria** button to display the specified number (prioritized by most-recent Alerts). For example, if you enter `50` in the **Count** field, then click the **Apply Criteria** button, the **Alert Manager** displays your most-recent 50 Alerts received (depending on your filtering configuration).

6. Edit your Alert notification rate.

The Alert display tools allow you to monitor your real-time Alerts more (or less) frequently than every 10 seconds (i.e., the default Alert notification rate).

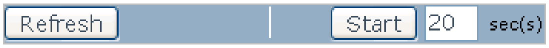


FIGURE: **Alert Manager** (Alert display tools)

To edit the Alert notification rate, and activate the auto-refresh feature, enter the number of seconds in the **sec(s)** field, then click the **Start** button.

Note: The auto refresh feature is not turned on by default. You must click the **Refresh** button. To turn on the auto refresh feature, click the **Start** button. You can customize the auto refresh rate in the text field next to the **Start** button.

7. Acknowledge/archive your Alerts.

Note: If you want to back up your Alerts and physically remove them from the DbProtect Audit and Threat Management system, see the *DbProtect Administrator's Guide*.

The **Alert Manager** acknowledge/archive buttons allow you to archive and acknowledge your Alerts.

When you:

- **acknowledge** an Alert, you affirm that you have reviewed it
- **archive** an Alert, you hide it from displaying on the Alert Manager, but you do not delete it.

Note: If you archive an unacknowledged Alert, DbProtect Audit and Threat Management marks the archived Alert as "acknowledged" and "archived" in the DbProtect Audit and Threat Management database.

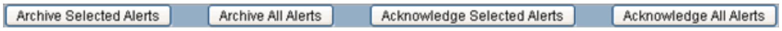


FIGURE: **Alert Manager** (acknowledge/archive buttons)

You can:

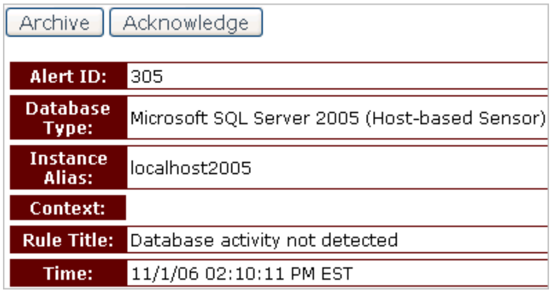
- acknowledge an individual Alert by checking the individual Alert and clicking the **Acknowledge Selected Alerts** button, *or* you can click the Alert ID to display the Alert detail pop up and click the **Acknowledge** button
- acknowledge **all** Alerts by clicking the **Acknowledge All Alerts** button
- archive individual Alerts by checking the individual Alert and clicking the **Archive Selected Alerts** button, *or* you can click the Alert ID to display the Alert detail pop up and click the **Archive** button
- archive **all** Alerts by clicking the **Archive All Alerts** button.

Note: You can click the **Archive** tab at the top of the page to display the **Archive** section of the Alert Manager and display your archived Alerts; see Step 8.

The Alert detail pop up also allows you to acknowledge or archive the Alert; for more information, see Step 8.

8. View Alert detail.

Click an **Alert ID** in the **Alerts** portion of the **Alert Manager** (see Step 4) to display an Alert detail pop up.



Alert ID:	305
Database Type:	Microsoft SQL Server 2005 (Host-based Sensor)
Instance Alias:	localhost2005
Context:	
Rule Title:	Database activity not detected
Time:	11/1/06 02:10:11 PM EST

FIGURE: Alert detail pop up

The Alert detail pop up displays the following information about a given Alert:

- **Alert ID:**
- **Database Type:**
- **Instance Alias:**
- **Context:**
- **Rule Title:**

- **Time:**
- **Login/User Name:**
- **Network User:**
- **Source of Event:**

Note: When host-based Sensors for DB2 (all supported platforms) fire a failed login Alert, the **Source of Event:** field is blank. When host- and network-based Sensors for Oracle (all supported platforms) fire a failed or successful login Alert, the **Source of Event:** field is blank.

- **SQL Text:**
- **Records Affected:**

Note: The **Records Affected:** row is a **result set**, which refers to the number of records returned as the result of executing a SQL statement; for more information, see *Understanding result sets*. When DbProtect Audit and Threat Management stores identical SQL statements, and their **Risk Level:** is **Info-1**, **Info-2**, or **Info-3**, then DbProtect Audit and Threat Management aggregates the **Records Affected**.

Important: Alerts from host-based Sensor for Oracle on *nix platforms do **not** contain a value for the **Records Affected:** field.

- **Client Application Name:**

Note: When host- and network-based Sensors for Oracle (all supported platforms) fire a failed or successful login Alert, the **Client Application Name:** field is blank.

- **Risk Level:**
- **CVE Reference #:**
- **Description**.

The Alert detail pop up allows you to click the **Acknowledge** and **Archive** buttons to acknowledge or archive the Alert, respectively; for more information, see Step 7.

Policies

This chapter consists of the following topics:

- *What is a Policy?*
- *ASAP Updating Rules in your Sensors*
- *Understanding the Policy Manager*
- *What do the risk levels mean?*
- *What are the default Policies?*
- *Creating a Policy*
- *Editing a Policy*
- *Importing a Policy*
- *Exporting a Policy*
- *Deploying a Policy*
- *Deleting a Policy*
- *Policy Editor rule categories*.

What is a Policy?

A **Policy** is a set of security Rules which identifies the conditions under which Alerts are fired and sent to DbProtect Audit and Threat Management. Such activity may include intrusion attempts, or other malicious behavior. Policies can also monitor database activity of authorized users. Different Sensors, SIDs, or database instances may require different Policies, since intrusion risk and data sensitivity often vary between database installations.

Once you register a Sensor, you must then deploy the configuration of a database instance or SID to a host- or network-based Sensor. Subsequently, the Sensor fires Alerts when the conditions/criterion of a Policy's Rules are met (*except* when Rules or conditions are filtered or excepted); for more information, see *What is a Filter?*

Note: You can, optionally, deploy a Policy during database SID or instance configuration; *Configuring a Sensor and deploying the configuration information*. However, deploying a Policy via the **Policy Manger** allows you to deploy Policies to **multiple** instances simultaneously, which may (or may not) be monitored by the same Sensor.

You can:

- create a new Policy using the **Policy Editor**, applying security Rules available in the **Policy Editor**; for more information, see *Creating a Policy*
- edit built-in Policies using the **Policy Editor**, then "save as" a new Policy (built-in Policies cannot be overwritten); for more information, see *Editing a Policy*
- import or export a Policy file (in XML format); for more information, see *Importing a Policy* and *Exporting a Policy*, respectively
- deploy a Policy to a Sensor with the **Policy Manager**; for more information, see *Deploying a Policy*
- delete a Policy with the **Policy Manager**; for more information, see *Deleting a Policy*.

ASAP Updating Rules in your Sensors

Prior to the release of Console Management Server version 4.1 and Sensor version 3.9 (both released as part of DbProtect 2009.1R4), if you wanted to update the security Rules in a Sensor, you had to manually upgrade both your Console and your Sensor.

However, starting with Console Management Server version 4.1, the **Sensor Manager** page allows you to perform an ASAP Update of security Rules in your host- or network-based Sensors, as long as:

- the Console Management Server is at least version 4.1
- the Sensor is at least version 3.9
- the Sensor is registered (for more information, see *Registering a Sensor*)
- the Sensor does **not** already contain the latest available security Rules from the Application Security, Inc. security Rules **knowledgebase**.

For **detailed instructions** on ASAP Updating security Rules in your Sensors, see *Performing an ASAP Update of Rules in your Sensors*.

After you ASAP Update your Sensor with the latest security Rules, you can use the **Policy Editor** to update Policies (deployed to your Sensors) with these new security Rules; for more information, see *Creating a Policy* and *Editing a Policy*.

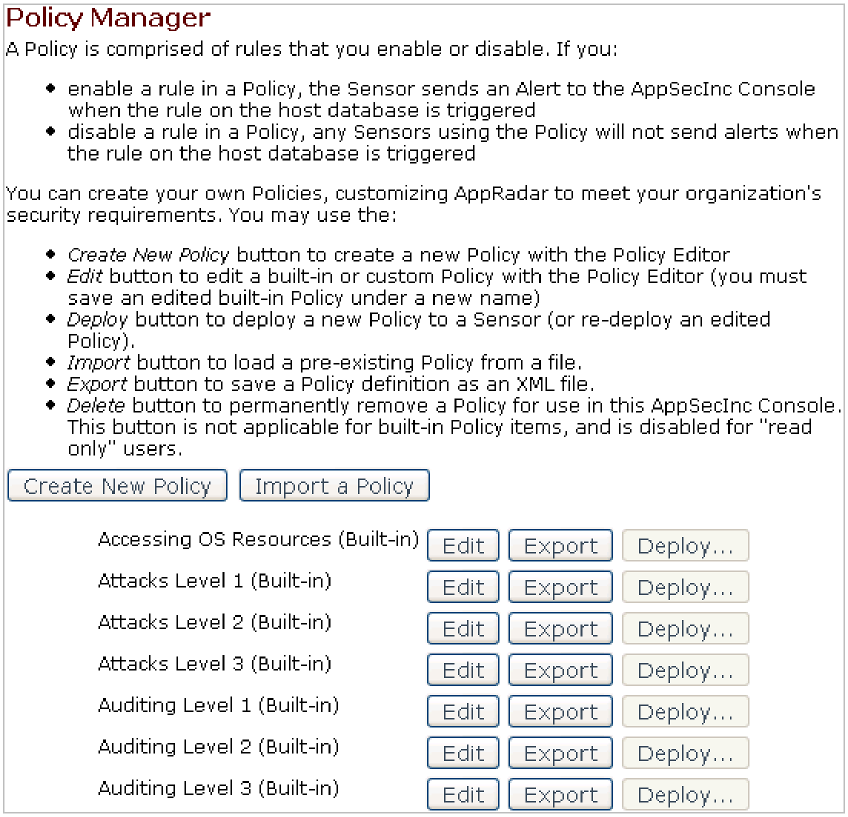
What do the risk levels mean?

Every Rule in an Policy is associated, by default, with a risk level. You can modify these risk levels in a custom Policy. The risk levels are:

- **High: Security Alert**
- **Medium: Security Alert**
- **Low: Security Alert**
- **Info-1: Interval-based/Parameterless SQL**
- **Info-2: Exact-time/Parameterless SQL**
- **Info-3: Interval-based/Exact SQL**
- **Info-4: Exact-time/Exact SQL**.

Understanding the Policy Manager

The **Policy Manager** is shown below (partial).



Policy Manager

A Policy is comprised of rules that you enable or disable. If you:

- enable a rule in a Policy, the Sensor sends an Alert to the AppSecInc Console when the rule on the host database is triggered
- disable a rule in a Policy, any Sensors using the Policy will not send alerts when the rule on the host database is triggered

You can create your own Policies, customizing AppRadar to meet your organization's security requirements. You may use the:

- *Create New Policy* button to create a new Policy with the Policy Editor
- *Edit* button to edit a built-in or custom Policy with the Policy Editor (you must save an edited built-in Policy under a new name)
- *Deploy* button to deploy a new Policy to a Sensor (or re-deploy an edited Policy).
- *Import* button to load a pre-existing Policy from a file.
- *Export* button to save a Policy definition as an XML file.
- *Delete* button to permanently remove a Policy for use in this AppSecInc Console. This button is not applicable for built-in Policy items, and is disabled for "read only" users.

Accessing OS Resources (Built-in)	Edit	Export	Deploy...
Attacks Level 1 (Built-in)	Edit	Export	Deploy...
Attacks Level 2 (Built-in)	Edit	Export	Deploy...
Attacks Level 3 (Built-in)	Edit	Export	Deploy...
Auditing Level 1 (Built-in)	Edit	Export	Deploy...
Auditing Level 2 (Built-in)	Edit	Export	Deploy...
Auditing Level 3 (Built-in)	Edit	Export	Deploy...

FIGURE: **Policy Manager**

The **Policy Manager** allows you to:

- create a Policy; for more information, see *Creating a Policy*
- edit a Policy; for more information, see *Editing a Policy*
- import a Policy; for more information, see *Importing a Policy*
- export a Policy; for more information, see *Exporting a Policy*
- deploy a Policy; for more information, see *Deploying a Policy*
- delete a Policy; for more information, see *Deleting a Policy*.

What are the default Policies?

DbProtect Audit and Threat Management is configured with **default Polices**. The rules contained in these Polices are database-platform-specific. The default Policies are:

- **Accessing OS Resources (Built-in).** This default Policy selects Rules that monitor for attempts to access OS-level resources.
- **Attacks Level 1 (Built-in), Attacks Level 2 (Built-in)**, and **Attacks Level 3 (Built-in).** These default Policies were developed by Application Security, Inc. security researchers to detect attempts to attack your database. Level 1 attacks are the *least* stringent; Level 3 attacks are the *most* stringent.
- **Auditing Level 1 (Built-in)**, **Auditing Level 2 (Built-in)**, **Auditing Level 3 (Built-in),** and **Auditing Level 4 (Built-in).** These default Policies were developed by Application Security, Inc. researchers to audit activity on your database. Level 1 audits are the *least* comprehensive; Level 4 audits are the *most* comprehensive.
- **Buffer Overflows (Built-in).** This default Policy selects all Rules related to buffer overflow attempts.
- **FISMA Policy (Built-In)**, **HIPAA Policy (Built-In)**, **Payment Card Industry Data Security Standard (Built-In),** and **Sarbanes-Oxley Policy (Built-In).** All of our built-in Policies were a result of a joint effort between Application Security, Inc.'s R&D Team SHATTER and DbProtect Audit and Threat Management users all over the world across all industries. All of the following built-in Policies were created in response to facilitate the database auditing and threat monitoring requirements of users within each respective vertical:

  -**FISMA Policy (Built-in).** The Federal Information Security Management Act (FISMA) provides a comprehensive framework for ensuring effective information security controls for all federal information and assets. This built-in Policy is enabled with all of the baseline rules and events to monitor all access to Federal databases.

  -**HIPAA Policy (Built-in).** The Health Insurance Portability and Accountability Act (HIPAA) is designed to protect all forms of personal health information (PHI), by defending the patients' rights to have their health information kept private and preserving control of how their PHI data is used and when it is disclosed. This built-in Policy is enabled with all of the baseline rules and events to facilitate monitoring all access to PHI by unique ID.

  -**Payment Card Industry Data Security Standard (Built-in).** To unify disparate efforts, credit card companies created the Payment Card Industry (PCI) Data Security Standard. Spearheaded by Visa and MasterCard, PCI offers a common framework for protecting sensitive cardholder data for all card brands. This built-in Policy is enabled with all of the baseline rules and events to facilitate monitoring all access to cardholder data by unique ID.

-**Sarbanes-Oxley Policy (Built-in).** The Sarbanes-Oxley Act (SOX) radically redesigned federal regulation of public company corporate governance and Reporting obligations by demanding executives, auditors, securities analysts, and legal counsel be accountable for the integrity of financial Reporting. This built-in Policy is enabled with all of the baseline rules and events to facilitate monitoring all access to SOX-relevant databases.

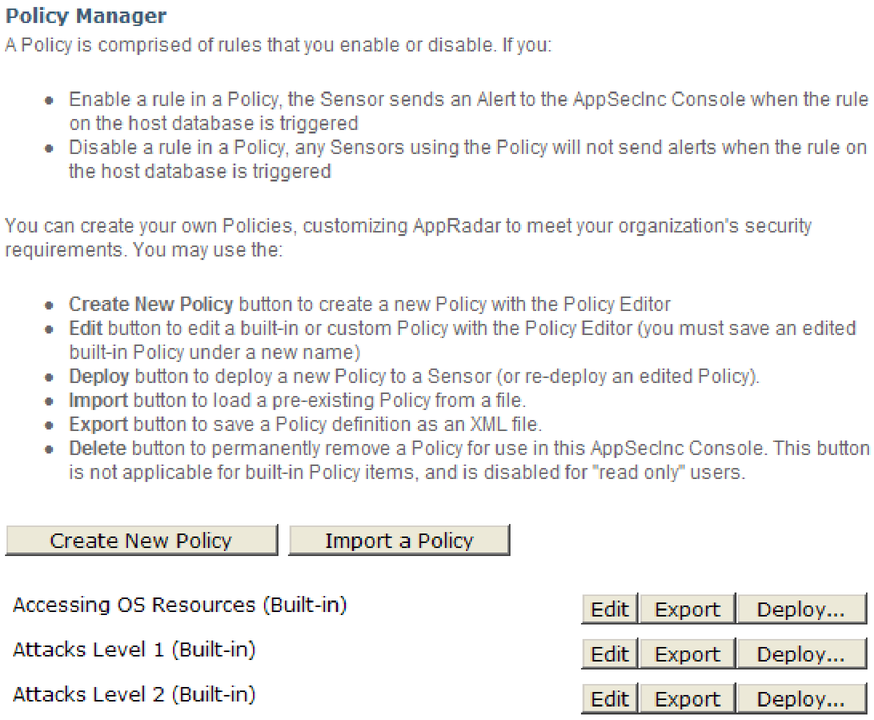
- **Password Attacks (Built-in).** This default Policy selects all Rules that detect attempts to guess passwords by trying likely combinations of characters or exploiting certain vulnerabilities.
- **Privilege Escalation (Built-in).** This default Policy selects all Rules that detect attempts to exploit known vulnerabilities to achieve privilege escalation, and in doing so perform tasks they are not authorized to perform.
- **Security Tools (Built-in).** This default Policy selects all Rules that check for tools that scan your database, in order to determine who is running these tools, when, and against which database.
- **Web Application Attacks (Built-in).** This default Policy selects all Rules that monitor against possible access-related attacks.
- **Miscellaneous (Built-in).** This default Policy selects all Rules that detect attacks and events that do not necessarily fall within any of the other provided Activity DbProtect Monitoring and Auditing Rule categories.

Creating a Policy

To create a Policy:

1. Do one of the following to display the **Policy Manager** page:

- Click the **Policies** workflow link on the **Home** page.
- Click the **Policies** tab from anywhere on the page.



Policy Manager

A Policy is comprised of rules that you enable or disable. If you:

- Enable a rule in a Policy, the Sensor sends an Alert to the AppSecInc Console when the rule on the host database is triggered
- Disable a rule in a Policy, any Sensors using the Policy will not send alerts when the rule on the host database is triggered

You can create your own Policies, customizing AppRadar to meet your organization's security requirements. You may use the:

- **Create New Policy** button to create a new Policy with the Policy Editor
- **Edit** button to edit a built-in or custom Policy with the Policy Editor (you must save an edited built-in Policy under a new name)
- **Deploy** button to deploy a new Policy to a Sensor (or re-deploy an edited Policy).
- **Import** button to load a pre-existing Policy from a file.
- **Export** button to save a Policy definition as an XML file.
- **Delete** button to permanently remove a Policy for use in this AppSecInc Console. This button is not applicable for built-in Policy items, and is disabled for "read only" users.

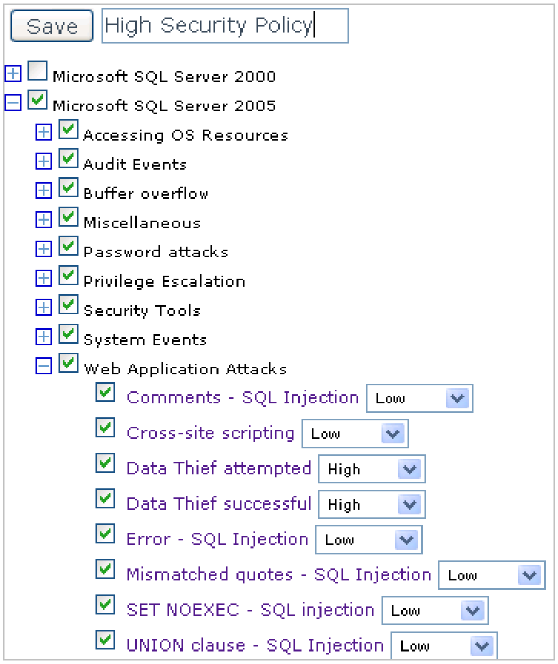
Accessing OS Resources (Built-in)

Attacks Level 1 (Built-in)

Attacks Level 2 (Built-in)

FIGURE: Policy Manager

2. Click the **Create New Policy** button to display the **Policy Editor** page.



Save | High Security Policy

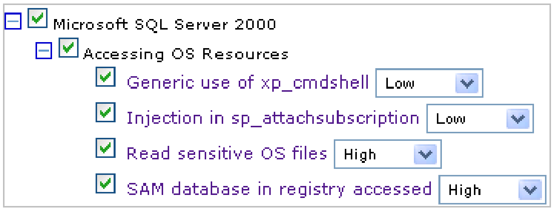
- ⊞ ☐ Microsoft SQL Server 2000
- ⊟ ☑ Microsoft SQL Server 2005
  - ⊞ ☑ Accessing OS Resources
  - ⊞ ☑ Audit Events
  - ⊞ ☑ Buffer overflow
  - ⊞ ☑ Miscellaneous
  - ⊞ ☑ Password attacks
  - ⊞ ☑ Privilege Escalation
  - ⊞ ☑ Security Tools
  - ⊞ ☑ System Events
  - ⊟ ☑ Web Application Attacks
    - ☑ Comments - SQL Injection: Low
    - ☑ Cross-site scripting: Low
    - ☑ Data Thief attempted: High
    - ☑ Data Thief successful: High
    - ☑ Error - SQL Injection: Low
    - ☑ Mismatched quotes - SQL Injection: Low
    - ☑ SET NOEXEC - SQL injection: Low
    - ☑ UNION clause - SQL Injection: Low

FIGURE: Policy Editor

3. Create your Policy.

Click one or more database platforms that you want your custom Policy to monitor. Your choices are:

- **Microsoft SQL Server 2000**
- **Microsoft SQL Server 2005**
- **Microsoft SQL Server 2008**
- **Oracle Database**
- **Sybase ASE (Network)**
- **DB2 (Network)**.



- ⊟ ☑ Microsoft SQL Server 2000
  - ⊟ ☑ Accessing OS Resources
    - ☑ Generic use of xp_cmdshell: Low
    - ☑ Injection in sp_attachsubscription: Low
    - ☑ Read sensitive OS files: High
    - ☑ SAM database in registry accessed: High

FIGURE: **Policy Editor** (icons, checkboxes, drop-downs, and Rule links)

You can:

- click a **+** icon next to a platform name to display the underlying default Rules (or click the **-** icon to collapse)
- check a checkbox next to a platform name to select all built-in Rules that apply for this platform (or uncheck to de-select all)
- click a **+** icon next to a default Policy category to display the underlying Rules (or click the **-** icon to collapse)
- check a checkbox next to a default Policy category to select all underlying Rules for the Policy (or uncheck to de-select all)
- check a checkbox next to:

  -an individual Rule to activate the Rule in the Policy (or uncheck to deactivate)

  -a Filter to add the Filter to the Policy (or uncheck to remove); for more information, see *Filters*
- click an individual Rule/Filter link to display Rule/Filter details in the right frame of the **Policy Editor**
- use the individual Rule drop-downs to change the risk level of an individual Rule from its default setting. Your choices are: **High**, **Medium**, **Low**, or **Informational** (i.e., **Info-1**, **Info-2**, **Info-3**, and **Info-4**), which are typically for audit events. Audit events are written to a table in the DbProtect Audit and Threat Management database, but **not** displayed on the **Alert Manager** page of the DbProtect Audit and Threat Management UI. For more information, see *What do the risk levels mean?*

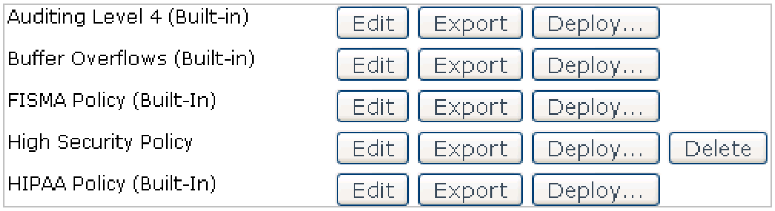
4. Enter your custom Policy name (e.g., `High Security Policy`) in the field next to the **Save** button.

Note: Policy names **must** be unique.

5. Click the **Save** button.

Important: If you have created any Filters/Exception for a specific platform, you must enable them separately. Turning on off the base Rules for a particular platform does **not** automatically also turn on all of the Filters/Exceptions that may currently exist for a database platform. For more information, see *Filters*.

The **Policy Manager** page re-displays. Your custom Policy is listed.



Auditing Level 4 (Built-in)	Edit	Export	Deploy...	
Buffer Overflows (Built-in)	Edit	Export	Deploy...	
FISMA Policy (Built-In)	Edit	Export	Deploy...	
High Security Policy	Edit	Export	Deploy...	Delete
HIPAA Policy (Built-In)	Edit	Export	Deploy...	

FIGURE: **Policy Manager** (with a custom Policy added)

Note: A **Delete** button displays next to custom Policies. Unlike built-in Policies, you can delete a custom Policy; for more information, see *Deleting a Policy*.

6. You can now deploy your custom Policy to a Sensor; for more information, see *Deploying a Policy*.

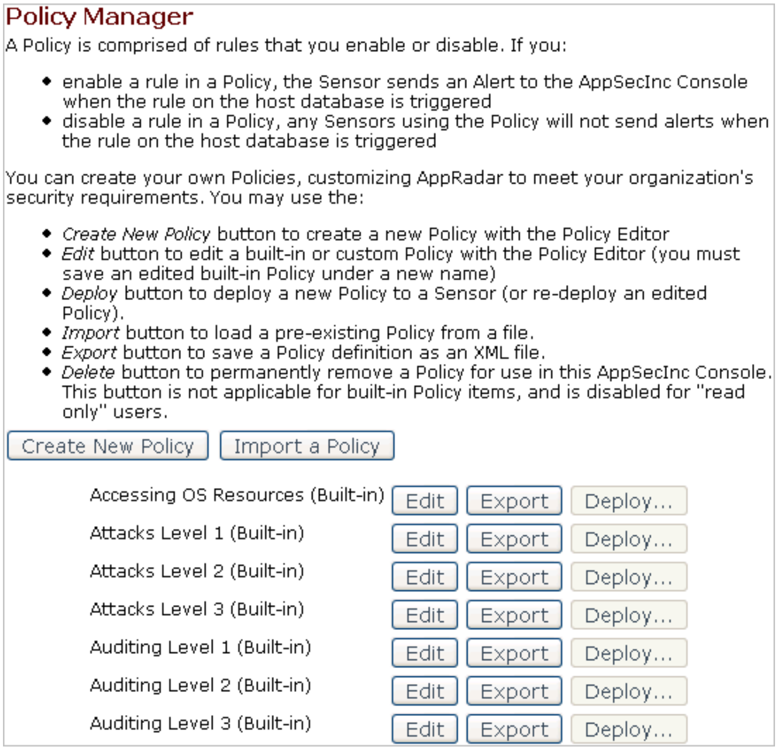
Editing a Policy

The **Policy Manager** allows you to edit a built-in or custom Policy. You **cannot** save an edited built-in Policy under its original name, but you **can** use the "save as" option to save an edited built-in Policy under a different name.

To edit a Policy:

1. Do one of the following to display the **Policy Manager** page:

- Click the **Policies** workflow link on the **Home** page.
- Click the **Policies** tab from anywhere on the page.



Policy Manager

A Policy is comprised of rules that you enable or disable. If you:

- enable a rule in a Policy, the Sensor sends an Alert to the AppSecInc Console when the rule on the host database is triggered
- disable a rule in a Policy, any Sensors using the Policy will not send alerts when the rule on the host database is triggered

You can create your own Policies, customizing AppRadar to meet your organization's security requirements. You may use the:

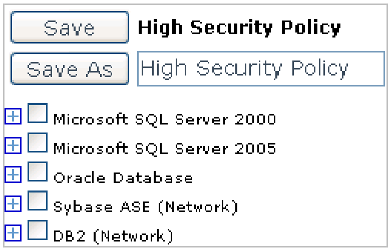
- *Create New Policy* button to create a new Policy with the Policy Editor
- *Edit* button to edit a built-in or custom Policy with the Policy Editor (you must save an edited built-in Policy under a new name)
- *Deploy* button to deploy a new Policy to a Sensor (or re-deploy an edited Policy).
- *Import* button to load a pre-existing Policy from a file.
- *Export* button to save a Policy definition as an XML file.
- *Delete* button to permanently remove a Policy for use in this AppSecInc Console. This button is not applicable for built-in Policy items, and is disabled for "read only" users.

Accessing OS Resources (Built-in)
Attacks Level 1 (Built-in)
Attacks Level 2 (Built-in)
Attacks Level 3 (Built-in)
Auditing Level 1 (Built-in)
Auditing Level 2 (Built-in)
Auditing Level 3 (Built-in)

FIGURE: Policy Manager

2. Click the **Edit** button next to the Policy you want to edit to display the **Policy Editor** dialog box.

Note: If you are editing a built-in Policy and saving it under a different name, then only the **Save As** button and field display (the original name of the Policy displays above). However, if you are editing a custom Policy, then both the **Save** and **Save As** buttons and fields display, allowing you to save the custom Policy under its original name or "save as" a new name, respectively.



High Security Policy

High Security Policy

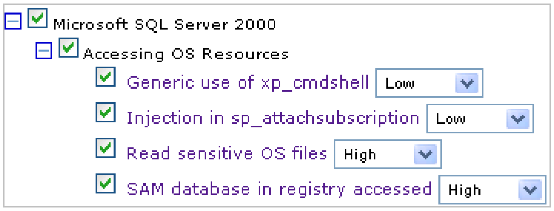
- ⊞ ☐ Microsoft SQL Server 2000
- ⊞ ☐ Microsoft SQL Server 2005
- ⊞ ☐ Oracle Database
- ⊞ ☐ Sybase ASE (Network)
- ⊞ ☐ DB2 (Network)

FIGURE: Policy Editor

3. Edit your Policy.

Click one or more database platforms that you want your custom Policy to monitor. Your choices are:

- **Microsoft SQL Server 2000**
- **Microsoft SQL Server 2005**
- **Microsoft SQL Server 2008**
- **Oracle Database**
- **Sybase ASE (Network)**
- **DB2 (Network)**.



⊟ ☑ Microsoft SQL Server 2000

⊟ ☑ Accessing OS Resources

- ☑ Generic use of xp_cmdshell Low
- ☑ Injection in sp_attachsubscription Low
- ☑ Read sensitive OS files High
- ☑ SAM database in registry accessed High

FIGURE: **Policy Editor** (icons, checkboxes, drop-downs, and Rule links)

You can:

- click a **+** icon next to a platform name to display the underlying Rules (or click the **-** icon to collapse)
- check a checkbox next to a platform name to select all default Policies for the platform (or uncheck to de-select all)

- click a **+** icon next to a default Policy category to display the underlying Rules (or click the **-** icon to collapse)
- check a checkbox next to a default Policy category to select all underlying Rules for the Policy (or uncheck to de-select all)
- check a checkbox next to:

  -an individual Rule to activate the Rule in the Policy (or uncheck to deactivate)

  -a Filter to add the Filter to the Policy (or uncheck to remove); for more information, see *Filters*
- click an individual Rule/Filter link to display Rule/Filter details in the right frame of the **Policy Editor**
- use the individual Rule drop-downs to change the risk level of an individual Rule from its default setting. Your choices are: **High**, **Medium**, **Low**, or **Informational** (i.e., **Info-1**, **Info-2**, **Info-3**, and **Info-4**), which are typically for audit events. Audit events are written to a table in the DbProtect Audit and Threat Management database, but **not** displayed on the **Alert Manager** page of the UI. For more information, see *What do the risk levels mean?*

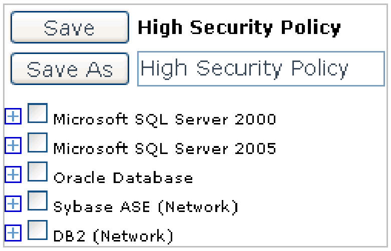
4. If you are editing:

- a built-in Policy and saving it as a custom Policy, then enter the custom Policy name in the field next to the **Save** button, and click the **Save** button
- an existing custom Policy (as shown below), then you can:

  -click the **Save** button to save the edited custom Policy under its original name

  -enter a *new* custom Policy name in the field next to the **Save As** button, and click the **Save As** button.

Note: Policy names **must** be unique.



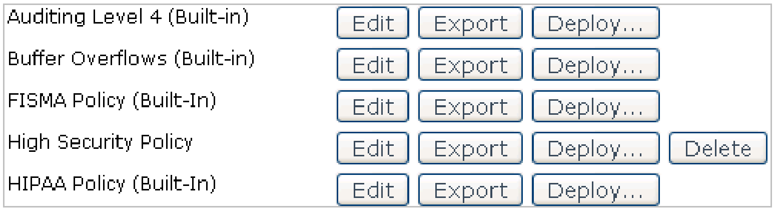
High Security Policy

High Security Policy

⊞ □ Microsoft SQL Server 2000
⊞ □ Microsoft SQL Server 2005
⊞ □ Oracle Database
⊞ □ Sybase ASE (Network)
⊞ □ DB2 (Network)

FIGURE: **Policy Editor** (when editing an *existing* custom Policy)

The **Policy Manager** page re-displays. Your custom Policy is listed.



Auditing Level 4 (Built-in)	Edit	Export	Deploy...	
Buffer Overflows (Built-in)	Edit	Export	Deploy...	
FISMA Policy (Built-In)	Edit	Export	Deploy...	
High Security Policy	Edit	Export	Deploy...	Delete
HIPAA Policy (Built-In)	Edit	Export	Deploy...	

FIGURE: **Policy Manager** (with a custom Policy added)

Note: A **Delete** button displays next to custom Policies. Unlike built-in Policies, you can delete a custom Policy; for more information, see *Deleting a Policy*.

5. You can now deploy your edited custom Policy to a Sensor; for more information, see *Deploying a Policy*.

Importing a Policy

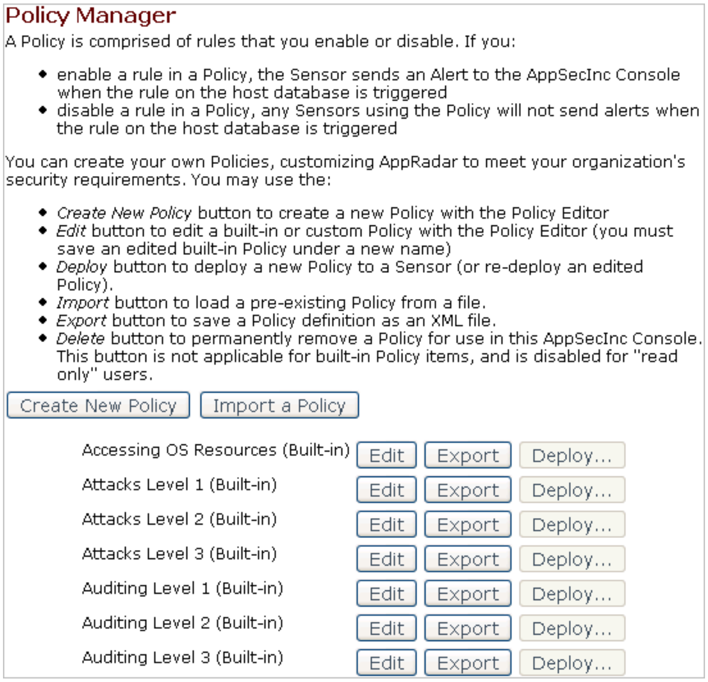
You can **import** an Policy file (in XML format).

Caution! Do **not** manually modify/create XML Policy files for import purposes; they may not work properly.

Important: When you import a Policy, it **must** include all Filters. If you import a Policy that includes custom Filters, the order of the Filters is significant.

To import a Policy:

1. Do one of the following to display the **Policy Manager** page:
   - Click the **Policies** workflow link on the **Home** page.
   - Click the **Policies** tab from anywhere on the page.



Policy Manager

A Policy is comprised of rules that you enable or disable. If you:

- enable a rule in a Policy, the Sensor sends an Alert to the AppSecInc Console when the rule on the host database is triggered
- disable a rule in a Policy, any Sensors using the Policy will not send alerts when the rule on the host database is triggered

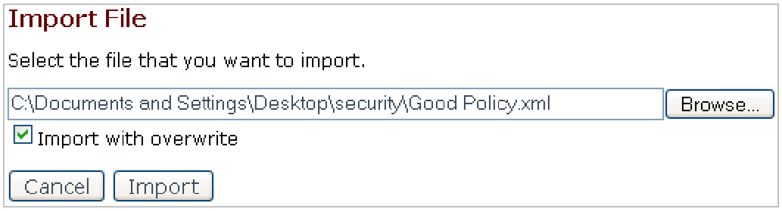
You can create your own Policies, customizing AppRadar to meet your organization's security requirements. You may use the:

- *Create New Policy* button to create a new Policy with the Policy Editor
- *Edit* button to edit a built-in or custom Policy with the Policy Editor (you must save an edited built-in Policy under a new name)
- *Deploy* button to deploy a new Policy to a Sensor (or re-deploy an edited Policy).
- *Import* button to load a pre-existing Policy from a file.
- *Export* button to save a Policy definition as an XML file.
- *Delete* button to permanently remove a Policy for use in this AppSecInc Console. This button is not applicable for built-in Policy items, and is disabled for "read only" users.

Accessing OS Resources (Built-in)	Edit	Export	Deploy...
Attacks Level 1 (Built-in)	Edit	Export	Deploy...
Attacks Level 2 (Built-in)	Edit	Export	Deploy...
Attacks Level 3 (Built-in)	Edit	Export	Deploy...
Auditing Level 1 (Built-in)	Edit	Export	Deploy...
Auditing Level 2 (Built-in)	Edit	Export	Deploy...
Auditing Level 3 (Built-in)	Edit	Export	Deploy...

FIGURE: **Policy Manager**

2. Click the **Import a Policy** button to display the **Import File** page.



Import File

Select the file that you want to import.

C:\Documents and Settings\Desktop\security\Good Policy.xml

☑ Import with overwrite

FIGURE: **Import File** page

3. Specify the location of the Policy file (must be in XML format). You can:
   - click the **Browse...** button to display the **File Upload** pop up and locate the Policy file you want to import (on your local computer or network)
   - enter the full path and file name of the XML Policy file you want to import (on your local computer or network).

Note: Check **Import with overwrite** to overwrite an existing Policy file automatically.

4. Click the **Import** button.

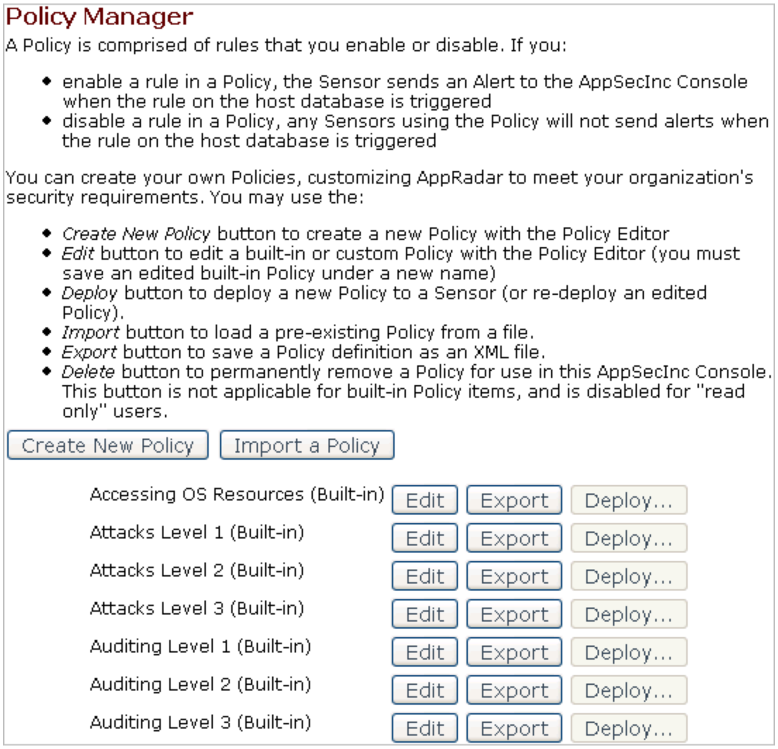
DbProtect Audit and Threat Management imports your Policy.

Exporting a Policy

You can **export** an Policy file (in XML format).

To export a Policy:

1. Do one of the following to display the **Policy Manager** page:
   - Click the **Policies** workflow link on the **Home** page.
   - Click the **Policies** tab from anywhere on the page.



Policy Manager

A Policy is comprised of rules that you enable or disable. If you:

- enable a rule in a Policy, the Sensor sends an Alert to the AppSecInc Console when the rule on the host database is triggered
- disable a rule in a Policy, any Sensors using the Policy will not send alerts when the rule on the host database is triggered

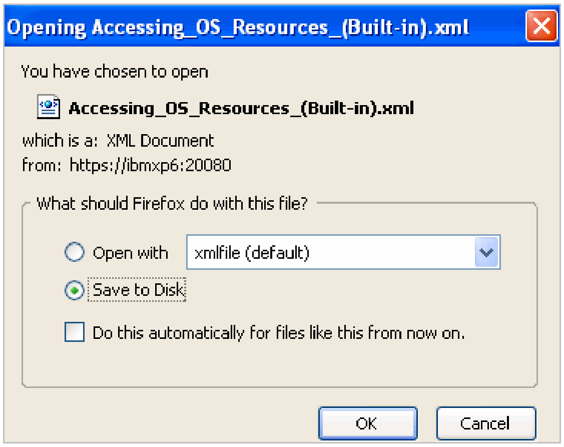
You can create your own Policies, customizing AppRadar to meet your organization's security requirements. You may use the:

- *Create New Policy* button to create a new Policy with the Policy Editor
- *Edit* button to edit a built-in or custom Policy with the Policy Editor (you must save an edited built-in Policy under a new name)
- *Deploy* button to deploy a new Policy to a Sensor (or re-deploy an edited Policy).
- *Import* button to load a pre-existing Policy from a file.
- *Export* button to save a Policy definition as an XML file.
- *Delete* button to permanently remove a Policy for use in this AppSecInc Console. This button is not applicable for built-in Policy items, and is disabled for "read only" users.

Create New Policy
Import a Policy
Accessing OS Resources (Built-in) Edit Export Deploy...
Attacks Level 1 (Built-in) Edit Export Deploy...
Attacks Level 2 (Built-in) Edit Export Deploy...
Attacks Level 3 (Built-in) Edit Export Deploy...
Auditing Level 1 (Built-in) Edit Export Deploy...
Auditing Level 2 (Built-in) Edit Export Deploy...
Auditing Level 3 (Built-in) Edit Export Deploy...

2. Click the **Export** button next to the Policy you want to export.

The **Open <Policy Name>.xml** dialog box displays.



Opening Accessing_OS_Resources_(Built-in).xml

You have chosen to open

Accessing_OS_Resources_(Built-in).xml

which is a: XML Document

from: https://ibmxp6:20080

What should Firefox do with this file?

○ Open with xmlfile (default)

● Save to Disk

□ Do this automatically for files like this from now on.

FIGURE: **Open <Policy Name>.xml** dialog box

3. Select **Save to Disk** (default).

Caution! Do **not** select **Open With**.

4. Click the **OK** button.

DbProtect Audit and Threat Management exports your Policy to the desktop (or other location specified, depending on your browser) as an XML file.

Deploying a Policy

After creating or editing a Policy, you can **deploy** it to a Sensor in order for it to take effect. You can deploy Policies to Sensors:

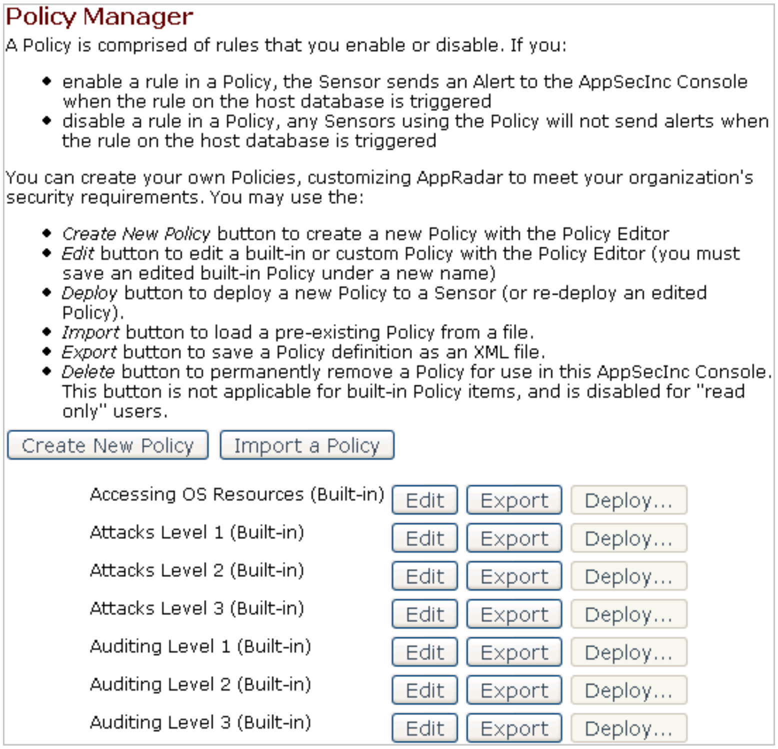
- during Sensor configuration and deployment; for more information, see *Configuring a Sensor and deploying the configuration information*
- from the **Policy Manager** (explained below).

Note: Deploying a Policy via the **Policy Manger** allows you to deploy Policies to **multiple** instances simultaneously, which may (or may not) be monitored by the same Sensor.

Caution! If you installed a host-based Sensor for Oracle to monitor Oracle databases on an Oracle RAC, you must deploy the exact same Policy for each host-based Sensor for Oracle (otherwise, you may get inconsistent results for the Alerts you are expecting to see). For more information, see ***Appendix C: Installing and Configuring a Host-Based Sensor for Oracle to Monitor Oracle Databases on an Oracle RAC***.

To deploy a Policy:

1. Do one of the following to display the **Policy Manager** page:
   - Click the **Policies** workflow link on the **Home** page.
   - Click the **Policies** tab from anywhere on the page.



Policy Manager

A Policy is comprised of rules that you enable or disable. If you:

- enable a rule in a Policy, the Sensor sends an Alert to the AppSecInc Console when the rule on the host database is triggered
- disable a rule in a Policy, any Sensors using the Policy will not send alerts when the rule on the host database is triggered

You can create your own Policies, customizing AppRadar to meet your organization's security requirements. You may use the:

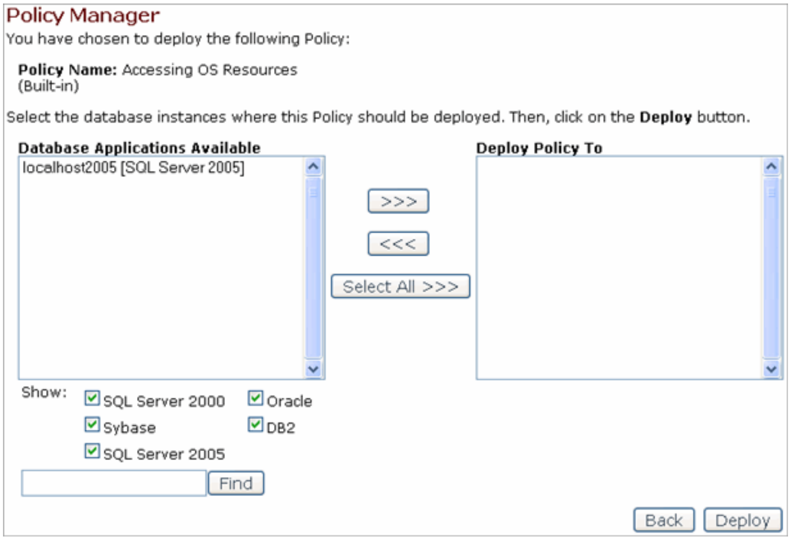
- *Create New Policy* button to create a new Policy with the Policy Editor
- *Edit* button to edit a built-in or custom Policy with the Policy Editor (you must save an edited built-in Policy under a new name)
- *Deploy* button to deploy a new Policy to a Sensor (or re-deploy an edited Policy).
- *Import* button to load a pre-existing Policy from a file.
- *Export* button to save a Policy definition as an XML file.
- *Delete* button to permanently remove a Policy for use in this AppSecInc Console. This button is not applicable for built-in Policy items, and is disabled for "read only" users.

Accessing OS Resources (Built-in)
Attacks Level 1 (Built-in)
Attacks Level 2 (Built-in)
Attacks Level 3 (Built-in)
Auditing Level 1 (Built-in)
Auditing Level 2 (Built-in)
Auditing Level 3 (Built-in)

FIGURE: Policy Manager

2. Click the **Deploy...** button next to the Policy you want to deploy to a Sensor.

A list of your registered Sensors displays. If no Sensors display, you need to configure and deploy a Sensor first; for more information, see *Configuring a Sensor and deploying the configuration information*.



Policy Manager

You have chosen to deploy the following Policy:

Policy Name: Accessing OS Resources (Built-in)

Select the database instances where this Policy should be deployed. Then, click on the **Deploy** button.

Database Applications Available

localhost2005 [SQL Server 2005]

Deploy Policy To

Show: ☑ SQL Server 2000 ☑ Oracle ☑ Sybase ☑ DB2 ☑ SQL Server 2005

FIGURE: Policy Manager

Two scroll-down boxes display:

- **Database Applications Available**
- **Deploy Policy To**.

These scroll-down boxes allow you to select database SIDs or instances where Sensors are registered, and deploy Policies for the Sensors to monitor.

You can also:

- check which database platforms your Policy should apply to (i.e., **SQL Server**, **Oracle**, **Sybase**, **DB2**) in the **Show:** portion of the page
- move database SIDs or instances from the **Database Applications Available** scroll-down box to the **Deploy Policy To** scroll-down box, and vice versa, by highlighting the database SID or instance and clicking either the **<<<** or **>>>** button.

  Clicking the >>> button *adds* the highlighted database SID or instance *to* the list of database SIDs or instances to be updated. Clicking the <<< button *removes* the highlighted database SID or instance *from* the list of database SIDs or instances to be updated.

Hint: Press <SHIFT> to highlight multiple consecutive database SIDs or instances. Press <CTRL> to highlight multiple non-consecutive database SIDs or instances.

- enter a Sensor name the find field, then click the **Find** button to display any Sensors with matching values.

3. Click the **Deploy** button.

DbProtect Audit and Threat Management deploys the Policy to the selected Sensor. The Sensor will fire Alerts whenever conditions in the Policy are met (**except** when a Rule or condition is filtered; for more information, see *What is a Filter?*).

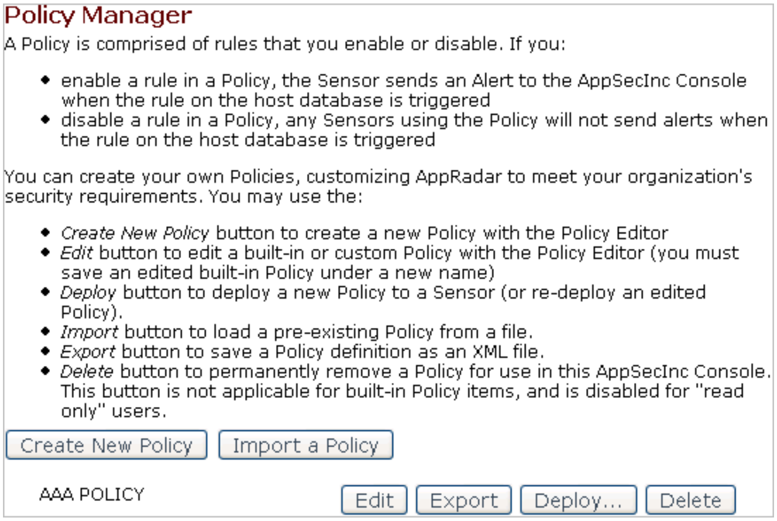
Deleting a Policy

You can only **delete** a custom Policy. You **cannot** delete built-in Policies or *any* deployed Policies (whether built-in or custom).

To delete a custom Policy:

1. Do one of the following to display the **Policy Manager** page:

- Click the **Policies** workflow link on the **Home** page.
- Click the **Policies** tab from anywhere on the page.



Policy Manager

A Policy is comprised of rules that you enable or disable. If you:

- enable a rule in a Policy, the Sensor sends an Alert to the AppSecInc Console when the rule on the host database is triggered
- disable a rule in a Policy, any Sensors using the Policy will not send alerts when the rule on the host database is triggered

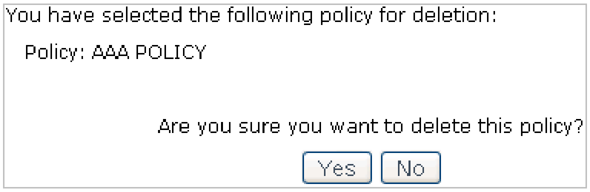
You can create your own Policies, customizing AppRadar to meet your organization's security requirements. You may use the:

- *Create New Policy* button to create a new Policy with the Policy Editor
- *Edit* button to edit a built-in or custom Policy with the Policy Editor (you must save an edited built-in Policy under a new name)
- *Deploy* button to deploy a new Policy to a Sensor (or re-deploy an edited Policy).
- *Import* button to load a pre-existing Policy from a file.
- *Export* button to save a Policy definition as an XML file.
- *Delete* button to permanently remove a Policy for use in this AppSecInc Console. This button is not applicable for built-in Policy items, and is disabled for "read only" users.

FIGURE: Policy Manager

2. Click the **Delete** button next to the custom Policy you want to delete.

The next page prompts you to confirm the delete.



You have selected the following policy for deletion:

Policy: AAA POLICY

Are you sure you want to delete this policy?

FIGURE: **Policy Manager**

3. Click the **Yes** button.

Your custom Policy is deleted from the **Policy Manager** list of built-in and custom Policies.

Policy Editor rule categories

Note: You can deploy a Sensor on a database host (for Oracle and SQL Server), or on another host that monitors network traffic to/from the database (for Oracle, Sybase, and DB2). You can activate most Rules for host- and network-based Sensors. However, certain Rules *only* work for network-based Sensors. Network-based only Rules are denoted in the Policy Editor.

Rules in the **Policy Editor** (which apply to SQL Server, Oracle, Sybase, and DB2 Rules) are divided into the following **Rule categories**:

- **Accessing OS Resources.** An important aspect of application security is ensuring the integrity of the operating system (OS) on which the application resides. These Rules monitor for OS access via database controls.
- **Audit Events.** These Rules allow Sensors to log the execution of database queries regardless of threat level. This provides administrators full awareness of what has been executed in the database, when, by whom, and where. Essentially, this is a category of events that can provide an audit trail of all database activity with "real-time" alerting on changes or key events. This functionality is provided without any impact on performance and with no modifications to the application or underlying database.
- **Buffer Overflow.** Buffer overflows can cause a database server to crash, or cause the memory in the stack to be overwritten (including the return address of the calling function). This can result in an Exception being thrown. These Rules focus on this type of attack and Alerts are fired if the Sensor sees the attack pattern being executed. For example: SQL Server provides a built-in function called `BULK INSERT` which allows data to be uploaded from a file directly to a table. The function `BULK INSERT` does not properly allocate enough memory when called with a long string as the name of the file from which to load. This can cause the stack to be overwritten and allows an attacker to inject executable code onto the stack.

- **Miscellaneous.** These Rules include attacks and events that do not necessarily fall within any of the other provided Rule categories.
- **Password Attacks.** Attempts to guess passwords by trying likely combinations of characters or exploiting certain vulnerabilities are simplistic attacks that can be used against a database. For example, one method of breaking into a database is to script a password attack on that database. This attack involves using a dictionary of usernames and passwords to attempt to log into the database. When performed using a script, a large number of passwords can be attempted rapidly. This can be an effective strategy for an attacker to break into a database. DbProtect Audit and Threat Management is designed to handle scripted password attacks and can be configured to send out a notification whenever it detects 100 failed login attempts within one minute.
- **Privilege Escalation.** Access controls deal with determining which users are allowed to perform what actions. Access controls are designed to restrict users from performing tasks they are not authorized to perform. These Rules check for attempts to exploit known vulnerabilities to achieve privilege escalation.
- **Security Tools.** DbProtect Audit and Threat Management can detect various tools that scan the database. Although these tools may not be inherently malicious, it can be helpful to know who is running these tools, when, and against which database.
- **Web Application Attacks.** These Rules can be enabled to monitor against possible access-related attacks. Attacks may include attempts to elevate privileges and gain access to powerful resources within a database. SQL injection attack Rules can also be set within the Web Application Attacks category. SQL Injection occurs when an attacker is “injecting” or manipulating SQL code. By adding unexpected SQL to a query, an attacker is able to manipulate a database in many unanticipated ways. For example, one common technique used to detect a SQL injection vulnerability is to insert a single quote and observe the results for an error message. If unmatched single quotes are found in SQL statements being executed by the web application, it may be an attacker searching for SQL injection vulnerabilities.
- **User-Defined Filters.** User-Defined Filters are divided into the following three categories:

  -**User-Defined Security Filters**, i.e., Filters created either via the **Audit Filter Wizard** or **Advanced Filter and Exceptions Editor** that have a **Risk Level** higher than **Informational**); for more information, see *Working with the Audit Filter Wizard* and *Working with the Advanced Filter and Exception Editor*, respectively

  -**User Defined Audits**, i.e., Filters created either via the **Audit Filter Wizard** or **Advanced Filter and Exceptions Editor** that have a **Risk Level** of **Informational**); for more information, see *Working with the Audit Filter Wizard* and *Working with the Advanced Filter and Exception Editor*, respectively

  -**User-Defined Exceptions**, i.e., Filters created either via the **Exception Wizard** or the **Advanced Filter and Exceptions Editor** that prohibit an Alert from firing under certain circumstances; for more information, see *Working with the Exception Wizard* and *Working with the Advanced Filter and Exception Editor*, respectively.

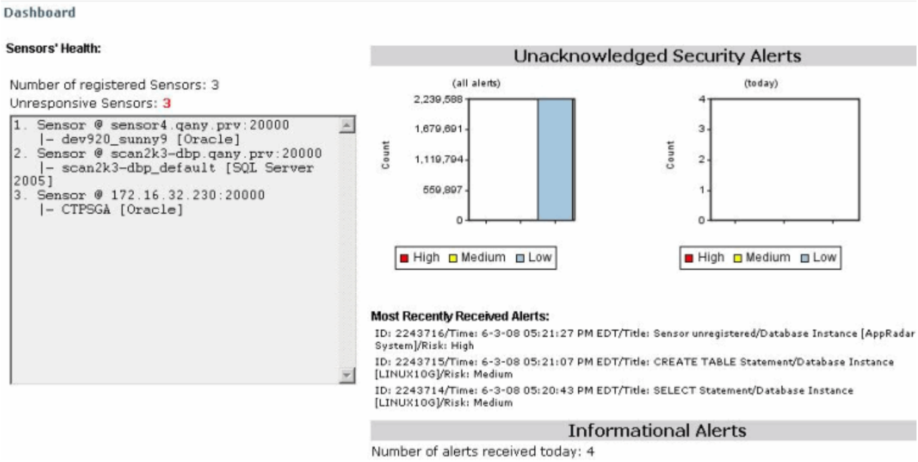
Dashboard

This chapter consists of the following topics:

- *Understanding the Dashboard*
- *Monitoring Alerts (via the Dashboard)*
- *Monitoring the "health" of your Sensors (via the Dashboard).*

Understanding the Dashboard

The **Dashboard** is shown below.



Dashboard

Sensors' Health:

Number of registered Sensors: 3
Unresponsive Sensors: 3

```
1. Sensor @ sensor4.qany.prv:20000
   |- dev920_sunny9 [Oracle]
2. Sensor @ scan2k3-dbp.qany.prv:20000
   |- scan2k3-dbp_default [SQL Server
2005]
3. Sensor @ 172.16.32.230:20000
   |- CTPSGA [Oracle]
```

Unacknowledged Security Alerts

Most Recently Received Alerts:

ID: 2243716/Time: 6-3-08 05:21:27 PM EDT/Title: Sensor unregistered/Database Instance [AppRadar System]/Risk: High

ID: 2243715/Time: 6-3-08 05:21:07 PM EDT/Title: CREATE TABLE Statement/Database Instance [LINUX10G]/Risk: Medium

ID: 2243714/Time: 6-3-08 05:20:43 PM EDT/Title: SELECT Statement/Database Instance [LINUX10G]/Risk: Medium

Informational Alerts

Number of alerts received today: 4

FIGURE: Dashboard

The **Dashboard** provides a graphical, high-level summary of Alerts, audits, and total Alert volume. You can also monitor the "health" of your registered Sensors from the Dashboard. For more information, see *Monitoring, filtering, acknowledging, and archiving Alerts (via the Alert Manager)* and *Monitoring the "health" of your Sensors (via the Dashboard)*, respectively.

Monitoring Alerts (via the Dashboard)

DbProtect Audit and Threat Management receives Alerts from the registered Sensors. The **Dashboard** provides a graphical, high-level summary of unacknowledged Alerts, audit events (i.e., Informational Alerts), most recently received Alerts, and total Alert volume. The **Dashboard** automatically refreshes itself every 30 seconds to update the display of new, real-time Alerts.

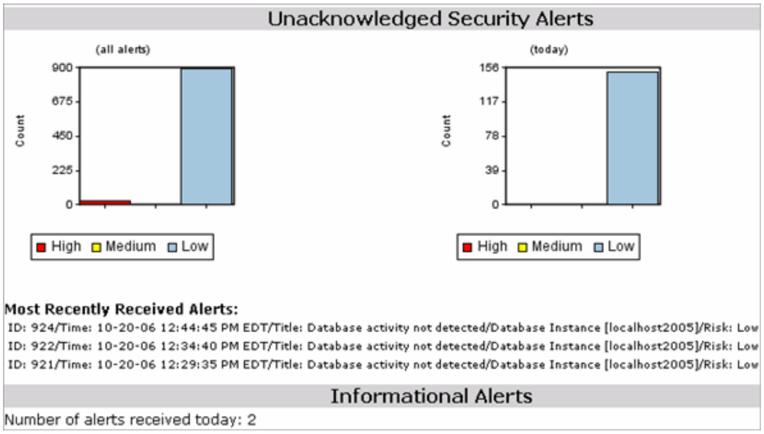
Caution! When you have not used DbProtect Audit and Threat Management for a while, your Session normally times out. However, on certain pages, it does **not**. Specifically, DbProtect Audit and Threat Management does **not** time out on the **Alert Manager**, the **Dashboard**, and the **ASAP Update** portion of the **Sensor Manager**.

To monitor Alerts (via the **Dashboard**):

1. Do one of the following to display the **Dashboard**:

- Click the **Dashboard - Graphical Summary** workflow link on **Home** page.
- Click the **Dashboard** tab from anywhere on the page.

The unacknowledged Alerts portion of the **Dashboard** displays your unacknowledged Alerts (all Alerts and today's Alerts), most recently received Alerts, and audit events (i.e., Informational Alerts).



Most Recently Received Alerts:

ID: 924/Time: 10-20-06 12:44:45 PM EDT/Title: Database activity not detected/Database Instance [localhost2005]/Risk: Low

ID: 922/Time: 10-20-06 12:34:40 PM EDT/Title: Database activity not detected/Database Instance [localhost2005]/Risk: Low

ID: 921/Time: 10-20-06 12:29:35 PM EDT/Title: Database activity not detected/Database Instance [localhost2005]/Risk: Low

Informational Alerts

Number of alerts received today: 2

FIGURE: **Dashboard** (Alert portion)

2. Your **Dashboard** options follow. If you want to view your:

- **unacknowledged Alerts**, then go to Step 3
- **most recently received Alerts**, then go to Step 4
- **Informational Alerts**, then go to Step 5.

3. To view your unacknowledged Alerts.

The color-coded graphs in the unacknowledged Alerts portion of the **Dashboard** display your unacknowledged **High**, **Medium**, and **Low** risk Alerts (i.e., all Alerts and today's Alerts).

Note: For more information, see *What do the risk levels mean?*

4. To view your most recently-received Alerts.

The most recently-received Alerts portion of the **Dashboard** displays your unacknowledged **High**, **Medium**, and **Low** risk Alerts (i.e., all Alerts and for today only).

Note: For more information, see *What do the risk levels mean?*

5. To view your Informational Alerts.

The bottom portion of the **Dashboard** displays the number of Informational (audit) Alerts received today.

Note: For more information, see *What do the risk levels mean?*

Monitoring the "health" of your Sensors (via the Dashboard)

You can monitor the "health" of your registered Sensors via the **Sensor Manager** and the **Dashboard**. If you're not receiving Alerts, it **could** be because your registered Sensor is "unhealthy". A "healthy" Sensor is:

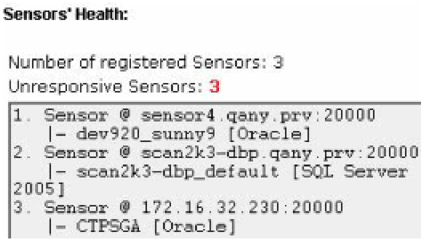
- **"up and running"** on the database SID or instance where it is registered
- **actively collecting/interpreting data and firing Alerts** to DbProtect Audit and Threat Management in accordance with its deployed Policies.

For more information, see the *DbProtect Administrator's Guide*.

To monitor the "health" of your Sensors via the **Dashboard**:

1. Do one of the following to display the **Dashboard**:
   - Click the **Dashboard - Graphical Summary** workflow link on **Home** page.
   - Click the **Dashboard** tab from anywhere on the page.

The Sensor "health" portion of the **Dashboard** displays your registered Sensors.



Sensors' Health:

Number of registered Sensors: 3
Unresponsive Sensors: 3

```
1. Sensor @ sensor4.qany.prv:20000
   |- dev920_sunny9 [Oracle]
2. Sensor @ scan2k3-dbp.qany.prv:20000
   |- scan2k3-dbp_default [SQL Server
2005]
3. Sensor @ 172.16.32.230:20000
   |- CTPSGA [Oracle]
```

FIGURE: **Dashboard** (Sensor "health" portion)

2. The **Sensor “health”** portion of the **Dashboard** allows you to view the:

- **Number of registered Sensors**
- **Unresponsive Sensors**.

An unresponsive Sensor is “unhealthy”; for more information, see the *DbProtect Administrator’s Guide*.

Filters

This chapter consists of the following topics:

- *What is a Filter?*
- *What are Global Filters and Global Exceptions?*
- *Understanding the Filter Manager*
- *Working with the Audit Filter Wizard*
- *Working with the Exception Wizard*
- *Working with the Advanced Filter and Exception Editor*
- *Writing expressions*
- *Joining expressions*
- *Editing a Filter*
- *Deleting a Filter*
- *Importing a Filter*
- *Exporting a Filter*.

What is a Filter?

This topic explains:

- *What do Filters do?*
- *Working with Filters*
- *Important column-level considerations for Filters and Exceptions*.

WHAT DO FILTERS DO?

Filters are custom Rules created for:

- auditing database activity
- inhibiting output of another Rule
- monitoring database activity in ways not provided for in the DbProtect Audit and Threat Management built-in Rules.

Like a built-in Rule, you can add a Filter to a Policy and, subsequently, deploy it to a Sensor.

Caution! Filters are only active when you include them in a Policy, then deploy the Policy.

Note: When you import a Policy, it **must** include all Filters. If you import a Policy that includes custom Filters, the order of the Filters is significant. For more information, see *Importing a Policy*.

The **Filter Manager** allows you to create and edit Filters that customize the effect of built-in Rules and Policies to better suit individual security needs. For more information, see *Understanding the Filter Manager*.

WORKING WITH FILTERS

There are three ways to work with Filters:

- **Audit Filter Wizard.** Allows you to create audit Rules for system objects. You can monitor `SELECT`, `INSERT`, `UPDATE` and `DELETE` activity against system and user tables in any database, and monitor the execution of stored procedures and functions; for more information, see *Working with the Audit Filter Wizard*.

  Example: The built-in Rule **User-table SELECT** generates an audit event any time a SQL query is executed against a user table. This audit Rule may result in a significant amount of data -- perhaps more than is required or really useful. Perhaps you only need to monitor a few database tables with this Rule. In other words, you don't want to deactivate the Rule -- but you want to limit its scope.

  Solution: Use the **Audit Filter Wizard** to restrict auditing to only the user tables you specify. (You can even design the Filter to monitor specific columns in the tables.)
- **Exception Wizard.** Allows you to create criteria to suppress built-in Rules from triggering. Exceptions are useful because they can reduce the volume of unremarkable Alerts and audits sent to DbProtect Audit and Threat Management and log file, respectively. For more information, see *Working with the Exception Wizard*.

  Examples: Consider the auditing event **drop table**. Your company requires you to audit the integrity of the database, but periodically maintenance is performed using the well-known **sa** account. By creating an Exception Filter when the account is `sa`, those **drop table** events will **not** be reported to DbProtect Audit and Threat Management.

  Or, assume you want to allow machine ABC to run `xp_cmdshell`, and **not** fire an Alert for the check **Generic use of xp_cmdshell**. You can enable the Rule and create an Exception for the **Source of Attack**, i.e., machine ABC.

  The Exception Wizard also allows you to create **Global Filters**. Global Exceptions allow you to monitor all database activity (for a selected database type), and configure DbProtect Audit and Threat Management **not** to fire Alerts when certain criteria are met. For more information, see *What are Global Filters and Global Exceptions?*

- **Advanced Filter and Exception Editor.** Allows you to customize any built-in Rule or create new ones. It contains a flexible expression editor for creating arbitrarily complex Rules; for more information, see *Working with the Advanced Filter and Exception Editor*.

  Example: The Rule **Accessing list of logins** monitors the system table (**sysxlogins**) which contains the list of valid logins and password hashes for the database server. Attempts to access this data may indicate an attacker is trying to access the table information. In some cases, however, it is legitimate for an account to access the **sysxlogins** table. For instance, the application **BILL SYSTEM** is configured to access the **sysxlogins** table as part of its normal operations. However, this is the only system authorized to perform such a function.

  To monitor the **sysxlogins** table for unauthorized access -- with the exception of the **BILL SYSTEM** application -- you can create a Filter to notify you when *any* application *except* **BILL SYSTEM** is not accessing the **sysxlogins** table. You can add criteria to the Rule with the following expression: `Application is not equal to "BILL SYSTEM"`

  The Advanced Filter and Exception Editor also allows you to create **Global Filters** and **Global Exceptions**. Global Filters allow you to monitor all database activity (for a selected database type), and configure DbProtect Audit and Threat Management to fire Alerts only when certain criteria are met. **Global Exceptions**, on the other hand, allow you to monitor all database activity (for a selected database type), and configure DbProtect Audit and Threat Management **not** to fire Alerts when certain criteria are met. For more information, see *What are Global Filters and Global Exceptions?*

For advice (and an example) on writing XML Rules in **Advanced Filter Editor**, see *Writing expressions*.

IMPORTANT COLUMN-LEVEL CONSIDERATIONS FOR FILTERS AND EXCEPTIONS

DbProtect Audit and Threat Management allows you to select multiple columns when you define a Filter or an Exception. If you are defining:

- a Filter, and *any* of the selected columns are found in the query, then the Rule will fire. This includes the `*` wild card, which includes *all* columns.
- an Exception, and if *any* of the selected columns are found in the query, then the Rule will **not** fire. This includes the `*` wild card, which includes *all* columns.

Note: DbProtect Audit and Threat Management also supports filtering at the row level with the application of custom Filters. For assistance with customizing this feature, email Application Security, Inc. Support at `support@appsecinc.com`.

What are Global Filters and Global Exceptions?

There may be cases when you do not want to monitor database activity related to a specific Rule, but rather you want to monitor all database activity, in special cases. This can be done in DbProtect Audit and Threat Management using either Global Filters or Global Exceptions.

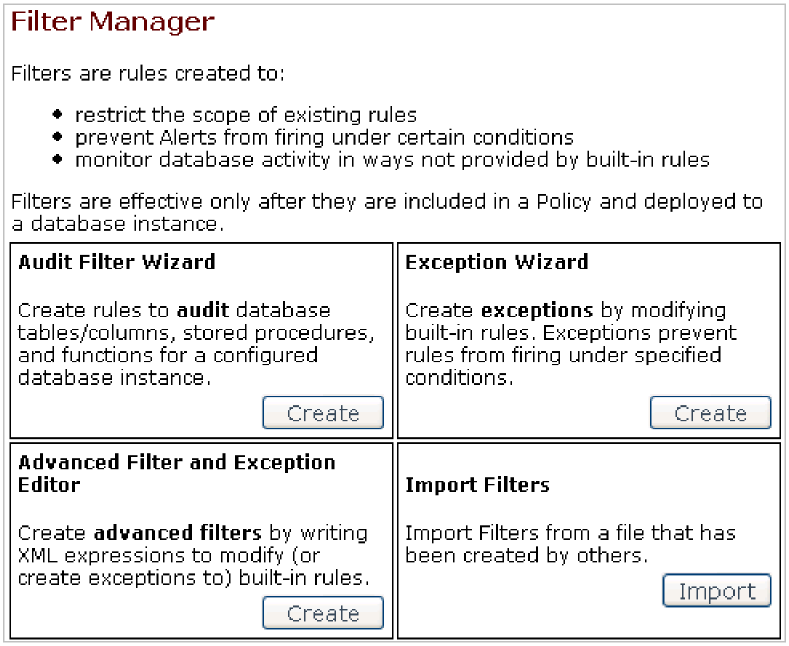
Global Filters allow you to monitor all database activity (for a selected database type), and configure DbProtect Audit and Threat Management to fire Alerts only when certain criteria are met. **Global Exceptions**, on the other hand, allow you to monitor all database activity (for a selected database type), and configure DbProtect Audit and Threat Management **not** to fire Alerts when certain criteria are met.

You can only create Global Filters using the **Advanced Filter and Exception Editor**. However, both the **Exception Wizard** and the **Advanced Filter and Exception Editor** allow you to create Global Exceptions. For more information on:

- creating Global Filters with the **Advanced Filter and Exception Editor**, see *Working with the Advanced Filter and Exception Editor*
- creating Global Exceptions with the **Exception Wizard** and the **Advanced Filter and Exception Editor**, see and *Working with the Exception Wizard* and *Working with the Advanced Filter and Exception Editor*, respectively.

Understanding the Filter Manager

The **Filter Manager** is shown below.



Filter Manager

Filters are rules created to:

- restrict the scope of existing rules
- prevent Alerts from firing under certain conditions
- monitor database activity in ways not provided by built-in rules

Filters are effective only after they are included in a Policy and deployed to a database instance.

Audit Filter Wizard

Create rules to **audit** database tables/columns, stored procedures, and functions for a configured database instance.

Exception Wizard

Create **exceptions** by modifying built-in rules. Exceptions prevent rules from firing under specified conditions.

Advanced Filter and Exception Editor

Create **advanced filters** by writing XML expressions to modify (or create exceptions to) built-in rules.

Import Filters

Import Filters from a file that has been created by others.

FIGURE: **Filter Manager** page

The **upper portion** of the **Filter Manager** allows you to:

- create Filters and Exceptions using the **Audit Filter Wizard**, the **Exception Wizard**, and the **Advanced Filter and Exception Editor**; for more information, see *What is a Filter?*
- import a Filter; for more information, see *Importing a Filter*.

The lower (**My Filters**) portion of the **Filter Manager** page:

- displays your existing Filters, including the name and the risk level assigned during Filter creation
- allows you to edit or delete any displayed Filter; for more information, see *Editing a Filter* and *Deleting a Filter*, respectively.

Working with the Audit Filter Wizard

The **Audit Filter Wizard** allows you to create audit Rules for system objects. You can monitor `SELECT`, `INSERT`, `UPDATE` and `DELETE` activity against system and user tables in any database, and monitor the execution of stored procedures and functions.

This topic consists of the following sub-topics:

- *Oracle DBA considerations*
- *DB2 DBA considerations (for network-based Sensors for DB2)*
- *DB2 DBA considerations (for host-based Sensors for DB2)*
- *Sybase DBA considerations*
- *Creating a Filter with the Audit Filter Wizard.*

ORACLE DBA CONSIDERATIONS

If you are using a **host- or network-based Sensor for Oracle on Windows** for Activity Monitoring and Auditing, and you want to use Filters, then you **must** enter an Oracle user name and password during Sensor registration and configuration; for more information on configuring a:

- **host-based Sensor for Oracle on Windows**, see *Configuring a host-based Sensor to monitor Oracle SIDs and services and deploying the configuration information (when Sensor is installed on a *nix-based operating system).*
- **network-based Sensor for Oracle on Windows**, see *Configuring a network-based Sensor to monitor Oracle SIDs and services and deploying the configuration information (when Sensor is installed on Windows).*

The user name/password pair is **not** used to monitor your database. The pair is only used by the **Audit Filter Wizard** to collect object information from the database.

Note: This requirement does **not** apply to host-based Sensors for Oracle on *nix platforms for Activity Monitoring and Auditing. For these types of Sensors, the account running the Sensor process should have the same primary group as the `oracle` account, and no further credentials should be necessary.

The host- or network-based Sensor for Oracle on Windows service account **must** be part of **both** the `administrator` and `ora_dba windows` groups.

The **Audit Filter Wizard** for Oracle does **not** require full DBA permissions. You only need to specify the following set of permissions:

- `SELECT on SYS.DBA_OBJECTS`
- `SELECT on SYS.DBA_TAB_COLUMNS`
- `SELECT on SYS.DBA_USERS`
- `SELECT on SYS.DBA_TABLES`
- `SELECT on SYS.DBA_VIEWS`
- `SELECT on SYS.DBA_SEQUENCES`

When you finish configuring DbProtect Activity Monitoring and Auditing and defining all Rules, you can re-configure your Sensors **without** an Oracle user name and password, then re-deploy the Sensors. For more information, see the *DbProtect Installation Guide*.

DB2 DBA CONSIDERATIONS (FOR NETWORK-BASED SENSORS FOR DB2)

If you're a DB2 DBA, and you plan to create a custom Filter for DB2, you must:

- install the appropriate DB2 administrative client drivers on the server where the network-based Sensor for DB2 resides
- catalog the DB2 client drivers to recognize the monitored DB2 database (either through Discovery or reference).

The reason you must catalog your monitored DB2 databases is so they will display in the Audit Filter Wizard; for more information, see *Creating a Filter with the Audit Filter Wizard*. In other words, you must make the client "aware" of these DB2 databases. With any client, you must always catalog the resources you're going to use, starting with a node (i.e., the server itself), then a database on the node to which you're connected.

The Audit Filter Wizard does not require full DBA permissions. However, a custom Filter for DB2 does require read access to the following tables:

- `sysibm.systables`
- `sysibm.syscolumns`
- `sysibm.sysroutines`

For more information on DB2 client driver installation, see "Appendix G: DB2 Administrative Client Driver Installation" in the *DbProtect Installation Guide*.

DB2 DBA CONSIDERATIONS (FOR HOST-BASED SENSORS FOR DB2)

The `DBADM` permissions required to run the host-based Sensor for DB2 (`SYSADM` if the `appradar` user wants to monitor failed logins) are sufficient to create a Filter with the Audit Filter Wizard. For more information, see the *DbProtect Installation Guide*.

SYBASE DBA CONSIDERATIONS

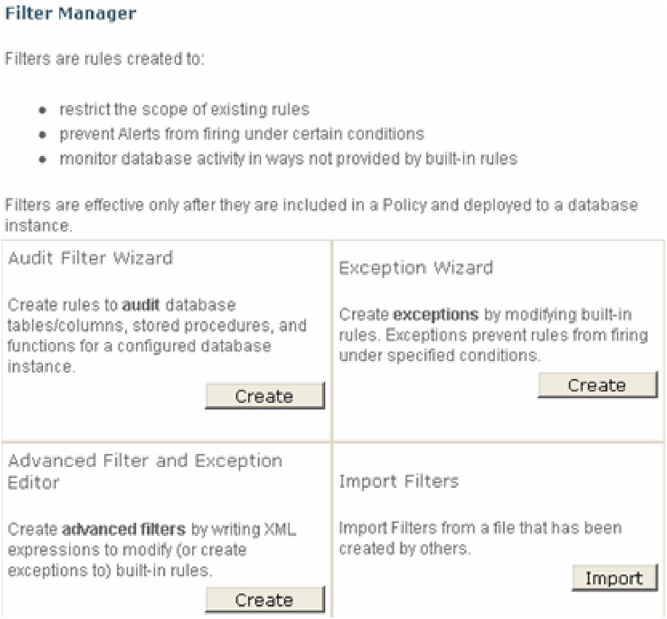
The **Audit Filter Wizard** for Sybase does **not** require full DBA permissions. You only require access to read the following tables: `master..sysdatabases` and the `sysobjects`, `sysusers`, and `syscolumns` tables in the target databases being Audited.

For more information, see the *DbProtect Installation Guide*.

CREATING A FILTER WITH THE AUDIT FILTER WIZARD

To create a Filter using the **Audit Filter Wizard**:

1. Do one of the following to display the **Filter Manager** page:
   - Click the **Filters** workflow link on the **Home** page.
   - Click the **Filters** tab from anywhere on the page.



Filter Manager

Filters are rules created to:

- restrict the scope of existing rules
- prevent Alerts from firing under certain conditions
- monitor database activity in ways not provided by built-in rules

Filters are effective only after they are included in a Policy and deployed to a database instance.

Audit Filter Wizard

Create rules to **audit** database tables/columns, stored procedures, and functions for a configured database instance.

Exception Wizard

Create **exceptions** by modifying built-in rules. Exceptions prevent rules from firing under specified conditions.

Advanced Filter and Exception Editor

Create **advanced filters** by writing XML expressions to modify (or create exceptions to) built-in rules.

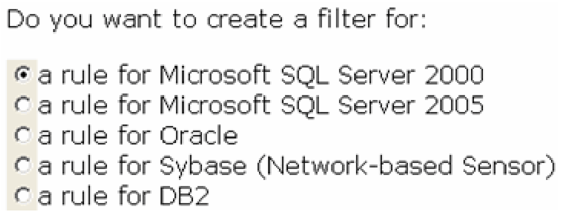
Import Filters

Import Filters from a file that has been created by others.

FIGURE: Filter Manager

2. Click the **Create** button in the **Audit Filter Wizard** portion of the page.

The first **Audit Filter Wizard** page displays.



Do you want to create a filter for:

● a rule for Microsoft SQL Server 2000
○ a rule for Microsoft SQL Server 2005
○ a rule for Oracle
○ a rule for Sybase (Network-based Sensor)
○ a rule for DB2

FIGURE: **Audit Filter Wizard**

3. Select whether you want to create a Rule for:

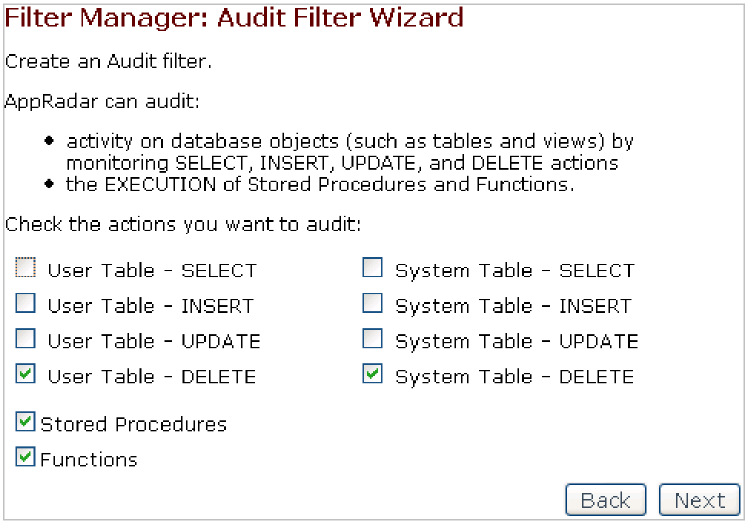
- **Microsoft SQL Server 2000** (host-based Sensor)
- **Microsoft SQL Server 2005** (host-based Sensor)
- **Microsoft SQL Server 2008** (host-based Sensor)
- **Oracle** (host-based or network-based Sensor)
- **Sybase** (network-based Sensor)
- **DB2** (host-based or network-based Sensor).

Note: If you're a DB2 DBA, and you have a network-based Sensor for DB2 installed, and you plan to create a custom Filter for DB2, then you must: a.) install the appropriate DB2 administrative client drivers on the server where the network-based Sensor for DB2 resides; b.) catalog the DB2 client drivers to recognize the monitored DB2 database (either through Discovery or reference).

You must catalog your monitored DB2 databases so they will display in the Audit Filter Wizard. In other words, you must make the client "aware" of these DB2 databases. With any client, you must always catalog the resources you're going to use, starting with a node (i.e., the server itself), then a database on the node to which you're connected. For more information on DB2 client driver installation, see "Appendix G: DB2 Administrative Client Driver Installation" in the *DbProtect Installation Guide*.

4. Click the **Next** button.

The next **Audit Filter Wizard** page displays.



Filter Manager: Audit Filter Wizard

Create an Audit filter.

AppRadar can audit:

- activity on database objects (such as tables and views) by monitoring SELECT, INSERT, UPDATE, and DELETE actions
- the EXECUTION of Stored Procedures and Functions.

Check the actions you want to audit:

□ User Table - SELECT	□ System Table - SELECT
□ User Table - INSERT	□ System Table - INSERT
□ User Table - UPDATE	□ System Table - UPDATE
☑ User Table - DELETE	☑ System Table - DELETE

☑ Stored Procedures

☑ Functions

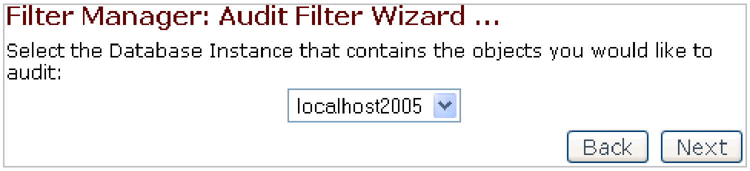
FIGURE: Audit Filter Wizard

5. Check the action(s) you want to audit. DbProtect Audit and Threat Management can audit:

- activity on **database objects** (such as tables and views) by monitoring `SELECT`, `INSERT`, `UPDATE`, and `DELETE` actions
- the `EXECUTION` of **stored procedures** and **functions**.

6. Click the **Next** button.

The next **Audit Filter Wizard** page displays.



Filter Manager: Audit Filter Wizard ...

Select the Database Instance that contains the objects you would like to audit:

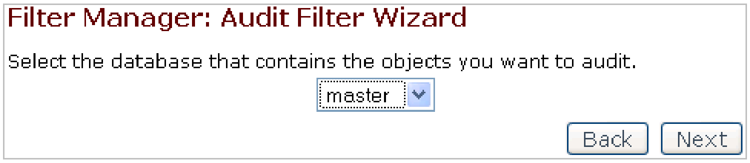
localhost2005

FIGURE: Audit Filter Wizard

7. Use the drop-down to select the alias name for the configured database instance or SID that contains the objects you want to audit.

8. Click the **Next** button.

The next **Audit Filter Wizard** page displays.



Filter Manager: Audit Filter Wizard

Select the database that contains the objects you want to audit.

FIGURE: Audit Filter Wizard

9. Use the drop-down to select the database you want to Audit.

To **create a custom Filter** for:

- **Oracle**, you must have the following privileges: `all_users`, `all_tables`, `all_tab_columns`, and `all_objects`
- **Sybase**, you require access to read the following tables: `master..sysdatabases` and the `sysobjects`, `sysusers`, and `syscolumns` tables in the target databases being Audited.
- **DB2**, you **must** install the appropriate DB2 administrative client drivers (for more information on DB2 client driver installation, see the *DbProtect Installation Guide*), and configure it to recognize the monitored database (either through Discovery or reference). Creating a custom Filter for DB2 also requires access to read the following tables:

  `-sysibm.systables`
  `-ysibm.syscolumns`
  `-sysibm.sysroutines`

For more information, see the "Rights" row in the *Creating a Filter with the Audit Filter Wizard* table.

10. Click the **Next** button.

The next **Audit Filter Wizard** page displays. Up to three portions of the page display, depending on whether you selected to audit **database objects**, and/or the `EXECUTION` of **stored procedures** and/or **functions** in Step 5.

If you selected to audit:

- **database objects** in Step 5, then go to Step 11
- **stored procedures** in Step 5, then go to Step 12
- **functions** in Step 5, then go to Step 13.

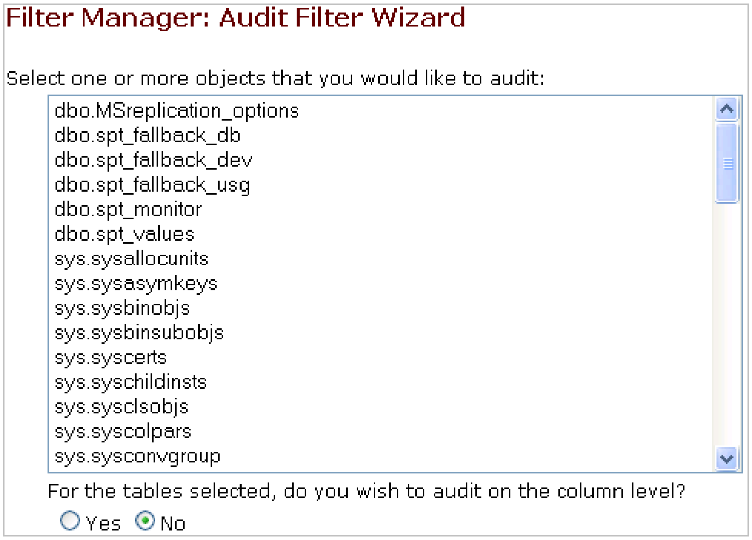
11. If you selected to audit **database objects** in Step 5, then the **Audit Filter Wizard** page allows you to:

- use the scroll-down box to highlight one or more database objects you want to audit

Hint: Press <SHIFT> to highlight multiple consecutive objects. Press <CTRL> to highlight multiple non-consecutive objects.

- select whether you want to audit the selected database objects at the column level (**Yes** or **No**).

Note: DbProtect Audit and Threat Management allows you to select multiple columns when you define a Filter or an Exception. If you are defining a Filter, and the selected columns are found in a query, then the Rule will fire. For more information, see *Important column-level considerations for Filters and Exceptions*.



Filter Manager: Audit Filter Wizard

Select one or more objects that you would like to audit:

dbo.MSreplication_options
dbo.spt_fallback_db
dbo.spt_fallback_dev
dbo.spt_fallback_usg
dbo.spt_monitor
dbo.spt_values
sys.sysallocunits
sys.sysasymkeys
sys.sysbinobjs
sys.sysbinsubobjs
sys.syscerts
sys.syschildinsts
sys.sysclsobjs
sys.syscolpars
sys.sysconvgroup

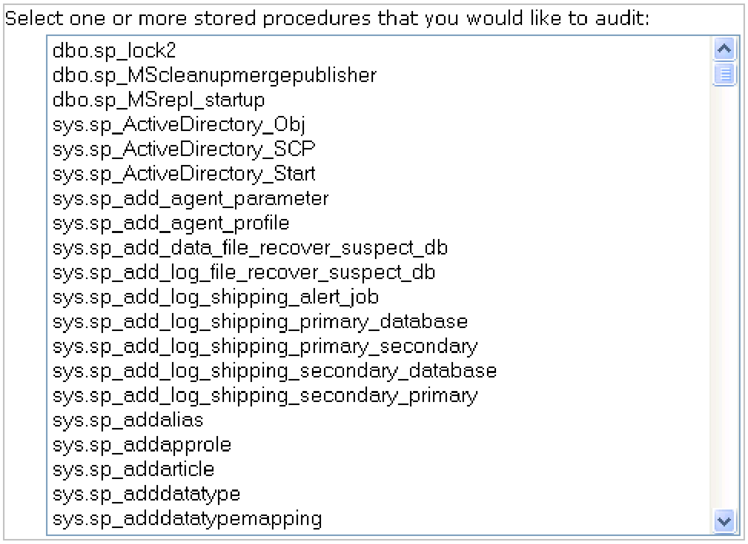
For the tables selected, do you wish to audit on the column level?

○ Yes ● No

FIGURE: Audit Filter Wizard

12. If you selected to audit stored procedures in Step 5, then the Audit Filter Wizard page allows you to use the scroll-down box to highlight one or more stored procedures you want to audit.

Hint: Press <SHIFT> to highlight multiple consecutive objects. Press <CTRL> to highlight multiple non-consecutive objects.



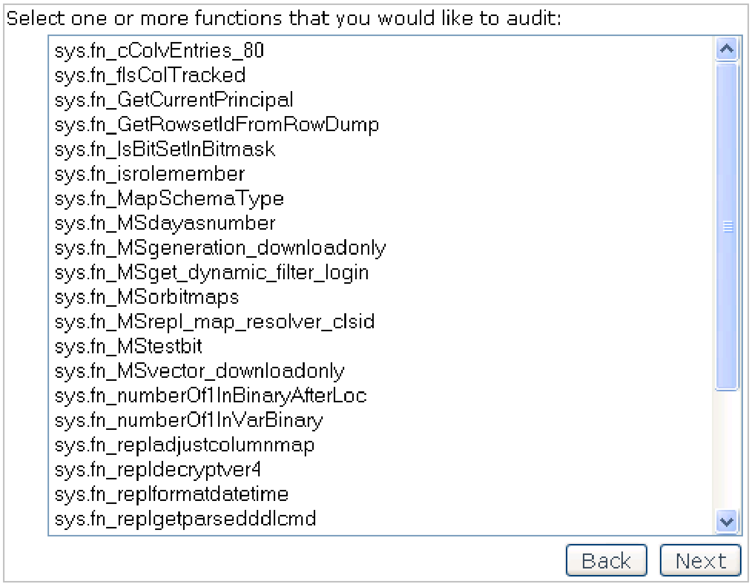
Select one or more stored procedures that you would like to audit:

dbo.sp_lock2
dbo.sp_MScleanupmergepublisher
dbo.sp_MSrepl_startup
sys.sp_ActiveDirectory_Obj
sys.sp_ActiveDirectory_SCP
sys.sp_ActiveDirectory_Start
sys.sp_add_agent_parameter
sys.sp_add_agent_profile
sys.sp_add_data_file_recover_suspect_db
sys.sp_add_log_file_recover_suspect_db
sys.sp_add_log_shipping_alert_job
sys.sp_add_log_shipping_primary_database
sys.sp_add_log_shipping_primary_secondary
sys.sp_add_log_shipping_secondary_database
sys.sp_add_log_shipping_secondary_primary
sys.sp_addalias
sys.sp_addapprole
sys.sp_addarticle
sys.sp_adddatatype
sys.sp_adddatatypemapping

FIGURE: Audit Filter Wizard

13. If you selected to audit **functions** in Step 5, then the **Audit Filter Wizard** page allows you to use the scroll-down box to highlight one or more functions you want to audit.

Hint: Press <SHIFT> to highlight multiple consecutive objects. Press <CTRL> to highlight multiple non-consecutive objects.



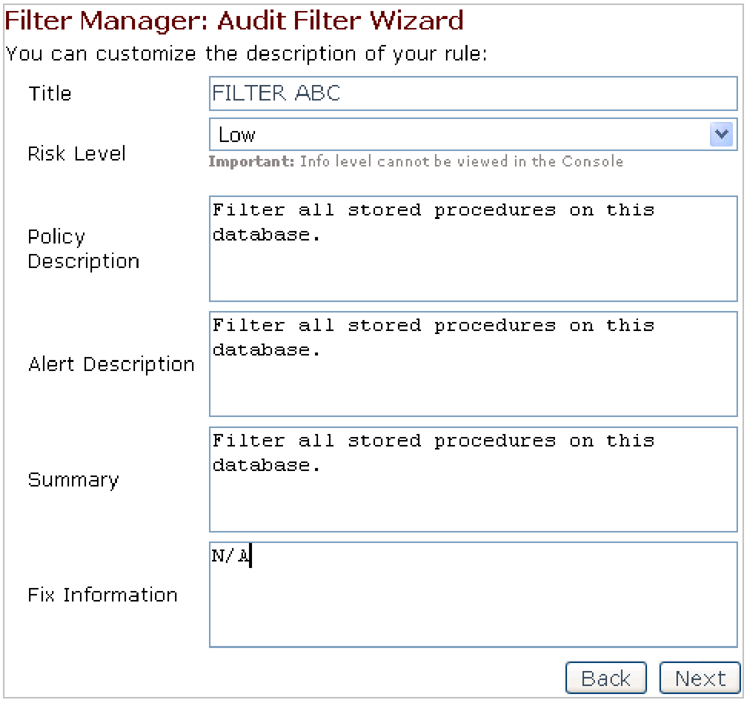
Select one or more functions that you would like to audit:

sys.fn_cColvEntries_80
sys.fn_fIsColTracked
sys.fn_GetCurrentPrincipal
sys.fn_GetRowsetIdFromRowDump
sys.fn_IsBitSetInBitmask
sys.fn_isrolemember
sys.fn_MapSchemaType
sys.fn_MSdayasnumber
sys.fn_MSgeneration_downloadonly
sys.fn_MSget_dynamic_filter_login
sys.fn_MSorbitmaps
sys.fn_MSrepl_map_resolver_clsid
sys.fn_MStestbit
sys.fn_MSvector_downloadonly
sys.fn_numberOf1InBinaryAfterLoc
sys.fn_numberOf1InVarBinary
sys.fn_repladjustcolumnmap
sys.fn_repldecryptver4
sys.fn_replformatdatetime
sys.fn_replgetparsedddlcmd

FIGURE: **Audit Filter Wizard**

14. Click the **Next** button.

The next **Audit Filter Wizard** page displays.



Filter Manager: Audit Filter Wizard

You can customize the description of your rule:

Title	FILTER ABC
Risk Level	Low **Important:** Info level cannot be viewed in the Console
Policy Description	Filter all stored procedures on this database.
Alert Description	Filter all stored procedures on this database.
Summary	Filter all stored procedures on this database.
Fix Information	N/A

FIGURE: Audit Filter Wizard

15. This page allows you to enter descriptive information about your Filter.

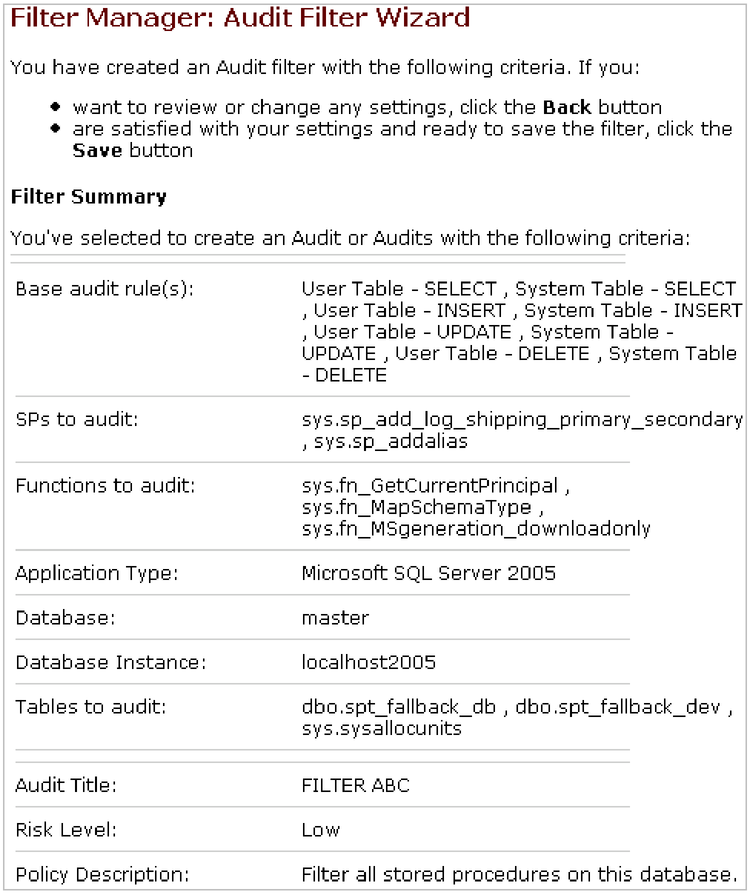
- *** Title** (required field). Enter the Filter title. There are no strict naming restrictions for Filters, other than size limit and alphanumeric characters. Application Security, Inc. recommends you adopt a naming convention for the Filters that are created; the title of the Filter is the first thing seen by an operator when an event occurs, and you choose an informative title, marking it with a special code if it's an Exception.
- *** Risk Level** (required field). Select a risk level for the audit event, i.e., **Informational** (i.e., **Info-1**, **Info-2**, **Info-3**, and **Info-4**).

Note: The **Informational** risk levels are typically for audit events. Audit events are written to a table in the DbProtect database, but **not** displayed on the Alert Manager page on the UI. For more information, see *What do the risk levels mean?*

- **Policy Description.** Enter a description of any corporate Policy that governs this Filter Rule.
- **Alert Description.** Enter an description of the Alert (and Filter).
- **Summary.** Enter a summary of the Alert (and Filter).
- **Fix Information.** Enter any fix information that is relevant to this Filter.

16. Click the **Next** button.

The next **Audit Filter Wizard** page displays.



Filter Manager: Audit Filter Wizard

You have created an Audit filter with the following criteria. If you:

- want to review or change any settings, click the **Back** button
- are satisfied with your settings and ready to save the filter, click the **Save** button

Filter Summary

You've selected to create an Audit or Audits with the following criteria:

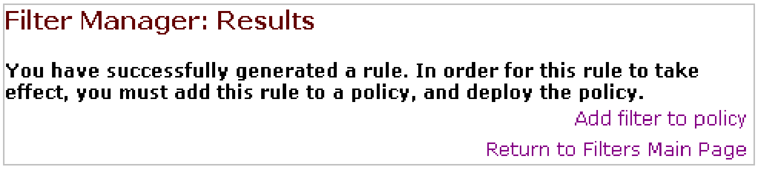
Base audit rule(s):	User Table - SELECT , System Table - SELECT , User Table - INSERT , System Table - INSERT , User Table - UPDATE , System Table - UPDATE , User Table - DELETE , System Table - DELETE
SPs to audit:	sys.sp_add_log_shipping_primary_secondary , sys.sp_addalias
Functions to audit:	sys.fn_GetCurrentPrincipal , sys.fn_MapSchemaType , sys.fn_MSgeneration_downloadonly
Application Type:	Microsoft SQL Server 2005
Database:	master
Database Instance:	localhost2005
Tables to audit:	dbo.spt_fallback_db , dbo.spt_fallback_dev , sys.sysallocunits
Audit Title:	FILTER ABC
Risk Level:	Low
Policy Description:	Filter all stored procedures on this database.

FIGURE: Audit Filter Wizard

17. At this point, the **Audit Filter Wizard** has enough information to save your Filter. If you:

- want to review or change any settings you can click the **Back** button or any link that displays on the page
- are satisfied with your settings and ready to save your Filter, click the **Save** button.

DbProtect Audit and Threat Management saves your Filter. The **Filter Manager: Results** page displays.



Filter Manager: Results

You have successfully generated a rule. In order for this rule to take effect, you must add this rule to a policy, and deploy the policy.

FIGURE: **Filter Manager: Results** page

18. In order for your Filter to take effect, you **must** add the Filter to a Policy (whether you create a new Policy, or edit an existing Policy), then deploy the Policy.

You can click the:

- **Add filter to policy** link to display the **Policy Manager**, add the Filter to the Policy, then deploy the Policy; for more information, see *Creating a Policy* if you want to add the Filter to a new Policy, or *Editing a Policy* if you want to add the Filter to an existing Policy
- **Return to Filters Main Page** link to re-display the **Filter Manager**.

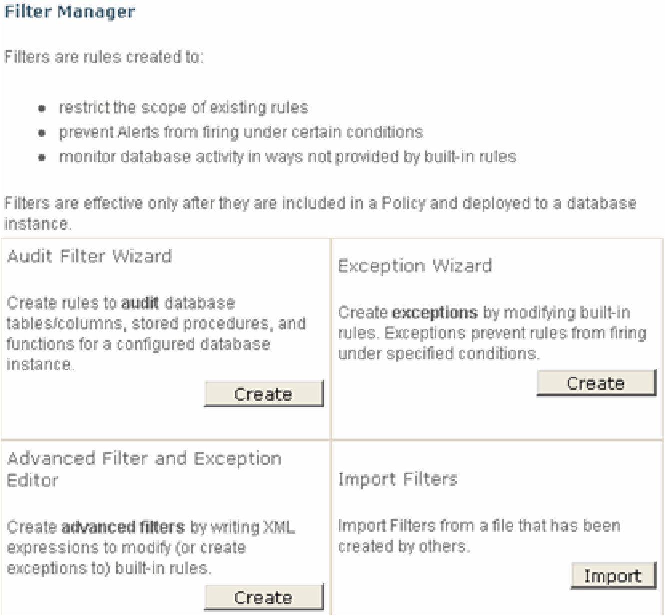
Working with the Exception Wizard

The **Exception Wizard** allows you to create Exceptions, i.e., conditions applied to Rules that prevent Alerts from firing for a given login name, source of attack, and/or application name.

There may be cases when you do not want to monitor database activity related to a specific Rule, but rather you want to monitor all database activity, in special cases. This can be done in DbProtect Audit and Threat Management using **Global Exceptions**. Global Exceptions allow you to monitor all database activity (for a selected database type), and configure DbProtect Audit and Threat Management **not** to fire Alerts when certain criteria are met. The **Exception Wizard** allows you to create Global Exceptions. For more information, see *What are Global Filters and Global Exceptions?*

To create regular and global Exception using the **Exception Wizard**:

1. Do one of the following to display the **Filter Manager** page:
   - Click the **Filters** workflow link on the **Home** page.
   - Click the **Filters** tab from anywhere on the page.



Filter Manager

Filters are rules created to:

- restrict the scope of existing rules
- prevent Alerts from firing under certain conditions
- monitor database activity in ways not provided by built-in rules

Filters are effective only after they are included in a Policy and deployed to a database instance.

Audit Filter Wizard

Create rules to **audit** database tables/columns, stored procedures, and functions for a configured database instance.

Create

Exception Wizard

Create **exceptions** by modifying built-in rules. Exceptions prevent rules from firing under specified conditions.

Create

Advanced Filter and Exception Editor

Create **advanced filters** by writing XML expressions to modify (or create exceptions to) built-in rules.

Create

Import Filters

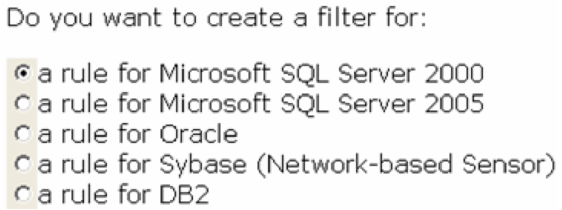
Import Filters from a file that has been created by others.

Import

FIGURE: Filter Manager

2. Click the **Create** button in the **Exception Wizard** portion of the page.

The first **Exception Wizard** page displays.



Do you want to create a filter for:

● a rule for Microsoft SQL Server 2000
○ a rule for Microsoft SQL Server 2005
○ a rule for Oracle
○ a rule for Sybase (Network-based Sensor)
○ a rule for DB2

FIGURE: Exception Wizard

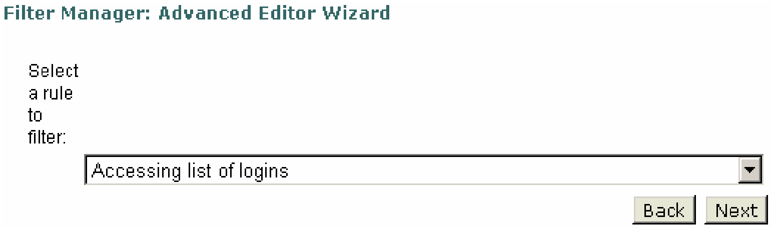
3. Select whether you want to create an Exception for:
   - **Microsoft SQL Server 2000** (host-based Sensor)
   - **Microsoft SQL Server 2005** (host-based Sensor)
   - **Microsoft SQL Server 2008** (host-based Sensor)

- **Oracle** (host-based or network-based Sensor)
- **Sybase** (network-based Sensor)
- **DB2** (host-based or network-based Sensor).

Note: If you are going to use a network-based Sensor to monitor a DB2 server, you must install the appropriate DB2 administrative client drivers. This requirement does **not** apply to host-based Sensors for DB2. For more information, see the *DbProtect Installation Guide*.

4. Click the **Next** button.

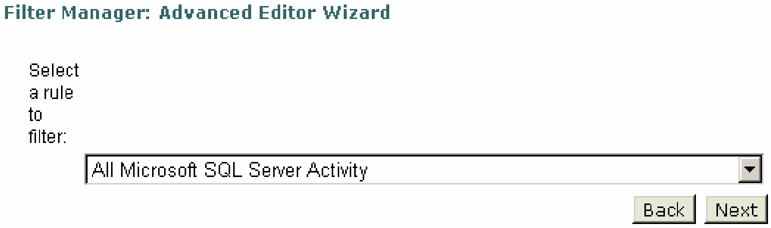
The next **Exception Wizard** page displays. You can select an individual Rule for which to create an Exception (e.g., **Accessing list of logins**).


Filter Manager: Advanced Editor Wizard

Select a rule to filter: Accessing list of logins

FIGURE: **Exception Wizard**

Or you can select the **All <Database Type> Server Activity** Rule to create a Global Exception (e.g., **All Microsoft SQL Server Activity**). For more information, see *What are Global Filters and Global Exceptions?*

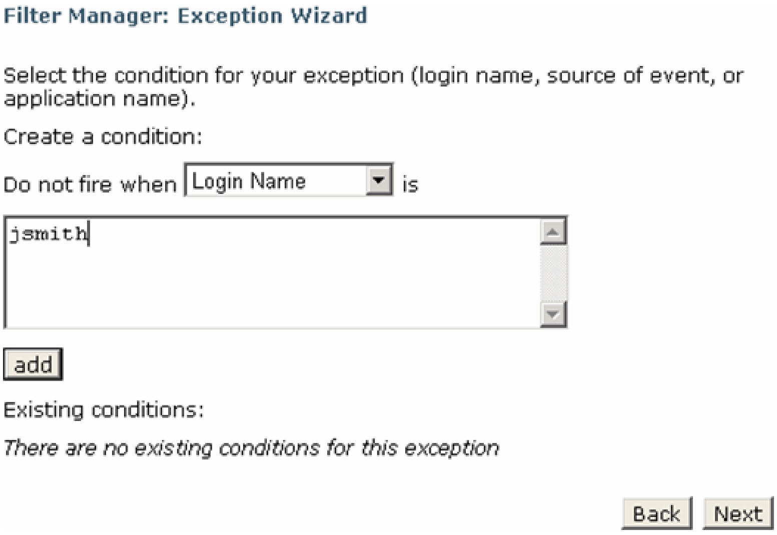

Filter Manager: Advanced Editor Wizard

Select a rule to filter: All Microsoft SQL Server Activity

FIGURE: **Exception Wizard**

5. Click the **Next** button.

The next **Exception Wizard** page displays.



Filter Manager: Exception Wizard

Select the condition for your exception (login name, source of event, or application name).

Create a condition:

Do not fire when Login Name is

jsmith

There are no existing conditions for this exception

FIGURE: Exception Wizard

6. This page has two parts: a **"do not fire when"** drop-down and a text box/ **add** button.

- The **"do not fire when"** drop-down allows you to select one of the following Exception conditions (i.e., when Alerts should **not** fire).

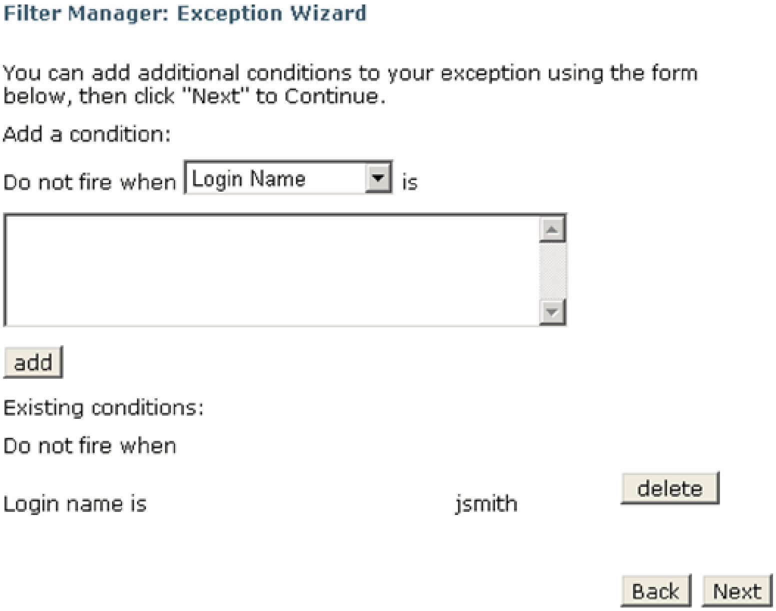
  -**Liogin Name.** The user name a potential source of Alerts may attempt to authenticate as.

  -**Source of Attack.** The network hostname or IP of a potential Alert source.

  -**Application Name.** The name of an application, as it registers itself with SQL Server, Oracle, Sybase, or DB2.

- Use the text box to specify the conditions under which to avoid firing an Alert. For example, if you select **Login Name** in the **"do not fire when"** drop-down, and enter `jsmith` in the text box, then the Rule selected in Step 4 will **not** fire when the individual with the login name `jsmith` performs the monitored action.

7. Click the **add** button to add additional criteria to your Exception. The added criteria display dynamically at the bottom of the page.



Filter Manager: Exception Wizard

You can add additional conditions to your exception using the form below, then click "Next" to Continue.

Add a condition:

Do not fire when Login Name is

Existing conditions:

Do not fire when

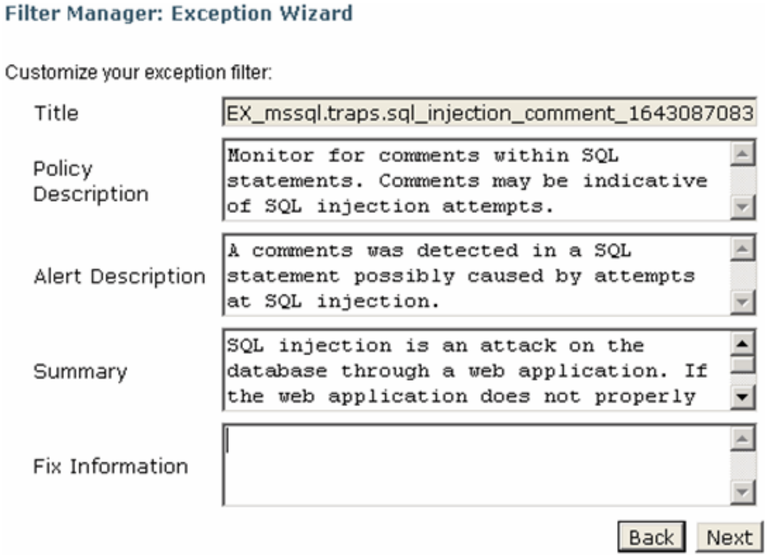
Login name is jsmith

FIGURE: Exception Wizard

Hint: You can click the **delete** button to delete any added Exception criteria before continuing.

8. Once you have added all your Exception criteria, click the **Next** button.

The next **Exception Wizard** page displays.



Filter Manager: Exception Wizard

Customize your exception filter:

Title: EX_mssql.traps.sql_injection_comment_1643087083

Policy Description: Monitor for comments within SQL statements. Comments may be indicative of SQL injection attempts.

Alert Description: A comments was detected in a SQL statement possibly caused by attempts at SQL injection.

Summary: SQL injection is an attack on the database through a web application. If the web application does not properly

Fix Information:

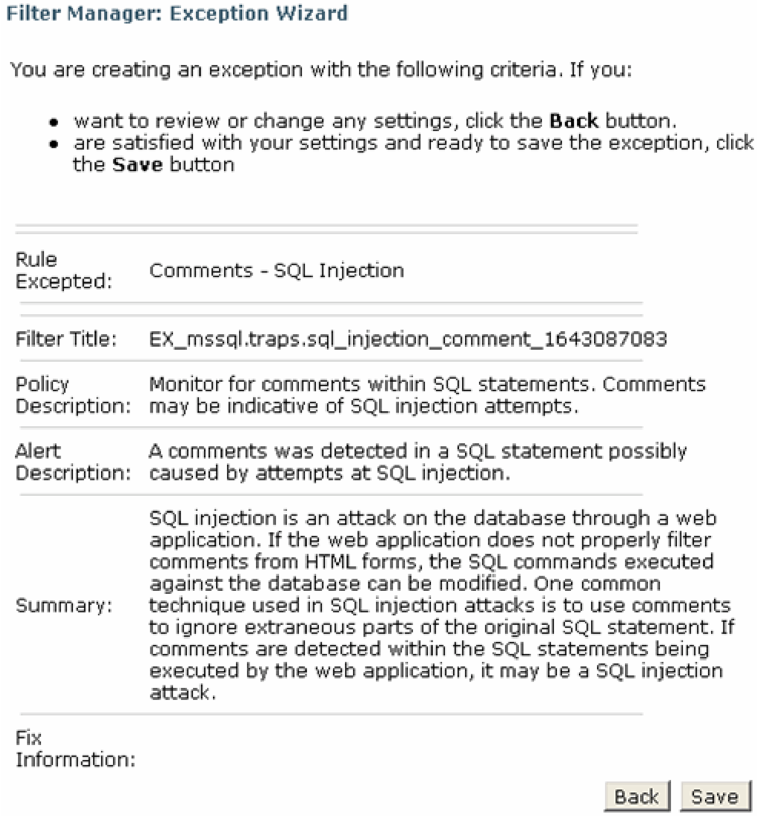
FIGURE: **Exception Wizard**

9. This page allows you to enter descriptive information about the Exception.

- * **Title** (required field). Enter the Exception title. There are no strict naming restrictions for Exceptions, other than size limit and alphanumeric characters. Application Security, Inc. recommends you adopt a naming convention for the Exceptions that are created; the title of the Exception is the first thing seen by an operator when an event occurs, and you choose an informative title, marking it with a special code if it's an Exception.
- **Policy Description.** Enter a description of any corporate Policy that governs this Exception Rule.
- Alert Description. Enter an description of the Alert (and Exception).
- Summary. Enter a summary of the Alert (and Exception).
- Fix Information. Enter any fix information that is relevant to this Exception.

10. Click the **Next** button.

The next **Exception Wizard** page displays.



Filter Manager: Exception Wizard

You are creating an exception with the following criteria. If you:

- want to review or change any settings, click the **Back** button.
- are satisfied with your settings and ready to save the exception, click the **Save** button

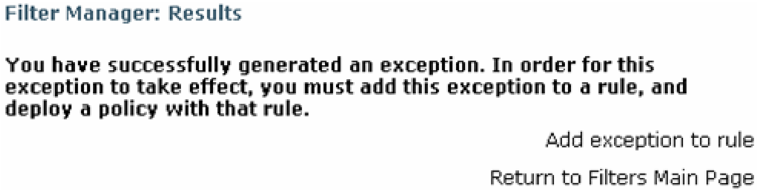
Rule Excepted:	Comments - SQL Injection
Filter Title:	EX_mssql.traps.sql_injection_comment_1643087083
Policy Description:	Monitor for comments within SQL statements. Comments may be indicative of SQL injection attempts.
Alert Description:	A comments was detected in a SQL statement possibly caused by attempts at SQL injection.
Summary:	SQL injection is an attack on the database through a web application. If the web application does not properly filter comments from HTML forms, the SQL commands executed against the database can be modified. One common technique used in SQL injection attacks is to use comments to ignore extraneous parts of the original SQL statement. If comments are detected within the SQL statements being executed by the web application, it may be a SQL injection attack.
Fix Information:	

FIGURE: **Exception Wizard**

11. At this point, the **Exception Wizard** has enough information to save your Exception. If you:

- want to review or change any settings you can click the **Back** button or any link that displays on the page
- are satisfied with your settings and ready to save your Exception, click the **Save** button.

DbProtect Audit and Threat Management saves your Exception. The **Filter Manager: Results** page displays.



Filter Manager: Results

You have successfully generated an exception. In order for this exception to take effect, you must add this exception to a rule, and deploy a policy with that rule.

FIGURE: **Filter Manager: Results** page

12. In order for the Exception to take effect, you must add the Exception to a Rule. You can click the:

- **Add Exception to rule** link to display the **Policy Manager**, add the Exception to a Rule in a Policy, then deploy the Policy; for more information, see *Creating a Policy* if you want to add the Exception to a rule in a new Policy, or *Editing a Policy* if you want to add the Exception to a rule in an existing Policy
- **Return to Filters Main Page** link to re-display the **Filter Manager**.

Working with the Advanced Filter and Exception Editor

The **Advanced Filter and Exception Editor** allows you to customize any built-in Rule, or create new ones. It contains a flexible expression editor for creating arbitrarily complex Rules.

Example: The Rule **Accessing list of logins** monitors the system table (**sysxlogins**) which contains the list of valid logins and password hashes for the database server. Attempts to access this data may indicate an attacker is trying to access the table information. In some cases, however, it is legitimate for an account to access the **sysxlogins** table. For instance, the application **BILL SYSTEM** is configured to access the **sysxlogins** table as part of its normal operations. However, this is the only system authorized to perform such a function.

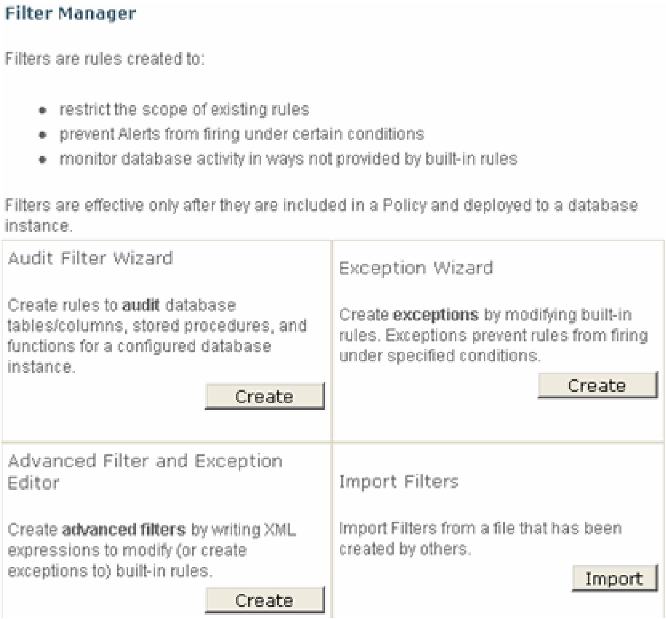
To monitor the **sysxlogins** table for unauthorized access -- with the exception of the **BILL SYSTEM** application -- you can create a Filter to notify you when *any* application *except* **BILL SYSTEM** is not accessing the **sysxlogins** table. You can add criteria to the Rule with the following expression: `Application is not equal to “BILL SYSTEM”`

The topic *Writing expressions* also contains advice (and an example) on writing XML Rules in the **Advanced Filter and Exception Editor**.

There may be cases when you do not want to monitor database activity related to a specific Rule, but rather you want to monitor all database activity, in special cases. This can be done in DbProtect Audit and Threat Management using **Global Filters** and **Global Exceptions**. **Global Filters** allow you to monitor all database activity (for a selected database type), and configure DbProtect Audit and Threat Management to fire Alerts only when certain criteria are met. Global Exceptions allow you to monitor all database activity (for a selected database type), and configure DbProtect Audit and Threat Management **not** to fire Alerts when certain criteria are met. The **Advanced Filter and Exception Editor** allows you to create Global Filters and Global Exceptions. For more information, see *What are Global Filters and Global Exceptions?*

To create Filters (regular and Global) and Exceptions (regular and Global) using the **Advanced Filter and Exception Editor**:

1. Do one of the following to display the **Filter Manager** page:
   - Click the **Filters** workflow link on the **Home** page.
   - Click the **Filters** tab from anywhere on the page.



Filter Manager

Filters are rules created to:

- restrict the scope of existing rules
- prevent Alerts from firing under certain conditions
- monitor database activity in ways not provided by built-in rules

Filters are effective only after they are included in a Policy and deployed to a database instance.

Audit Filter Wizard

Create rules to **audit** database tables/columns, stored procedures, and functions for a configured database instance.

Exception Wizard

Create **exceptions** by modifying built-in rules. Exceptions prevent rules from firing under specified conditions.

Advanced Filter and Exception Editor

Create **advanced filters** by writing XML expressions to modify (or create exceptions to) built-in rules.

Import Filters

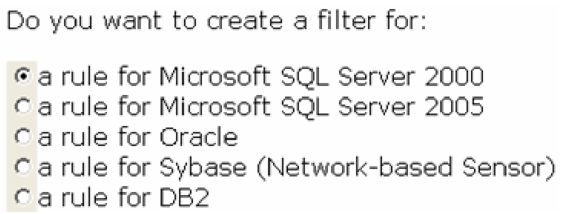
Import Filters from a file that has been created by others.

S

FIGURE: Filter Manager

2. Click the **Create** button in the **Advanced Filter and Exception Editor** of the page.

The first **Advanced Filter and Exception Editor** page displays.



Do you want to create a filter for:

● a rule for Microsoft SQL Server 2000
○ a rule for Microsoft SQL Server 2005
○ a rule for Oracle
○ a rule for Sybase (Network-based Sensor)
○ a rule for DB2

FIGURE: **Advanced Filter and Exception Editor**

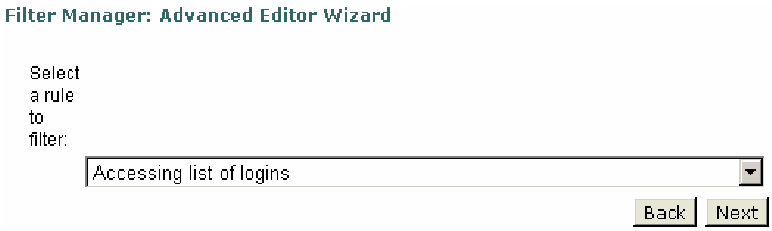
3. Select whether you want to create a Rule for:

- **Microsoft SQL Server 2000** (host-based Sensor); for more information on Microsoft SQL Server name attributes, see *SQL Server name attributes*
- **Microsoft SQL Server 2005** (host-based Sensor); for more information on Microsoft SQL Server name attributes, see *SQL Server name attributes*
- **Microsoft SQL Server 2008** (host-based Sensor); for more information on Microsoft SQL Server name attributes, see *SQL Server name attributes*
- **Oracle** (host-based or network-based Sensor); for more information on Oracle name attributes, see *Oracle name attributes*
- **Sybase** (network-based Sensor); for more information on Sybase name attributes, see *Sybase name attributes*
- **DB2** (host-based or network-based Sensor); for more information on SQL Server name attributes, see *DB2 name attributes*.

Note: If you are going to use a network-based Sensor to monitor a DB2 server, you must install the appropriate DB2 administrative client drivers. This requirement does not apply to host-based Sensors for DB2. For more information, see the *DbProtect Installation Guide*.

4. Click the **Next** button.

The next **Advanced Filter and Exception Editor** page displays. You can select an individual Rule for which to create an Exception (e.g., **Accessing list of logins**).

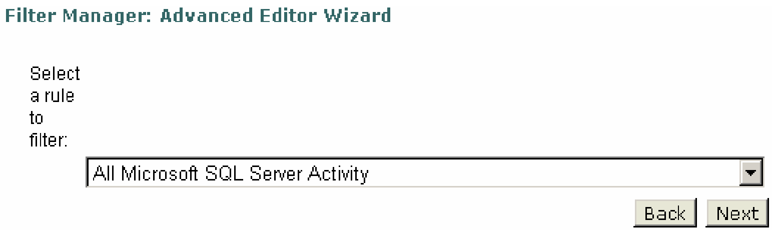


Filter Manager: Advanced Editor Wizard

Select a rule to filter: Accessing list of logins

FIGURE: Advanced Filter and Exception Editor

Or you can select the **All <Database Type> Server Activity** Rule to create a Global Filter or a Global Exception (e.g., **All Microsoft SQL Server Activity**). For more information, see *What are Global Filters and Global Exceptions?*



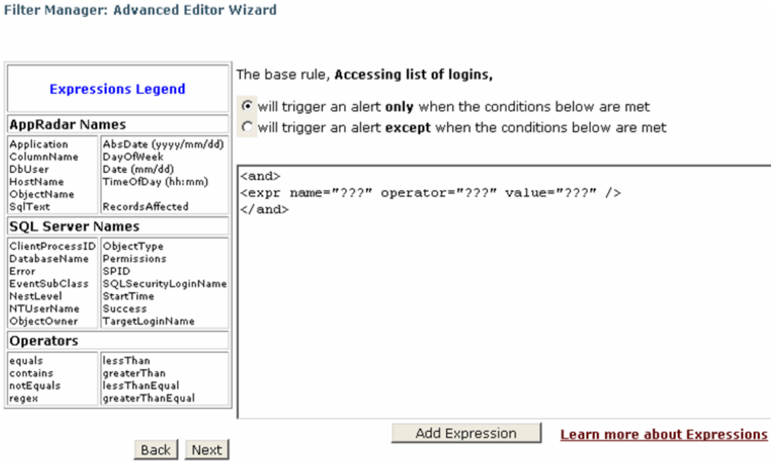
Filter Manager: Advanced Editor Wizard

Select a rule to filter: All Microsoft SQL Server Activity

FIGURE: Advanced Filter and Exception Editor

5. Click the **Next** button.

The next **Advanced Filter and Exception Editor** page displays.



Filter Manager: Advanced Editor Wizard

Expressions Legend

AppRadar Names	
Application ColumnName DbUser HostName ObjectName SqlText	AbsDate (yyyy/mm/dd) DayOfWeek Date (mm/dd) TimeOfDay (hh:mm) RecordsAffected

SQL Server Names	
ClientProcessID DatabaseName Error EventSubClass NestLevel NTUserName ObjectOwner	ObjectType Permissions SPID SQLSecurityLoginName StartTime Success TargetLoginName

Operators	
equals contains notEquals regex	lessThan greaterThan lessThanEqual greaterThanEqual

The base rule, **Accessing list of logins,**

● will trigger an alert **only** when the conditions below are met
○ will trigger an alert **except** when the conditions below are met

```
<and>
<expr name="???" operator="???" value="???" />
</and>
```

FIGURE: Advanced Filter and Exception Editor

This page consists of the following portions:

- **SQL Server Name Legend/AppRadar Names Legend/Operator Legend.** These legends allow you to copy/paste valid SQL Server names, DbProtect Audit and Threat Management names, and operators into the XML editor when you create your Rule.
- **Trigger conditions.** The trigger condition radio buttons allows you to select whether the base Rule will trigger an Alert *only* when or *except* when the conditions (expressed in the XML editor) are met.

Note: If you selected the **All <Database Type> Server Activity Rule** (e.g., **All Microsoft SQL Server Activity**) in Step 4, and you select you select will trigger and alert only when the conditions below are met, then you are creating a Global Filter. However, if you selected the **All <Database Type> Server Activity Rule** (e.g., **All Microsoft SQL Server Activity**) in Step 4, and you select **will trigger and alert except when the conditions below are met**, then you are creating a Global Exception. For more information, see *What are Global Filters and Global Exceptions?*

- **XML editor.** The XML editor allows you to write a Rule as an XML expression. You can copy/paste valid values from the legends. The XML editor is already activated once you display this page, and populated with a template of XML code containing "dummy" placeholder values.

Important: You **must** understand XML syntax, Boolean logic, and prefix-notation to create valid expressions. The topic *Joining expressions* also contains advice (and an example) on writing XML Rules in **Advanced Filter and Exception Editor**.

6. Do the following:

- Use the **XML editor** to create Rule criteria by joining together any number of expressions with `AND` and `OR` logical operators; for more information on expression writing, see *Writing expressions* and *Joining expressions*.

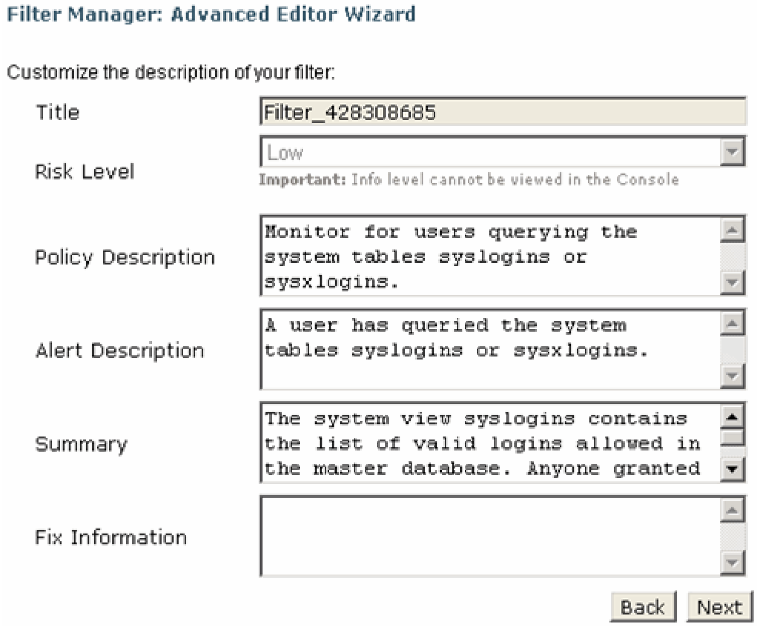
  For example:

  ```
  <and>
  <expr name="ObjectName" operator="equals" value="foo" />
  </and>
  ```

  The XML **must** be both well-formed and valid. The XML is valid if it contains a `name` attribute with a value shown in the **SQL Server Name Legend** and the **AppRadar Names Legend**, and an `operator` attribute with a value shown in the **Operator Legend**.
- In the **trigger conditions** portion, select whether your base Rule will trigger an Alert *only* when or *except* when the conditions (expressed in the XML editor) are met.
- Click the **Add Expression** button to append another template of XML code (with more "dummy" placeholder values).

7. When you're done, click the **Next** button.

The next **Advanced Filter and Exception Editor** page displays.



Filter Manager: Advanced Editor Wizard

Customize the description of your filter:

Title	Filter_428308685
Risk Level	Low **Important:** Info level cannot be viewed in the Console
Policy Description	Monitor for users querying the system tables syslogins or sysxlogins.
Alert Description	A user has queried the system tables syslogins or sysxlogins.
Summary	The system view syslogins contains the list of valid logins allowed in the master database. Anyone granted
Fix Information	

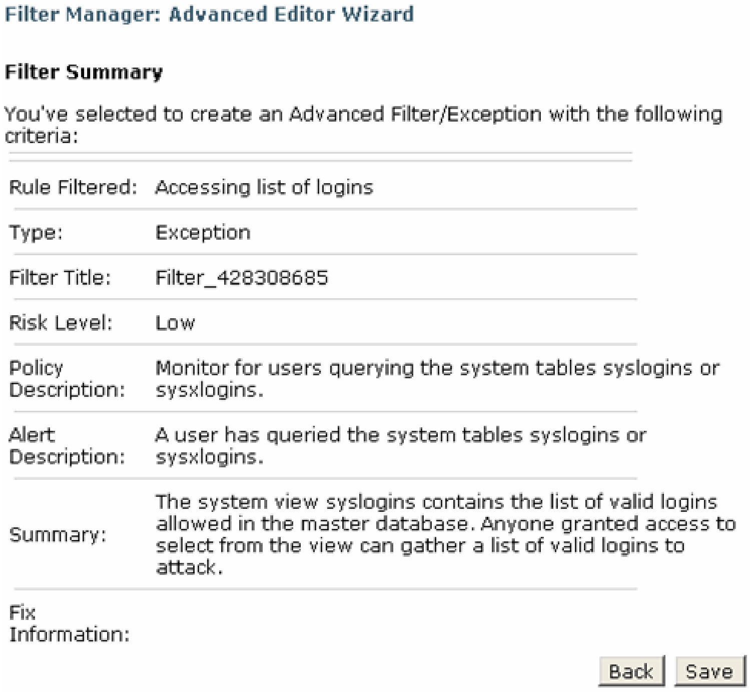
FIGURE: Advanced Filter and Exception Editor

8. This page allows you to enter descriptive information about the Rule.

- *** Title** (required field). Enter the Rule title. There are no strict naming restrictions for Rules, other than size limit and alphanumeric characters. Application Security, Inc. recommends you adopt a naming convention for the Rules that are created; the title of the Rule is the first thing seen by an operator when an event occurs, and you choose an informative title.
- *** Risk Level** (required field). Select a risk level. Your choices are: **High**, **Medium**, **Low**, or **Informational** (i.e., **Info-1**, **Info-2**, **Info-3**, and **Info-4**), which are typically for audit events. Audit events are written to a table in the DbProtect database, but **not** displayed on the **Alert Manager** page on the UI. For more information, see *What do the risk levels mean?*
- **Policy Description.** Enter a description of any corporate Policy that governs this Rule.
- **Alert Description.** Enter an description of the Alert (and Rule).
- **Summary.** Enter a summary of the Alert (and Rule).
- **Fix Information.** Enter any fix information that is relevant to this Rule.

9. Click the **Next** button.

The **Advanced Filter and Exception Editor: Summary** page displays.



Filter Manager: Advanced Editor Wizard

Filter Summary

You've selected to create an Advanced Filter/Exception with the following criteria:

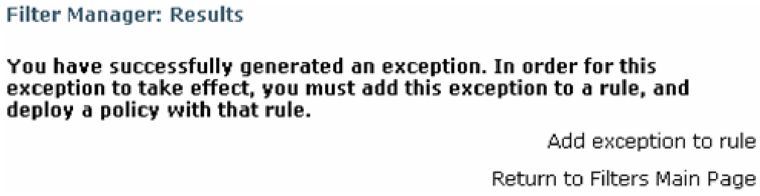
Rule Filtered:	Accessing list of logins
Type:	Exception
Filter Title:	Filter_428308685
Risk Level:	Low
Policy Description:	Monitor for users querying the system tables syslogins or sysxlogins.
Alert Description:	A user has queried the system tables syslogins or sysxlogins.
Summary:	The system view syslogins contains the list of valid logins allowed in the master database. Anyone granted access to select from the view can gather a list of valid logins to attack.
Fix Information:	

FIGURE: **Advanced Filter and Exception Editor: Summary** page

If you:

- want to review or change any settings you can click the **Back** button or any link that displays on the page
- are satisfied with your Rule settings, click the **Save** button.

Your Rule is saved. A confirmation page displays.



Filter Manager: Results

You have successfully generated an exception. In order for this exception to take effect, you must add this exception to a rule, and deploy a policy with that rule.

FIGURE: **Advanced Filter and Exception Editor: Confirmation** page

10. In order for the Rule to take effect, you must add the Rule to a Policy (whether you create a new Policy, or edit an existing Policy), then deploy the Policy.

From the confirmation page, you can click the:

- **Add filter to policy** link, to display the **Policy Manager**; for more information, see *Creating a Policy* or *Editing a Policy*, accordingly.
- **Return to Filters Main Page** link to display the main **Filter Manager** page.

Writing expressions

Expressions are written in eXtsensible Markup Language (XML), and are built on Boolean logic. This topic explains expressions, and provides practical examples to help you write Filters with the expression semantics.

Every DbProtect Audit and Threat Management expression consists of **two operands** and **one operator**. The two operands are the name operand and the **value operand**. The name operands are predefined values that map directly to the SQL Server or Oracle Profiler's data columns, and to special DbProtect Audit and Threat Management-defined values. The value operand may be any string, and is **not** restricted by DbProtect Audit and Threat Management; you must supply it.

This topic consists of the following sub-topics:

- *Expression syntax*
- *DbProtect AppRadar name attributes*
- *SQL Server name attributes*
- *DB2 name attributes*
- *Sybase name attributes*
- *Oracle name attributes*
- *Operator attributes*
- *Examples.*

EXPRESSION SYNTAX

The `expr` tag contains three attributes: **name**, **operator** and **value**. The syntax is:

```
<expr name="X" operator="Y" value="Z"/>
```

DBPROTECT APPRADAR NAME ATTRIBUTES

The following table includes valid **DbProtect AppRadar name attributes**, which are common for *all* Audit and Threat Management expressions across *all* supported database platforms.

DbProtect AppRadar Name Attribute	Details
`Application`	Name of the client application that created the connection to an instance of a given database type (i.e., Microsoft SQL Server 2000/2005/2008, DB2, Sybase, or Oracle). This column is populated with the values passed by the application rather than the displayed name of the program.
`ColumnName`	The name of the column of a table in which the user statement is running.
`DbUser`	Database user name.
`HostName`	The name of the machine (host) from which the client application is run.
`ObjectName`	Name of the referenced object.
`SqlText`	The SQL text command presented for execution by the client.
`AbsDate (yyyy/mm/dd)`	Absolute date.
`DayOfWeek`	The day of the week.
`Date (mm/dd)`	Date (month and date).
`TimeOfDay (hh:mm)`	Time of day in military time (e.g., `20:00` = 8 P.M.).
`RecordsAffected`	Indicates how many rows have been queried/updated as the result of executing a SQL statement; for more information, see *Understanding result sets*.

SQL SERVER NAME ATTRIBUTES

The following table includes valid **Microsoft SQL Server name attributes** (for Microsoft SQL Server 2000/2005/2008). An expression can contain SQL Profiler Data Columns, and DbProtect Audit and Threat Management-defined values.

SQL Server Name Attribute	Details
`ClientProcessID`	ID assigned by the host computer to the process where the client application is running. This data column is populated if the client process ID is provided by the client.
`DatabaseName`	Name of the database in which the user statement is running.
`Error`	Indicates if the SQL command yielded an error.
`EventSubClass`	Type of event subclass, providing further information about each event class. For example, event subclass values for the **Execution Warning** event class represent the type of execution warning: • `1` = **Query wait.** The query must wait for resources (for example, memory) before it can execute. • `2` = **Query time out.** The query timed out while waiting for required resources to execute. This data column is not populated for all event classes.
`NestLevel`	The nesting level of the stored procedure call. For example, `my_proc_a` stored procedure calls `my_proc_b`. In this case, `my_proc_a` has a `NestLevel` of `1`, `my_proc_b` has a `NestLevel` of `2`.
`NTUserName`	Windows NT 4.0 user name.
`ObjectOwner`	User who owns the referenced object.

SQL Server Name Attribute	Details
ObjectType	Value representing the type of the object involved in the event. Values are: **For Microsoft SQL Server 2000:** • 1 = Index • 2 = Database • 5 = Default • 8 = Stored Procedure • 9 = Function • 10 = Rule • 12 = System Table • 13 = Trigger • 17 = User Table • 18 = View • 19 = Extended Stored Procedure
	For Microsoft SQL Server 2005 and 2008: • 8259 = Check Constraint • 8260 = Default (constraint or standalone) • 8262 = Foreign-key Constraint • 8272 = Stored Procedure • 8274 = Rule • 8275 = System Table • 8276 = Trigger on Server • 8277 = (User-defined) Table • 8278 = View • 8280 = Extended Stored Procedure • 16724 = CLR Trigger • 16964 = Database • 16975 = Object • 17222 = FullText Catalog • 17232 = CLR Stored Procedure • 17235 = Schema • 17475 = Credential • 17491 = DDL Event • 17741 = Management Event • 17747 = Security Event • 17749 = User Event

SQL Server Name Attribute	Details
ObjectType *(cont'd)*	• 17985 = CLR Aggregate Function • 17993 = Inline Table-valued SQL Function • 18000 = Partition Function • 18002 = Replication Filter Procedure • 18004 = Table-valued SQL Function • 18259 = Server Role • 18263 = Microsoft Windows Group • 19265 = Asymmetric Key • 19277 = Master Key • 19280 = Primary Key • 19283 = ObfusKey • 19521 = Asymmetric Key Login • 19523 = Certificate Login • 19538 = Role • 19539 = SQL Login • 19543 = Windows Login • 20034 = Remote Service Binding • 20036 = Event Notification on Database • 20037 = Event Notification • 20038 = Scalar SQL Function • 20047 = Event Notification on Object • 20051 = Synonym • 20549 = End Point • 20801= Adhoc Queries which may be cached • 20816 = Prepared Queries which may be cached • 20819 = Service Broker Service Queue • 20821 = Unique Constraint • 21057 = Application Role • 21059 = Certificate • 21075 = Server • 21076 = Transact-SQL Trigger • 21313 = Assembly • 21318 = CLR Scalar Function • 21321 = Inline scalar SQL Function • 21328 = Partition Scheme • 21333 = User

SQL Server Name Attribute	Details
ObjectType *(cont'd)*	• 21571 = Service Broker Service Contract • 21572 = Trigger on Database • 21574 = CLR Table-valued Function • 21577 = Internal Table (For example, XML Node Table, Queue Table.) • 21581 = Service Broker Message Type • 21586 = Service Broker Route • 21587 = Statistics • 21825, 21827, 21831, 21843, 21847 = User • 22099 = Service Broker Service • 22601 = Index • 22604 = Certificate Login • 22611 = XMLSchema • 22868 = Type
Permissions	Integer value representing the type of permissions checked. Values are: • 1 = SELECT ALL • 2 = UPDATE ALL • 4 = REFERENCES ALL • 8 = INSERT • 16 = DELETE • 32 = EXECUTE (procedures only) • 4096 = SELECT ANY (at least one column) • 8192 = UPDATE ANY • 16384 = REFERENCES ANY
SPID	Server Process ID assigned by SQL Server to the process associated with the client.
SQLSecurity LoginName	Name of the login of the user (either SQL Server security login or the Windows login credentials in the form of DOMAIN\Username).
StartTime	Time when the event started, when available.
Success	Indicates if the SQL command yielded ran successfully.
TargetLoginName	For actions which target a login (for example, adding a new login), the name of the targeted login.

For more information about SQL Server Profiler Data Columns, see your SQL Server documentation.

DB2 NAME ATTRIBUTES

The following table includes valid **DB2 name attributes**. An expression can contain these DbProtect Audit and Threat Management-defined values.

DB2 Attribute	Details
DatabaseName	Name of the database in which the user statement is running.
OsUser	Name of the login of the operating system user running the database client.
SqlTextSize	The size of the SQL text command presented for execution by the client.

SYBASE NAME ATTRIBUTES

The following table includes valid **Sybase name attributes**. An expression can contain these DbProtect Audit and Threat Management-defined values.

Sybase Attribute	Details
DatabaseName	Name of the database in which the user statement is running.
OsUser	Name of the login of the operating system user running the database client.
SqlTextSize	The size of the SQL text command presented for execution by the client.

ORACLE NAME ATTRIBUTES

The following table includes valid **Oracle name attributes**.

Oracle Attribute	Details
OsUser	Name of the login of the operating system user running the database client.
SqlTextSize	The size of the SQL text command presented for execution by the client.

OPERATOR ATTRIBUTES

As a general rule, if you know specifically what value to compare, use the `equals` operator. If you need to search by a substring, then the `contains` operator makes more sense. The following table includes valid operator attributes.

Operator Attribute	Details
`equals`	Equals.
`contains`	The left operand contains the substring value of the right operand.
`notEquals`	Does not equal.
`regex`	Regular expression.
`lessThan`	Less than.
`greaterThan`	Greater than.
`lessThanEqual`	Less than or equal.
`greaterThanEqual`	Greater than equal.

- **`equals`.** This compares the name to the value field. The value must match exactly for this expression to be true. This operator is also case-sensitive. For example if we have an expression that compares the `"DatabaseName"` to `"Human_Resources"` as defined in:

  ```
  <expr name="DatabaseName" value="Human_Resources"
  operator="equals"></expr>
  ```

  So, when the `DatabaseName` is:

  -`"Human_Resources"`, the expression is `TRUE`

  -`"human_resources"`, the expression is `FALSE`

  -`"Human_Resources_Database"`, the expression is `FALSE`

  -`"Human_Resources "` (note extra space at the end), the expression is `FALSE`

  -`"Human_Resource"`, the expression is `FALSE`.

- **`contains`.** This operator searches for a substring contained in the value. It is case insensitive. For example, if you have an expression that compares the `"DatabaseName"` to `"Human_Resources"` as defined in:

  ```
  <expr name="DatabaseName" value="Human_Resources"
  operator="contains"></expr>
  ```

So, when the DatabaseName is:

-"Human_Resources", the expression is TRUE

-"human_resources", the expression is TRUE

-"Human_Resources_Database", the expression is TRUE

-"Human_Resources ", the expression is TRUE

-"DBHuman_Resources", the expression is TRUE

-"Human_Resource", the expression is FALSE

-"HR_Database", the expression is FALSE.

- **regex**. This operator is more complicated. It uses the regular expression pattern matching language to search for a value. This is a more advanced technique for searches, and should be reserved for more complex searches. For more information, visit some websites that discuss the regular expression language that is heavily used in programming languages such as Perl and Unix commands such as sed and grep. For more information, see *http://en.wikipedia.org/wiki/Regular_expression*.
- **notEquals**. This operator checks whether two values are different. It has the same semantics as the equals operator.
- **lessThan**. This operator checks whether one integer value is less than another integer value. It does **not** support real numbers. You **cannot** apply this operator to alphabetic values.
- **greaterThan**. This operator checks whether one integer value is greater than another integer value. It does **not** support real numbers. You **cannot** apply this operator to alphabetic values.
- **lessThanEqual**. This operator checks whether one integer value is less than, or equal to. another integer value. It does **not** support real numbers. You **cannot** apply this operator to alphabetic values.
- **greaterThanEqual**. This operator checks whether one integer value is greater than, or equal to, another integer value. It does **not** support real numbers. You **cannot** apply this operator to alphabetic values.

Example:

Below is an example of an XML expression written in the Advanced Filter Editor to Filter Rules for three specific databases; for more information, see *Working with the Advanced Filter and Exception Editor*.

```
<and>

  <or>

    <expr name="DatabaseName" value="Finance"
operator="equals"></expr>

    <expr name="DatabaseName" value="Human_Resources"
operator="equals"></expr>

    <expr name="DatabaseName" value="JCRS" operator="equals"></
expr>

  </or>

</and>
```

The enclosing `<and></and>` tags are not really necessary in this case. In plain English, this statement means: "Show this Alert when the database names are either 'Finance', 'Human_Resources', or 'JCRS', and ..."

And what? Well...nothing. So, you can simplify this expression to:

```
<or>

  <expr name="DatabaseName" value="Finance" operator="equals"></
expr>

  <expr name="DatabaseName" value="Human_Resources"
operator="equals"></expr>

  <expr name="DatabaseName" value="JCRS" operator="equals"></
expr>

</or>
```

Joining expressions

You can **join expressions** to form more complex Rules. Usually just monitoring the master database is not granular enough. You may only be interested in monitoring the master database in conjunction with the sa account. DbProtect Audit and Threat Management provides the boolean and **and/or** operators as XML tags to represent this.

EXAMPLES

Capture only events that are taking place in the master database that are performed by the sa account. Notice the use of the `<and>` tag to combine these two expressions:

```
<and>

<expr name="DatabaseName" operator="equals" value="master" />

<expr name="SQLSecurityLoginName" operator="equals"
value="sa" />

</and>
```

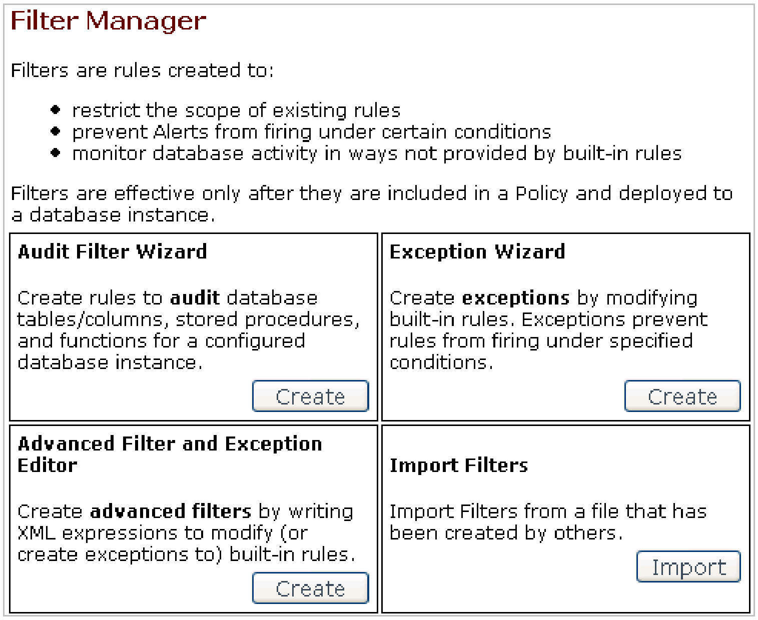
Capture only events that are taking place in the master database and are performed by either the sa account, or the **itsecurity** login (a SQL Server login that exists in this example). Note the combination of the `<and>` and `<or>` tags to express this Rule:

```
<and>

<expr name="DatabaseName" operator="equals" value="master" />

<or>

<expr name="SQLSecurityLoginName" operator="equals"
value="sa" />

<expr name="SQLSecurityLoginName" operator="equals"
value="itsecurity" />

</or>

</and>
```

Editing a Filter

To edit a Filter:

1. Do one of the following to display the **Filter Manager** page:
   - Click the **Filters** workflow link on the **Home** page.
   - Click the **Filters** tab from anywhere on the page.



Filter Manager

Filters are rules created to:

- restrict the scope of existing rules
- prevent Alerts from firing under certain conditions
- monitor database activity in ways not provided by built-in rules

Filters are effective only after they are included in a Policy and deployed to a database instance.

Audit Filter Wizard

Create rules to **audit** database tables/columns, stored procedures, and functions for a configured database instance.

Create

Exception Wizard

Create **exceptions** by modifying built-in rules. Exceptions prevent rules from firing under specified conditions.

Create

Advanced Filter and Exception Editor

Create **advanced filters** by writing XML expressions to modify (or create exceptions to) built-in rules.

Create

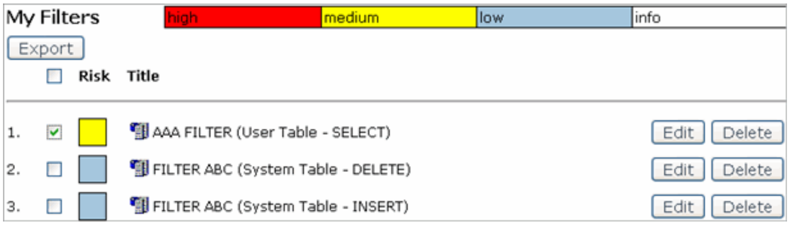
Import Filters

Import Filters from a file that has been created by others.

Import

FIGURE: Filter Manager

2. In the **My Filters** portion of the page, click the **Edit** button next to the Filter.



My Filters

high | medium | low | info

Export

	□	Risk	Title		
1.	☑	🟨	AAA FILTER (User Table - SELECT)	Edit	Delete
2.	□	🟦	FILTER ABC (System Table - DELETE)	Edit	Delete
3.	□	🟦	FILTER ABC (System Table - INSERT)	Edit	Delete

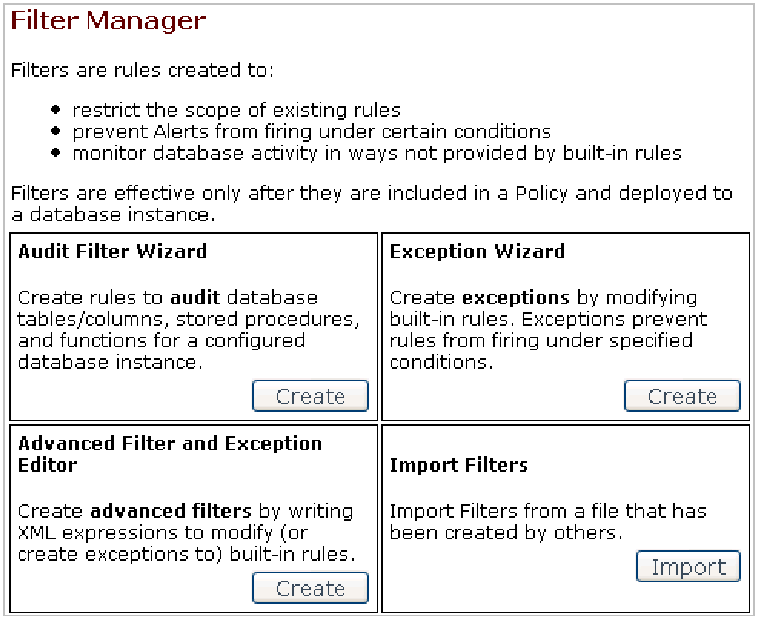
FIGURE: **Filter Manager** (**My Filters** portion)

The **Advanced Filter and Exception Editor** displays, allowing you to edit your Filter; for more information, see *Working with the Advanced Filter and Exception Editor*.

Deleting a Filter

To delete a Filter:

1. Do one of the following to display the **Filter Manager** page:
   - Click the **Filters** workflow link on the **Home** page.
   - Click the **Filters** tab from anywhere on the page.



Filter Manager

Filters are rules created to:

- restrict the scope of existing rules
- prevent Alerts from firing under certain conditions
- monitor database activity in ways not provided by built-in rules

Filters are effective only after they are included in a Policy and deployed to a database instance.

Audit Filter Wizard

Create rules to **audit** database tables/columns, stored procedures, and functions for a configured database instance.

Create

Exception Wizard

Create **exceptions** by modifying built-in rules. Exceptions prevent rules from firing under specified conditions.

Create

Advanced Filter and Exception Editor

Create **advanced filters** by writing XML expressions to modify (or create exceptions to) built-in rules.

Create

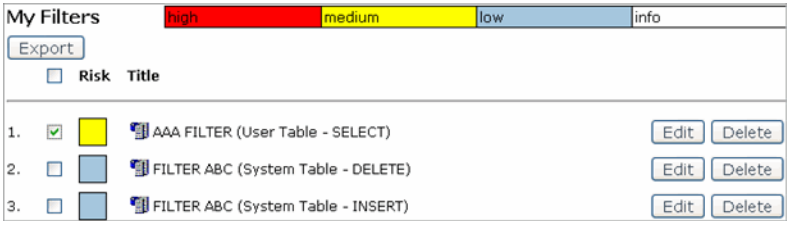
Import Filters

Import Filters from a file that has been created by others.

Import

FIGURE: Filter Manager

2. In the **My Filters** portion of the page:
   - check a Filter you want to delete
   - click the **Delete** button next to the Filter.



My Filters

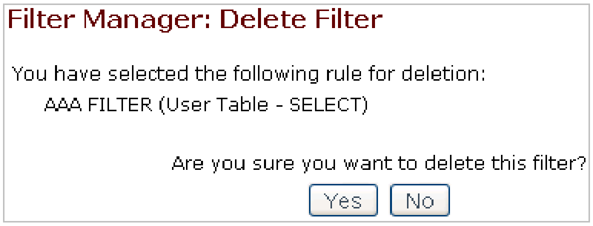
🟥 high 🟨 medium 🟦 low info

Export

	□	Risk	Title		
1.	☑	🟨	AAA FILTER (User Table - SELECT)	Edit	Delete
2.	□	🟦	FILTER ABC (System Table - DELETE)	Edit	Delete
3.	□	🟦	FILTER ABC (System Table - INSERT)	Edit	Delete

FIGURE: **Filter Manager** (**My Filters** portion)

A confirmation page prompts you to confirm the delete.



Filter Manager: Delete Filter

You have selected the following rule for deletion:

AAA FILTER (User Table - SELECT)

Are you sure you want to delete this filter?

FIGURE: Delete confirmation page

3. Click the **Yes** button to delete.

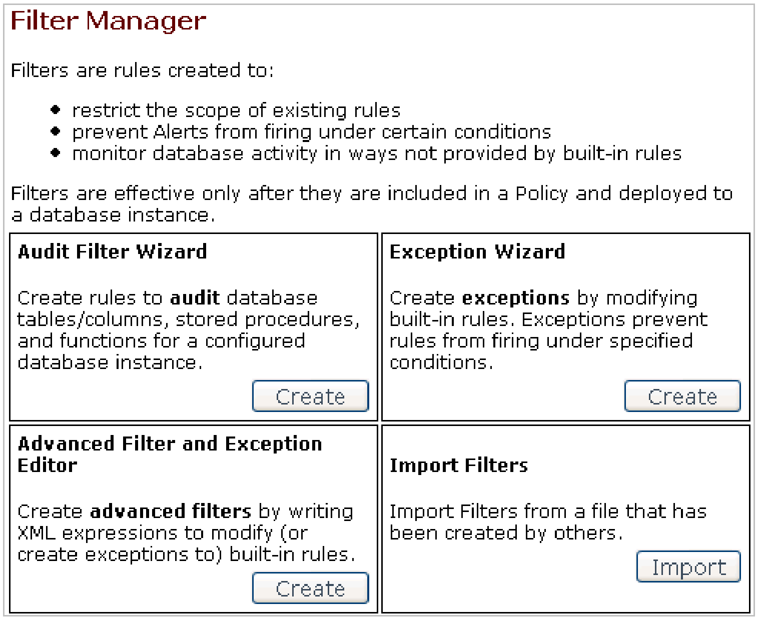
Your Filter is deleted.

Note: After you activate a Filter in a Policy, DbProtect Audit and Threat Management does **not** allow you to delete the Filter. You must de-select the Filter from any associated Policy. Then, you **must** re-deploy the Policy. For more information, see *Editing a Policy* and *Deploying a Policy*, respectively.

Importing a Filter

To import a Filter:

1. Do one of the following to display the **Filter Manager** page:
   - Click the **Filters** workflow link on the **Home** page.
   - Click the **Filters** tab from anywhere on the page.



Filter Manager

Filters are rules created to:

- restrict the scope of existing rules
- prevent Alerts from firing under certain conditions
- monitor database activity in ways not provided by built-in rules

Filters are effective only after they are included in a Policy and deployed to a database instance.

Audit Filter Wizard

Create rules to **audit** database tables/columns, stored procedures, and functions for a configured database instance.

Exception Wizard

Create **exceptions** by modifying built-in rules. Exceptions prevent rules from firing under specified conditions.

Advanced Filter and Exception Editor

Create **advanced filters** by writing XML expressions to modify (or create exceptions to) built-in rules.

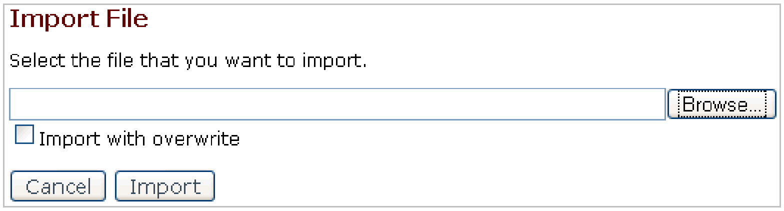
Import Filters

Import Filters from a file that has been created by others.

FIGURE: Filter Manager

2. Click the **Import** button in the **Import Filter** portion of the page.

The **Import File** page displays.



Import File

Select the file that you want to import.

FIGURE: Filter Manager

3. Specify the location of the Filter file (which must be in XML format). You can:
   - click the **Browse...** button to display the **File Upload** pop up and locate the Filter file you want to import (on your local computer or network)

- enter the full path and file name of the XML Filter file you want to import (on your local computer or network).

Note: Check **Import with overwrite** to overwrite an existing Filter file automatically.

4. Click the **Import** button.

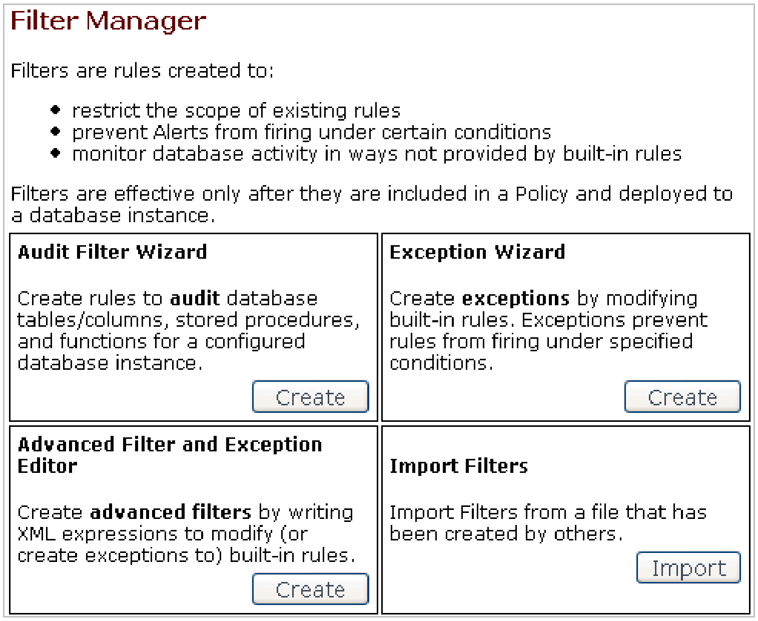
DbProtect Audit and Threat Management imports your Filter.

Exporting a Filter

To export a Filter:

1. Do one of the following to display the **Filter Manager** page:

- Click the **Filters** workflow link on the **Home** page.
- Click the **Filters** tab from anywhere on the page.



Filter Manager

Filters are rules created to:

- restrict the scope of existing rules
- prevent Alerts from firing under certain conditions
- monitor database activity in ways not provided by built-in rules

Filters are effective only after they are included in a Policy and deployed to a database instance.

Audit Filter Wizard

Create rules to **audit** database tables/columns, stored procedures, and functions for a configured database instance.

Exception Wizard

Create **exceptions** by modifying built-in rules. Exceptions prevent rules from firing under specified conditions.

Advanced Filter and Exception Editor

Create **advanced filters** by writing XML expressions to modify (or create exceptions to) built-in rules.

Import Filters

Import Filters from a file that has been created by others.

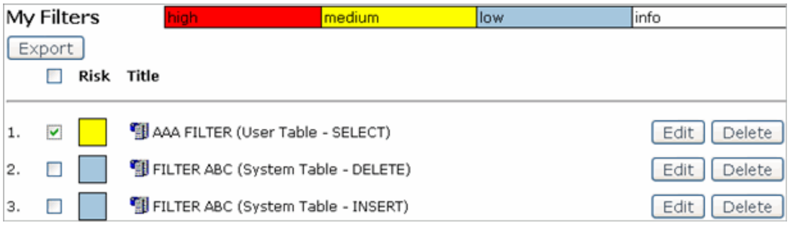
FIGURE: Filter Manager

2. In the **My Filters** portion of the page:

- check one or more Filters that you want to delete

Hint: Check the checkbox (below the **Export** button) to select all Filters at one time.

- click the **Export** button.



My Filters

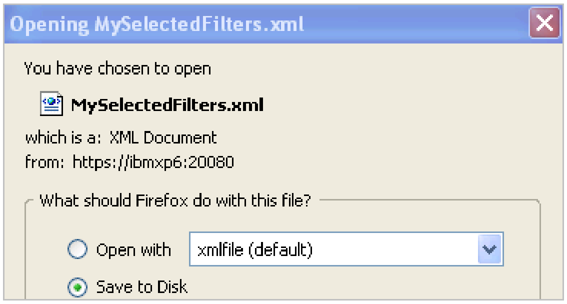
🟥 high 🟨 medium 🟦 low □ info

Export

	□	Risk	Title		
1.	☑	🟨	AAA FILTER (User Table - SELECT)	Edit	Delete
2.	□	🟦	FILTER ABC (System Table - DELETE)	Edit	Delete
3.	□	🟦	FILTER ABC (System Table - INSERT)	Edit	Delete

FIGURE: **Filter Manager** (**My Filters** portion)

The **Open MySelectedFilters.xml** dialog box displays.



Opening MySelectedFilters.xml

You have chosen to open

MySelectedFilters.xml

which is a: XML Document

from: https://ibmxp6:20080

What should Firefox do with this file?

○ Open with xmlfile (default)

● Save to Disk

FIGURE: **Open MySelectedFilters.xml** dialog box

3. Select **Save to Disk** (default).

Caution! Do **not** select **Open With**.

4. Click the **OK** button.

DbProtect Audit and Threat Management exports your selected Filters as an XML file (to your local computer or network).

Reports

This chapter consists of the following topics:

What are Reports?

DbProtect Audit and Threat Management allows you to run **Reports** on Alerts received from registered Sensors. A Report is a tabular and graphical display of the results of a query constrained by user-supplied criteria entered during the Report generation process.

In order to run a Report you must first create a Report **template**. After you create a Report template, you can either:

- immediately generate a Report from an existing template; for more information, see *Generating a Report from an existing template*
- schedule the Report to run later; for more information, see *Scheduling a Report*.

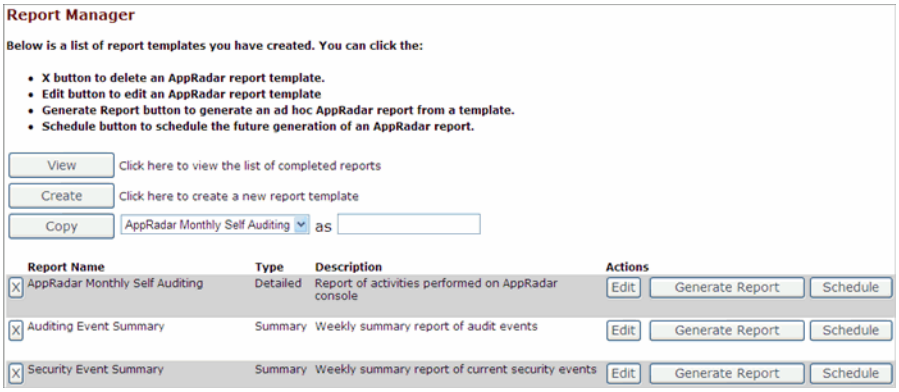
Specifically, you can generate the following DbProtect Audit and Threat Management Reports:

- **Auditing Event Summary Report**. This Report provides a weekly summary of all audit events; for more information, see *Understanding the Built-In Auditing Event Summary Report*.
- **Security Event Summary Report**. This Report provides a weekly summary of your Alerts; for more information, see *Understanding the Built-In Security Event Summary Report*.

- **AppRadar Monthly Self-Auditing Report**. This Report provides detailed information about recent activities performed with DbProtect Audit and Threat Management; for more information, see *Understanding the Built-In DbProtect AppRadar Monthly Self-Auditing Report*.

Understanding the Report Manager

The **Report Manager** is shown below.



Report Manager

Below is a list of report templates you have created. You can click the:

- X button to delete an AppRadar report template.
- Edit button to edit an AppRadar report template
- Generate Report button to generate an ad hoc AppRadar report from a template.
- Schedule button to schedule the future generation of an AppRadar report.

View — Click here to view the list of completed reports

Create — Click here to create a new report template

Copy — AppRadar Monthly Self Auditing as

	Report Name	Type	Description	Actions
X	AppRadar Monthly Self Auditing	Detailed	Report of activities performed on AppRadar console	Edit · Generate Report · Schedule
X	Auditing Event Summary	Summary	Weekly summary report of audit events	Edit · Generate Report · Schedule
X	Security Event Summary	Summary	Weekly summary report of current security events	Edit · Generate Report · Schedule

FIGURE: **Report Manager** page

The **Report Manager** consists of the following portions:

- **View/create/copy.** This portion of the **Report Manager** allows you to:

  -view a generated Report; for more information, see *Viewing a generated Report*

  -create a Report template; for more information, see *Creating a Report template*

  -copy a Report template; for more information, see *Copying a Report template*.

- **Delete buttons.** The delete buttons (represented as **X**s) allow you to delete Report templates; for more information, see *Deleting a Report template*.
- **Template detail.** This portion of the **Report Manager** displays each Report template **Name**, **Type** (i.e., **Summary** or **Detail**), and a brief **Description**.

- **Action buttons.** This portion of the **Report Manager** allows you to:

  -edit a Report template; for more information, see *Editing a Report template*

  -generate a Report from an existing template; for more information, see *Generating a Report from an existing template*

  -schedule a Report; for more information, see *Scheduling a Report*

  -delete a Report template; for more information, see *Deleting a Report template*.

Report navigation, viewing, and output

Every DbProtect Audit and Threat Management Report includes a toolbar with navigation, viewing, and output buttons.

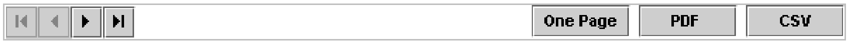


FIGURE: Report navigation, viewing, and output buttons

These buttons allow you to:

- navigate through multiple pages of a Report; for more information, see *Navigating through multiple pages of a Report*
- view the Report as a single page; for more information, see *Viewing your Report as one page*
- create a PDF of your Report, for more information, see *Creating a PDF of your Report (output)*
- export your Report to comma-separated value (CSV) format; for more information, see *Exporting your Report to CSV (output)*.

NAVIGATING THROUGH MULTIPLE PAGES OF A REPORT

To navigate through multiple pages of a Report:

1. DbProtect Audit and Threat Management Reports are sometimes dozens or hundreds of pages long. You can click the **navigation buttons** to move forward and backwards through the pages Report. Specifically, you can click the:

   - **|<** button to go **back** to the first page of the Report
   - < button to go **back** one page in the Report
   - >button to go **forward** one page in the Report
   - **>|** button to go **forward** to the last page of the Report.

VIEWING YOUR REPORT AS ONE PAGE

To view your Report as one page:

1. If you want to view your Report as just one page, click the **One Page** button in the **viewing and output buttons** portion of the Report.

The navigation buttons no longer display. Your Report displays as just one page. You can click the **<Back** button on your web browser to go back to the multiple page Report view.

CREATING A PDF OF YOUR REPORT (OUTPUT)

Note: You **must** have Adobe Acrobat installed.

To create a PDF of your Report:

1. Click the **PDF** button in the **viewing and output buttons** portion of the Report.

DbProtect Audit and Threat Management generates a PDF of your Report.

Scheduling your Reports

The **Report Scheduling** page allows you to schedule *how often* and *when* DbProtect Audit and Threat Management should generate a selected Report template into a Report.

The **Task Frequency:** drop-down on the **Report Scheduling** page allows you to select how often you want DbProtect Audit and Threat Management to generate the scheduled Report. Your choices are: **Once**, **Daily**, **Weekly**, and **Monthly**. The **Date Settings** portion of the **Report Scheduling** page allows you to enter the exact dates and times when the scheduled Report should begin and end. The following table explains different job frequency scenarios.

If you specify:	Then:
• **Task Frequency** = `DAILY` • **Start Date** = `10/01/06` • **End Date** = `12/31/06` • **Start Time** = `10:00 A.M.`	DbProtect Audit and Threat Management first generates your Report at 10:00 A.M. on October 1, 2006, then generates a new Report *every day* (i.e., on October 2, 3, 4, 5, 6, 7, and so on) at 10:00 A.M., until the end date, i.e., December 31, 2006.
• **Task Frequency** = `WEEKLY` • **Start Date** = `10/01/06` • **End Date** = `12/31/06` • **Start Time** = `10:00 A.M.`	DbProtect Audit and Threat Management first generates your Report at 10:00 A.M. on October 1, 2006, then generates a new Report *every week* (i.e., on October 8, 15, 22, and so on) at 10:00 A.M., until the end date, i.e., December 31, 2006.
• **Task Frequency** = `MONTHLY` • **Start Date** = `10/01/06` • **End Date** = `12/31/06` • **Start Time** = `10:00 A.M.`	DbProtect Audit and Threat Management first generates your Report at 10:00 A.M. on October 1, 2006, then generates a new Report *every month* (i.e., on November 1 and December 1) at 10:00 A.M., until the end date, i.e., December 31, 2006.

For more information, see *Scheduling a Report*.

EXPORTING YOUR REPORT TO CSV (OUTPUT)

You can save your Report in CSV format, or open it with the default application associated with the `.csv` extension (typically Excel).

Note: Excel cannot handle more than 65,536 rows of data. If your Report exceeds this size, you can select to save the `.csv` file to your hard drive or network, and open it with another application of your choice.

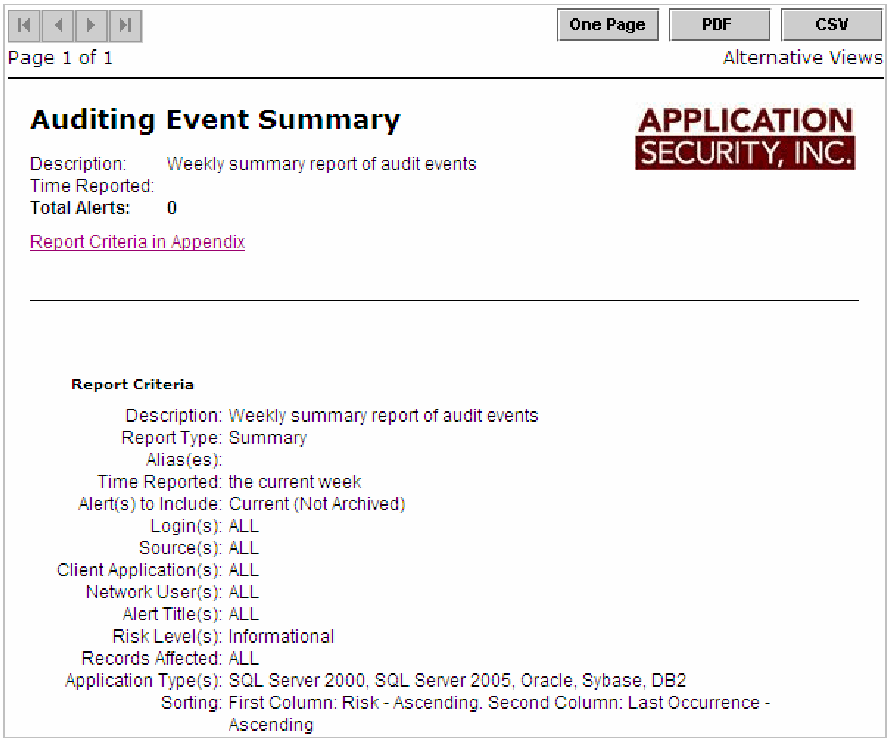
To export your Report to CSV:

1. Click the **CSV** button in the **viewing and output buttons** portion of the Report.

If Excel is the default application associated with the `.csv` extension, then Excel launches automatically and displays your Report data.

Understanding the Built-In Auditing Event Summary Report

The **Auditing Event Summary Report** is a built-in summary Report. It provides a weekly summary of all your audit events.



Auditing Event Summary

Description: Weekly summary report of audit events
Time Reported:
Total Alerts: 0

Report Criteria in Appendix

Report Criteria

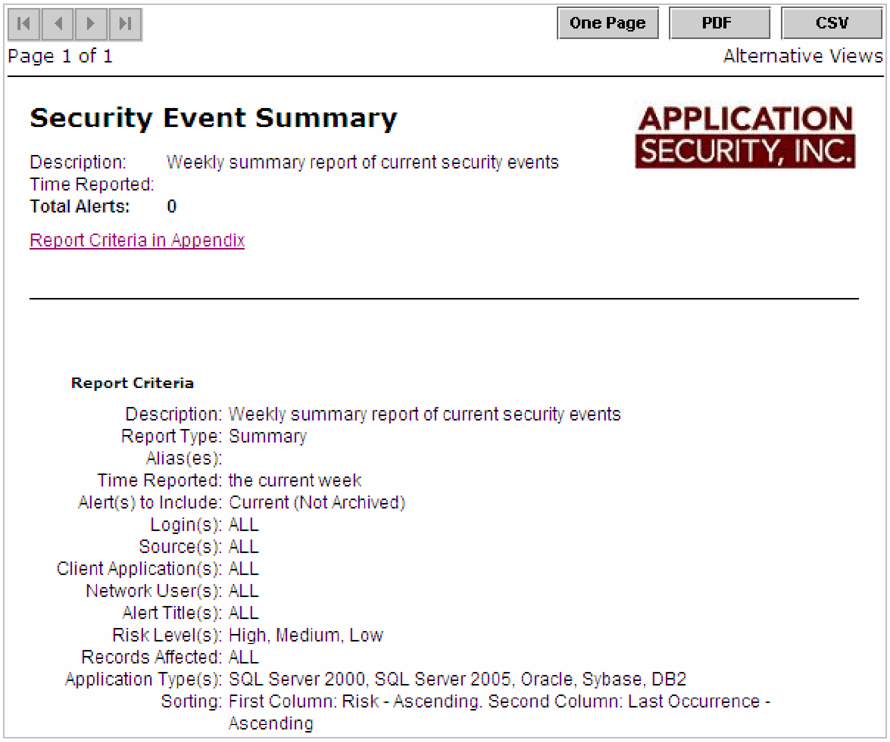
Description: Weekly summary report of audit events
Report Type: Summary
Alias(es):
Time Reported: the current week
Alert(s) to Include: Current (Not Archived)
Login(s): ALL
Source(s): ALL
Client Application(s): ALL
Network User(s): ALL
Alert Title(s): ALL
Risk Level(s): Informational
Records Affected: ALL
Application Type(s): SQL Server 2000, SQL Server 2005, Oracle, Sybase, DB2
Sorting: First Column: Risk - Ascending. Second Column: Last Occurrence - Ascending

FIGURE: Auditing Event Summary Report

The navigation, viewing, and output buttons at the top of the Report allow you to navigate through multiple pages of a Report, view the Report as a single page, create a PDF of your Report, and export your Report to CSV; for more information, see *Report navigation, viewing, and output*.

Understanding the Built-In Security Event Summary Report

The **Security Event Summary Report** is a built-in summary Report. It provides a weekly summary of your Alerts.



Security Event Summary

Description: Weekly summary report of current security events
Time Reported:
Total Alerts: 0

Report Criteria in Appendix

Report Criteria

Description: Weekly summary report of current security events
Report Type: Summary
Alias(es):
Time Reported: the current week
Alert(s) to Include: Current (Not Archived)
Login(s): ALL
Source(s): ALL
Client Application(s): ALL
Network User(s): ALL
Alert Title(s): ALL
Risk Level(s): High, Medium, Low
Records Affected: ALL
Application Type(s): SQL Server 2000, SQL Server 2005, Oracle, Sybase, DB2
Sorting: First Column: Risk - Ascending. Second Column: Last Occurrence - Ascending

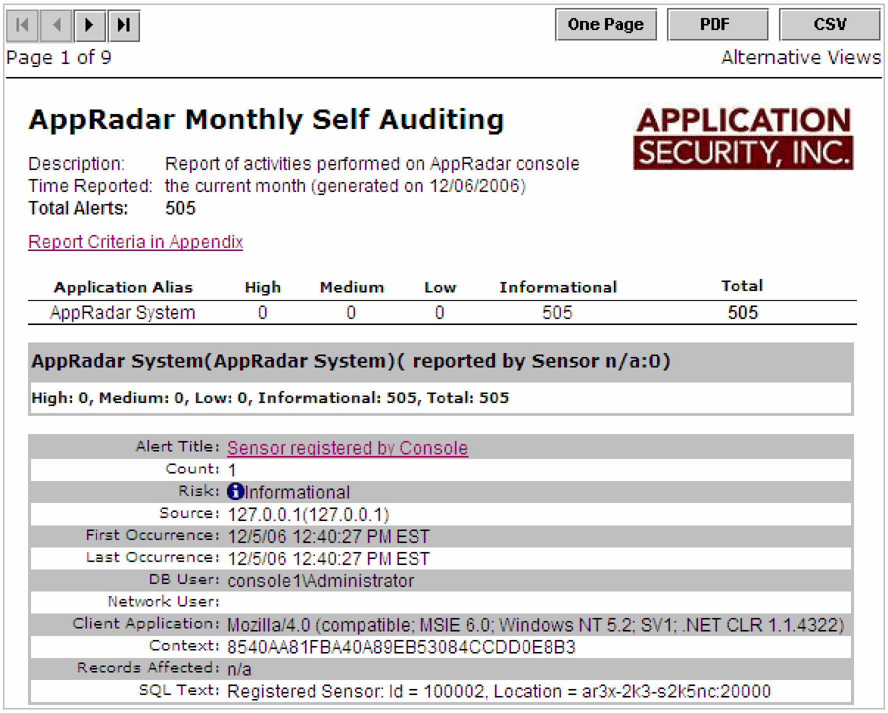
FIGURE: Security Event Summary Report

The navigation, viewing, and output buttons at the top of the Report allow you to navigate through multiple pages of a Report, view the Report as a single page, create a PDF of your Report, and export your Report to CSV; for more information, see *Report navigation, viewing, and output*.

Understanding the Built-In DbProtect AppRadar Monthly Self-Auditing Report

The **DbProtect AppRadar Monthly Self-Auditing Report** is a built-in detail Report. It provides detailed information about recent activities performed with DbProtect Audit and Threat Management.

Note: The **Records Affected:** rows are result sets, which refer to the number of records returned as the result of executing a SQL statement; for more information, see *Understanding result sets*. When DbProtect Audit and Threat Management stores identical SQL statements, and their **Risk Level:** is **Info-1**, **Info-2**, or **Info-3**, then DbProtect AppRadar aggregates the **Records Affected:**.



Page 1 of 9

AppRadar Monthly Self Auditing

Description: Report of activities performed on AppRadar console
Time Reported: the current month (generated on 12/06/2006)
Total Alerts: 505

Report Criteria in Appendix

Application Alias	High	Medium	Low	Informational	Total
AppRadar System	0	0	0	505	505

AppRadar System(AppRadar System)(reported by Sensor n/a:0)

High: 0, Medium: 0, Low: 0, Informational: 505, Total: 505

Alert Title:	Sensor registered by Console
Count:	1
Risk:	ℹInformational
Source:	127.0.0.1(127.0.0.1)
First Occurrence:	12/5/06 12:40:27 PM EST
Last Occurrence:	12/5/06 12:40:27 PM EST
DB User:	console1\Administrator
Network User:	
Client Application:	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; SV1; .NET CLR 1.1.4322)
Context:	8540AA81FBA40A89EB53084CCDD0E8B3
Records Affected:	n/a
SQL Text:	Registered Sensor: Id = 100002, Location = ar3x-2k3-s2k5nc:20000

FIGURE: DbProtect AppRadar Monthly Self-Auditing Report

The navigation, viewing, and output buttons at the top of the Report allow you to navigate through multiple pages of a Report, view the Report as a single page, create a PDF of your Report, and export your Report to CSV; for more information, see *Report navigation, viewing, and output*.

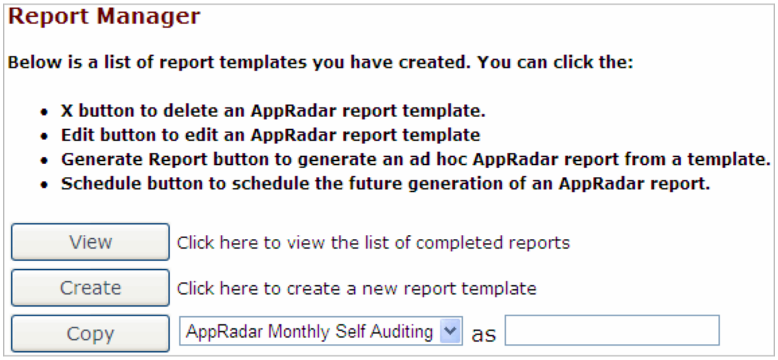
Creating a Report template

To create a Report template:

Do one of the following to display the **Report Manager** page:

- Click the **Reports** workflow link on the **Home** page.
- Click the **Reports** tab from anywhere on the page.

For more information, see *Understanding the Report Manager*.



Report Manager

Below is a list of report templates you have created. You can click the:

- X button to delete an AppRadar report template.
- Edit button to edit an AppRadar report template
- Generate Report button to generate an ad hoc AppRadar report from a template.
- Schedule button to schedule the future generation of an AppRadar report.

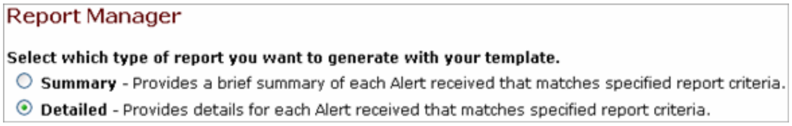
Click here to view the list of completed reports

Click here to create a new report template

FIGURE: Report Manager

2. Click the **Create** button in the **Report Manager** portion of the page.

The next **Report Manager** page displays.



Report Manager

Select which type of report you want to generate with your template.

○ **Summary** - Provides a brief summary of each Alert received that matches specified report criteria.

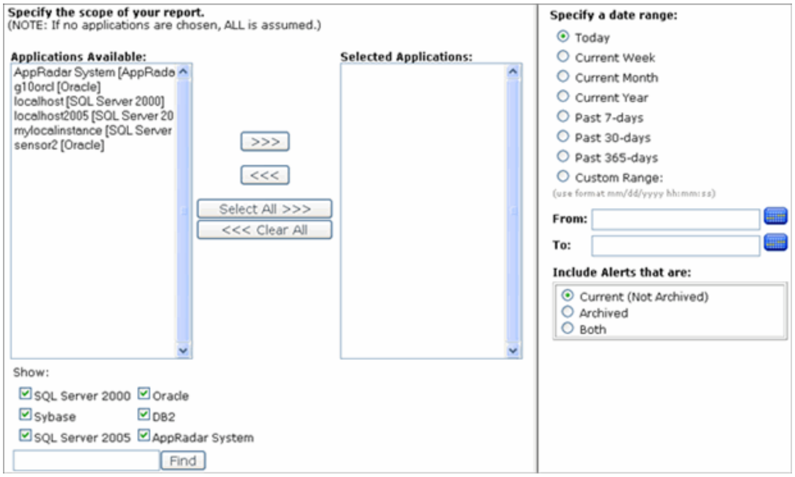
● **Detailed** - Provides details for each Alert received that matches specified report criteria.

FIGURE: Report Manager

3. Select whether you want to create a template for a **Summary Report** or a **Details Report**; for more information, see *What are Reports?*

4. Click the **Next** button.

The next **Report Manager** page displays (the same page for either Report type selected).



Specify the scope of your report.
(NOTE: If no applications are chosen, ALL is assumed.)

Applications Available:
AppRadar System [AppRada
g10orcl [Oracle]
localhost [SQL Server 2000]
localhost2005 [SQL Server 20
mylocalinstance [SQL Server
sensor2 [Oracle]

Selected Applications:

Show:
☑ SQL Server 2000 ☑ Oracle
☑ Sybase ☑ DB2
☑ SQL Server 2005 ☑ AppRadar System

Specify a date range:
● Today
○ Current Week
○ Current Month
○ Current Year
○ Past 7-days
○ Past 30-days
○ Past 365-days
○ Custom Range:
(use format mm/dd/yyyy hh:mm:ss)

From:
To:

Include Alerts that are:
● Current (Not Archived)
○ Archived
○ Both

FIGURE: Report Manager

5. This page allows you to specify Report criteria used to constrain which Alerts are included in your Report. It consists of the following portions:

- **Specify the scope of your Report.** This portion of the page allows you to highlight which applications you want to run your Report on, answering the question: "what Alerts have these applications triggered?"

  You can move applications from the **Application Available:** scroll-down box to the **Selected Applications:** scroll-down box, or vice versa, by highlighting an application and clicking the **<<<** or **>>>** button. Clicking the **>>>** button *adds* the highlighted application *to* the list of applications to Report on. Clicking the **<<<** button *removes* the highlighted application *from* the list of applications to Report on.

Hint: Click the **Select All>>>** button to move all applications from the **Applications Available:** scroll-down box to the **Selected Applications:** scroll-down box. Or, click the **<<<Clear All** button to move all applications from the **Selected Applications:** scroll-down box back to the **Applications Available:** scroll-down box.

- **Specify a date range.** This portion of the page allows you to specify a Reporting date range. You can select:

  -Today

  -Current Week

  -Current Month

  -Current Year

  -Past 7-days

  -Past 30-days

  -Past 365-days

  -Custom Range.

  If you select **Custom Range**, then you must enter a date range (down to a second) in the **From:** and **To:** fields, using the format `mm/dd/yyyy hh:mm:ss`.

Hint: You can click the calendar icons next to the **From:** and **To:** fields to display a calendar pop up and select your "from" and "to" dates in the date range.

- **Include Alerts.** This portion of the page allows you to select to Report on Alerts that are:

  -Current (Not Archived)

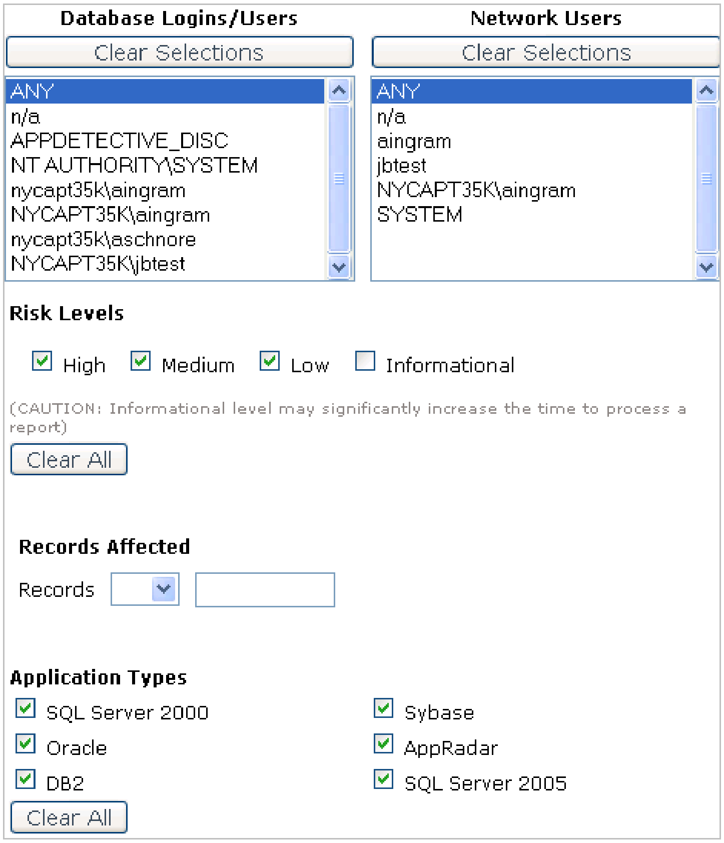
  -Archived

  -Both.

- **Show.** This portion of the page allows you to specify which database platforms you want to Report on (or **not** Report on). For example, maybe you only want to know about Oracle Alerts. You can also select **AppRadar System** if you want to know about system Alerts.
- **Find tool.** This portion of the page allows you to enter a search term in the text box, then click the **Find** button.

6. Click the **Next** button.

The next **Report Manager** page displays (the same page for both Report types). The left half of the page looks like this:



Database Logins/Users

Clear Selections

- ANY
- n/a
- APPDETECTIVE_DISC
- NT AUTHORITY\SYSTEM
- nycapt35k\aingram
- NYCAPT35K\aingram
- nycapt35k\aschnore
- NYCAPT35K\jbtest

Network Users

Clear Selections

- ANY
- n/a
- aingram
- jbtest
- NYCAPT35K\aingram
- SYSTEM

Risk Levels

☑ High ☑ Medium ☑ Low □ Informational

(CAUTION: Informational level may significantly increase the time to process a report)

Clear All

Records Affected

Records

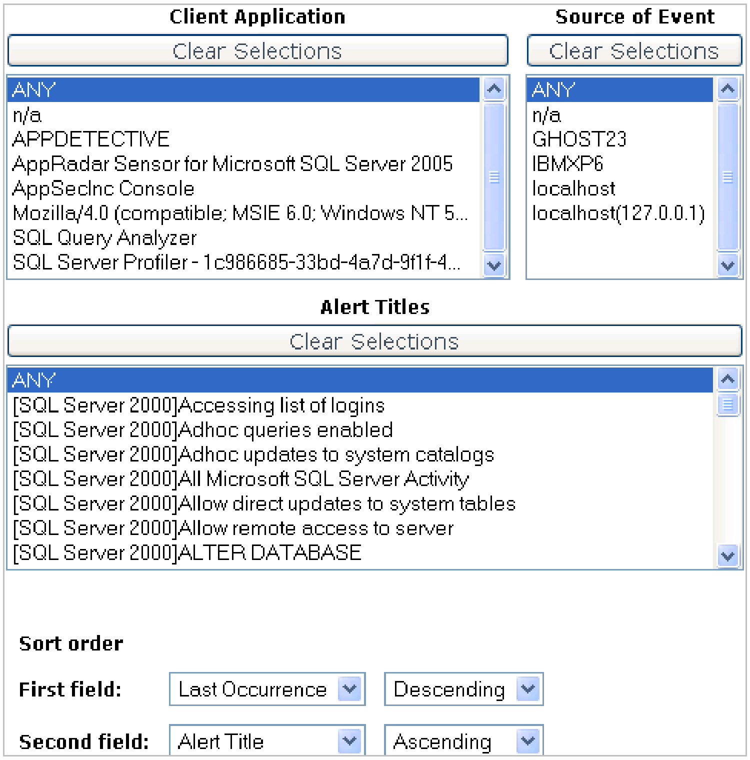
Application Types

☑ SQL Server 2000 ☑ Sybase
☑ Oracle ☑ AppRadar
☑ DB2 ☑ SQL Server 2005

Clear All

FIGURE: **Report Manager** (left half of the page)

The **right half** of the page looks like this:



Client Application:
ANY
n/a
APPDETECTIVE
AppRadar Sensor for Microsoft SQL Server 2005
AppSecInc Console
Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5...
SQL Query Analyzer
SQL Server Profiler - 1c986685-33bd-4a7d-9f1f-4...

Source of Event:
ANY
n/a
GHOST23
IBMXP6
localhost
localhost(127.0.0.1)

Alert Titles:
ANY
[SQL Server 2000]Accessing list of logins
[SQL Server 2000]Adhoc queries enabled
[SQL Server 2000]Adhoc updates to system catalogs
[SQL Server 2000]All Microsoft SQL Server Activity
[SQL Server 2000]Allow direct updates to system tables
[SQL Server 2000]Allow remote access to server
[SQL Server 2000]ALTER DATABASE

Sort order

First field: Last Occurrence Descending

Second field: Alert Title Ascending

FIGURE: **Report Manager** (right half of the page)

The **Report Manager** page allows you to specify Report criteria used to constrain which Alerts are included in your Report. Specifically, you must specify criteria in the following sections:

- **Database Logins/Users.** Allows you to highlight login/users to Report on, i.e., who logged in to the database, with or without success?
- **Network Users.** Allows you to highlight specific network users to Report on, i.e., did a specific network user generate Alerts?
- **Client Application.** Allows you to highlight which applications you want to Report on, i.e., which client applications generated Alerts?
- **Source of Event.** Allows you to highlight which database client computer you want to report on, i.e., on which database client computer did Alerts originate?
- **Alert Titles.** Allows you to highlight which specific Alerts you want to Report on.

Hint: Click the **Clear Selections** button to clear your highlighted selections.

- **Risk Level.** Select a risk level for the audit event, i.e., **Informational** (i.e., **Info-1**, **Info-2**, **Info-3**, and **Info-4**).

Note: The **Informational** risk levels are typically for audit events. Audit events are written to a table in the DbProtect database, but not displayed on the **Alert Manager** page on the UI. For more information, see *What do the risk levels mean?* If you check an **Informational** risk level checkbox (and depending on which Policies you have deployed) it may take a while to run your Reports because of the volume of data the DbProtect Audit and Threat Management reporting engine needs to process.

Hint: Click the **Clear All** button to clear your checked selections.

- **Records Affected.** Use the drop-down to select how many affected records you want to Report on. Or enter a value in the **Records Affected** field.

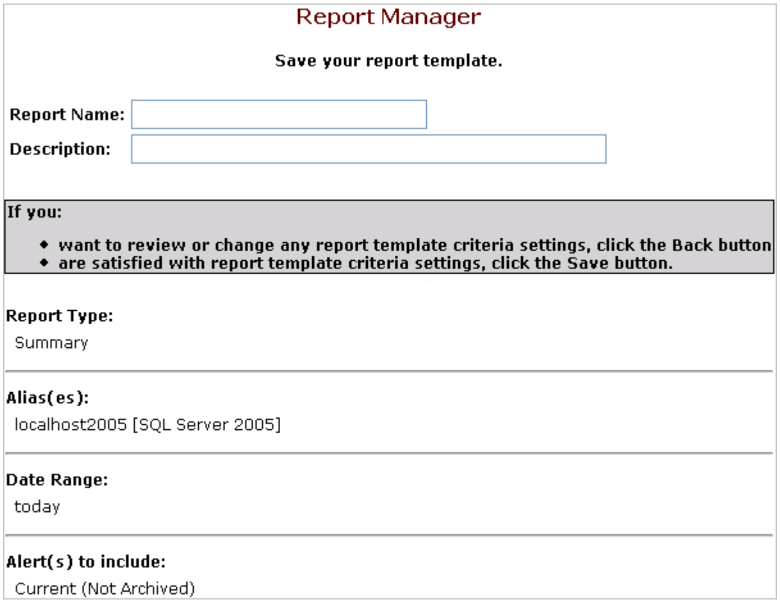
Note: This row is a result set, which refers to the number of records returned as the result of executing a SQL statement; for more information, see *Understanding result sets*. For queries that join multiple tables, **Records Affected** represents the number of rows the query retrieves. DbProtect Audit and Threat Management does **not** break down results by table. For example, if you run a query that joins your `CUSTOMER` table to your `CREDIT CARD` table, and the **Records Affected** indicates five rows, you can interpret this result to mean five customers with one credit card, or one customer with five credit cards.

- **Application Types.** Allows you to check one or more risk levels to Report on, i.e., **Microsoft SQL Server 2000/2005/2008**, **Oracle**, **Sybase**, **DB2**, or **AppRadar**. You **must** check at least one checkbox.
- **Sort Order.** Allows you to specify how you want to display your Report data.

  -**First field:**. and **Second field:** Use these drop-downs to select which data you want to display in the first field of your Report. Your choices are: **Count**, **Alert Title**, **Risk**, **Source**, **First Occurrence**, **Last Occurrence**, and **Context**.
- **Ascending** and **Descending**. Use these drop-downs to select whether you want your Report data to display in ascending or descending order, respectively.

7. Click the **Next** button.

The next **Report Manager** page displays.



Report Manager

Save your report template.

Report Name:

Description:

If you:

- want to review or change any report template criteria settings, click the Back button
- are satisfied with report template criteria settings, click the Save button.

Report Type:
Summary

Alias(es):
localhost2005 [SQL Server 2005]

Date Range:
today

Alert(s) to include:
Current (Not Archived)

FIGURE: Report Manager

8. This page allows you to enter descriptive information about the Exception.

- ***Report Name** (required field). Enter the Report template name. There are no strict naming restrictions for Exceptions, other than size limit and alphanumeric characters.
- **Description.** Enter a Report template description.

9. At this point, the **Report Manager** has enough information to save your Report template. The buttons at the bottom of this page allow you to go back and change settings, save your Report template and generate the Report later, or save the Report template and generate the Report now.

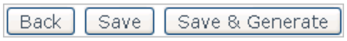


FIGURE: **Report Manager** buttons

- If you want to review or change any settings you can click the **Back** button or any link that displays on the page.

- If you are satisfied with your settings and you want to save your Report template and generate a Report *later*, then click the **Save** button. Your Report template is saved. The main **Report Manager** page displays your Report template. You can click the **Generate Report** button to generate the Report at any time; for more information, see *Generating a Report from an existing template*.
- If you are satisfied with your settings and you want to save your Report template and generate a Report *now*, then click the **Save & Generate** button.

DbProtect Audit and Threat Management displays your Report results on a separate page; for more information, see *Report navigation, viewing, and output*.

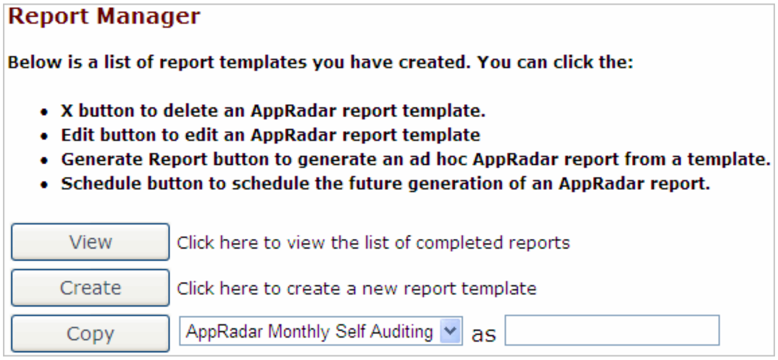
Generating a Report from an existing template

To generate a Report from an existing template:

1. Do one of the following to display the **Report Manager** page:

- Click the **Reports** workflow link on the **Home** page.
- Click the **Reports** tab from anywhere on the page.

For more information, see *Understanding the Report Manager*.



Report Manager

Below is a list of report templates you have created. You can click the:

- X button to delete an AppRadar report template.
- Edit button to edit an AppRadar report template
- Generate Report button to generate an ad hoc AppRadar report from a template.
- Schedule button to schedule the future generation of an AppRadar report.

View — Click here to view the list of completed reports

Create — Click here to create a new report template

Copy — AppRadar Monthly Self Auditing as

FIGURE: Report Manager

2. Click the **Generate Report** action button next to a Report template.

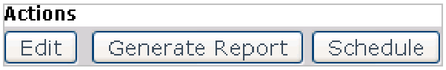


FIGURE: **Action** buttons

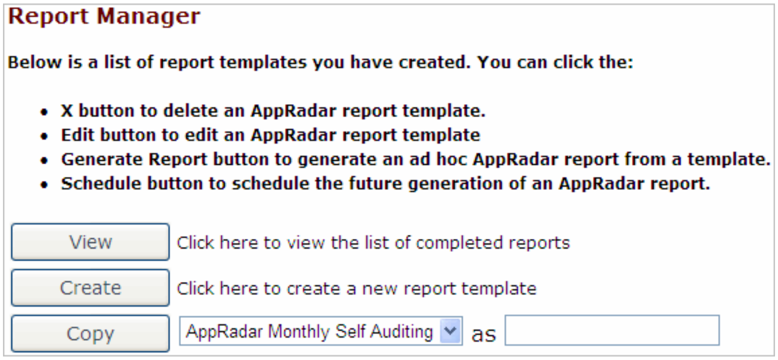
DbProtect Audit and Threat Management displays your Report results on a separate page; for more information, see *Report navigation, viewing, and output*.

Viewing a generated Report

To view a generated Report:

1. Do one of the following to display the **Report Manager** page:
   - Click the **Reports** workflow link on the **Home** page.
   - Click the **Reports** tab from anywhere on the page.

For more information, see *Understanding the Report Manager.*



Report Manager

Below is a list of report templates you have created. You can click the:

- **X button to delete an AppRadar report template.**
- **Edit button to edit an AppRadar report template**
- **Generate Report button to generate an ad hoc AppRadar report from a template.**
- **Schedule button to schedule the future generation of an AppRadar report.**

View — Click here to view the list of completed reports

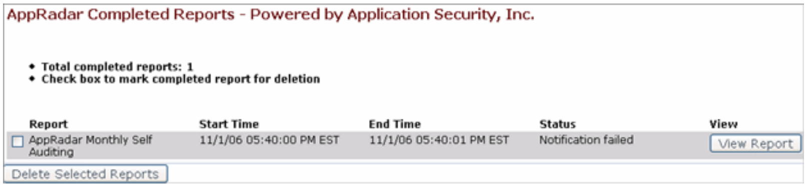
Create — Click here to create a new report template

Copy — AppRadar Monthly Self Auditing as

FIGURE: Report Manager

2. Click the **View** button.

The **Completed Reports** page displays your scheduled Reports, i.e., Reports that you scheduled from a template, **not** ad hoc Reports; for more information, see *Scheduling a Report.*



AppRadar Completed Reports - Powered by Application Security, Inc.

- **Total completed reports: 1**
- **Check box to mark completed report for deletion**

Report	Start Time	End Time	Status	View
□ AppRadar Monthly Self Auditing	11/1/06 05:40:00 PM EST	11/1/06 05:40:01 PM EST	Notification failed	View Report

Delete Selected Reports

FIGURE: Report Manager

3. Click the **View Report** button next to the generated Report that you want to view.

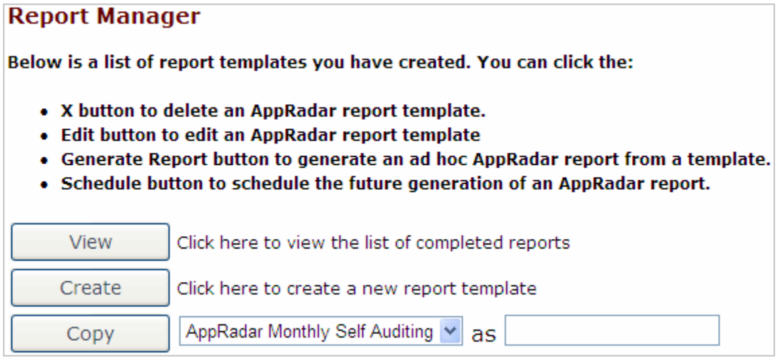
DbProtect Audit and Threat Management displays your Report results on a separate page; for more information, see *Report navigation, viewing, and output.*

Editing a Report template

To edit a Report template:

1. Do one of the following to display the **Report Manager** page:
   - Click the **Reports** workflow link on the **Home** page.
   - Click the **Reports** tab from anywhere on the page.

Assuming you've created Report templates, they display, too. If you have **not** created a Report template, see *Creating a Report template*.



Report Manager

Below is a list of report templates you have created. You can click the:

- X button to delete an AppRadar report template.
- Edit button to edit an AppRadar report template
- Generate Report button to generate an ad hoc AppRadar report from a template.
- Schedule button to schedule the future generation of an AppRadar report.

View Click here to view the list of completed reports

Create Click here to create a new report template

Copy AppRadar Monthly Self Auditing as

FIGURE: Report Manager

2. Click the **Edit** action button next to a Report template.

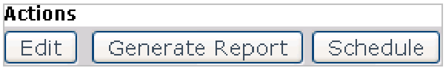


FIGURE: **Action** buttons

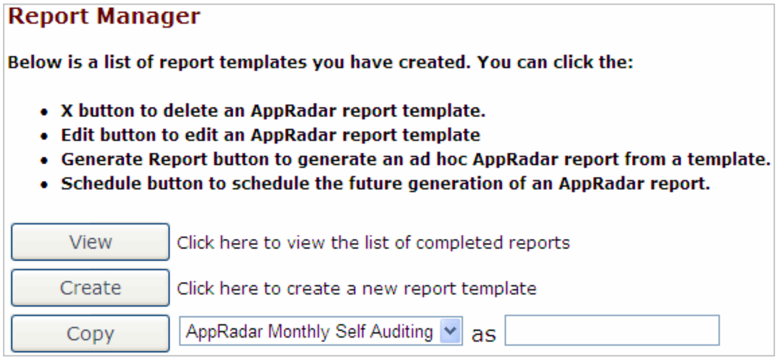
The next **Report Manager** displays your existing Report criteria. Now you can edit your Report template criteria as if you were creating a new Report template; for more information, see *Creating a Report template*.

Deleting a generated Report

To delete a generated Report:

1. Do one of the following to display the **Report Manager** page:
   - Click the **Reports** workflow link on the **Home** page.
   - Click the **Reports** tab from anywhere on the page.

For more information, see *Understanding the Report Manager*.



Report Manager

Below is a list of report templates you have created. You can click the:

- **X button to delete an AppRadar report template.**
- **Edit button to edit an AppRadar report template**
- **Generate Report button to generate an ad hoc AppRadar report from a template.**
- **Schedule button to schedule the future generation of an AppRadar report.**

Click here to view the list of completed reports

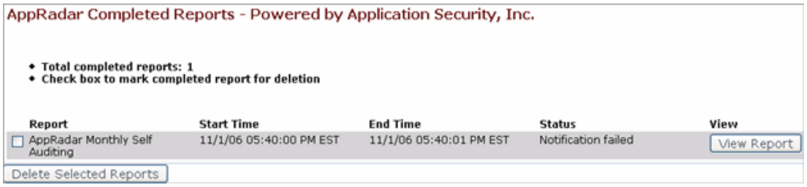
Click here to create a new report template

AppRadar Monthly Self Auditing as

FIGURE: Report Manager

2. Click the **View** button.

The **AppRadar Completed Reports** page displays all your generated Reports, i.e., Reports that you scheduled from a template; for more information, see *Scheduling a Report*.



AppRadar Completed Reports - Powered by Application Security, Inc.

- **Total completed reports: 1**
- **Check box to mark completed report for deletion**

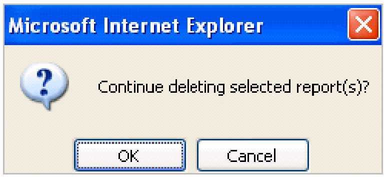
Report	Start Time	End Time	Status	View
□ AppRadar Monthly Self Auditing	11/1/06 05:40:00 PM EST	11/1/06 05:40:01 PM EST	Notification failed	View Report

FIGURE: Report Manager

3. Check the generated Report(s) that you want to delete.

4. Click the **Delete Selected Reports** button.

A pop up prompts you to confirm the delete.



Continue deleting selected report(s)?

FIGURE: Report Manager

5. Click the **OK** button to delete.

Your selected generated Report(s) is/are deleted.

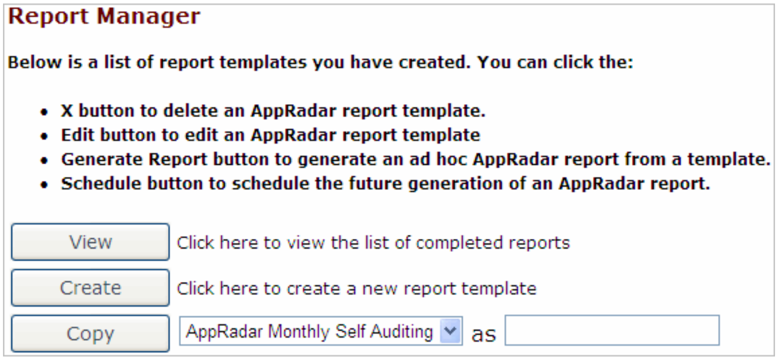
Deleting a Report template

To delete a Report template:

1. Do one of the following to display the **Report Manager** page:

- Click the **Reports** workflow link on the **Home** page.
- Click the **Reports** tab from anywhere on the page.

For more information, see *Understanding the Report Manager*.



Report Manager

Below is a list of report templates you have created. You can click the:

- **X button to delete an AppRadar report template.**
- **Edit button to edit an AppRadar report template**
- **Generate Report button to generate an ad hoc AppRadar report from a template.**
- **Schedule button to schedule the future generation of an AppRadar report.**

View — Click here to view the list of completed reports

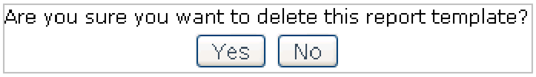
Create — Click here to create a new report template

Copy — AppRadar Monthly Self Auditing as

FIGURE: Report Manager

2. Click the **X** button next to the Report template you want to delete.

A confirmation page prompts you to confirm the delete.



Are you sure you want to delete this report template?

FIGURE: Report Manager

3. Click the **Yes** button to delete.

Your Report template is deleted.

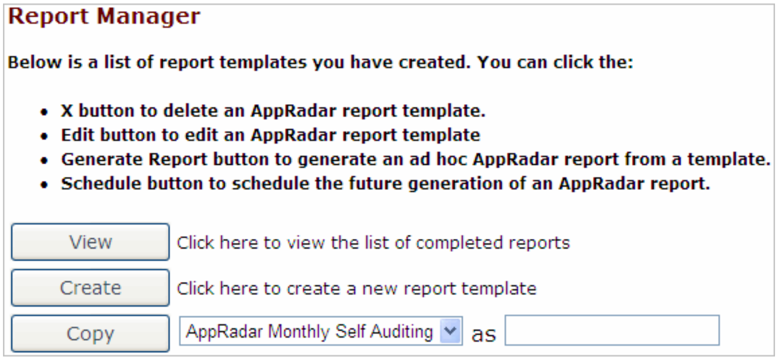
Copying a Report template

To copy a Report template:

1. Do one of the following:

- Click the **Report Manager** workflow link on the **Home** page.
- Click the **Reports** tab from anywhere on the page.

The **Report Manager** page displays.



Report Manager

Below is a list of report templates you have created. You can click the:

- X button to delete an AppRadar report template.
- Edit button to edit an AppRadar report template
- Generate Report button to generate an ad hoc AppRadar report from a template.
- Schedule button to schedule the future generation of an AppRadar report.

View
Click here to view the list of completed reports
Create
Click here to create a new report template
Copy
AppRadar Monthly Self Auditing
as

FIGURE: Report Manager

2. Use the template drop-down to select which existing Report template you want to copy.

3. Enter the new Report name in the **as** field (e.g., `Copy of Audit Event Summary Template`).

4. Click the **Copy** button to copy the Report template under the name specified in Step 3.

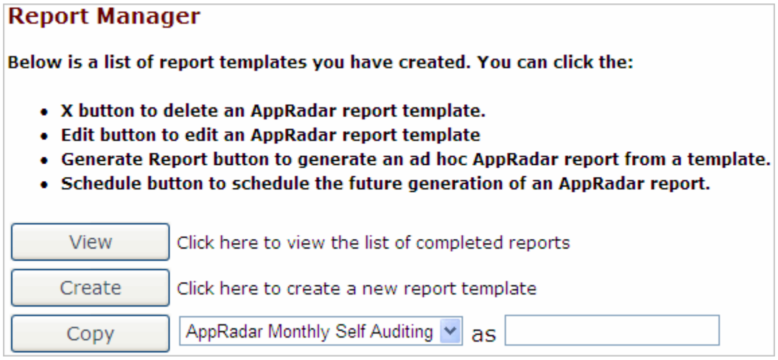
Your copied Report displays on the **Report Manager** list of available Reports. You can now edit the copied Report template to differentiate it from the original Report template; for more information, see *Editing a Report template*.

Scheduling a Report

To schedule a Report:

1. Do one of the following to display the **Report Manager** page:
   - Click the **Reports** workflow link on the **Home** page.
   - Click the **Reports** tab from anywhere on the page.

For more information, see *Understanding the Report Manager*.



Report Manager

Below is a list of report templates you have created. You can click the:

- X button to delete an AppRadar report template.
- Edit button to edit an AppRadar report template
- Generate Report button to generate an ad hoc AppRadar report from a template.
- Schedule button to schedule the future generation of an AppRadar report.

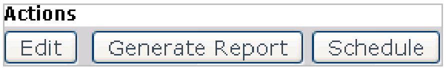
View Click here to view the list of completed reports

Create Click here to create a new report template

Copy AppRadar Monthly Self Auditing as

FIGURE: Report Manager

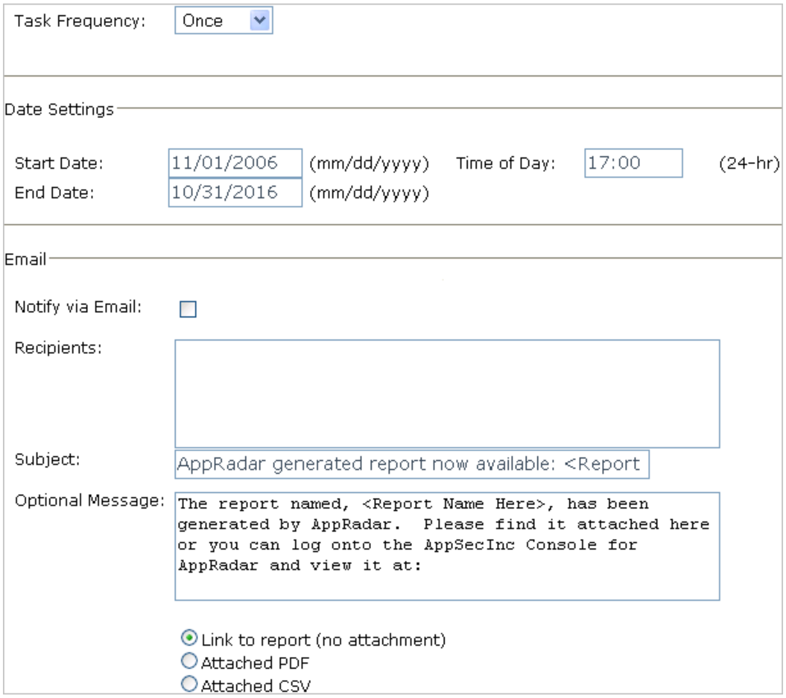
2. Click the **Schedule** action button next to a Report template.



Actions

FIGURE: **Action** buttons

The **Report Scheduling** page displays.



Task Frequency: Once

Date Settings

Start Date: 11/01/2006 (mm/dd/yyyy) Time of Day: 17:00 (24-hr)
End Date: 10/31/2016 (mm/dd/yyyy)

Email

Notify via Email: □

Recipients:

Subject: AppRadar generated report now available: <Report

Optional Message:

```
The report named, <Report Name Here>, has been
generated by AppRadar.  Please find it attached here
or you can log onto the AppSecInc Console for
AppRadar and view it at:
```

● Link to report (no attachment)
○ Attached PDF
○ Attached CSV

FIGURE: **Report Scheduling** page

3. The **Report Scheduling** page allows you to schedule *how often* and *when* DbProtect Audit and Threat Management should generate the selected Report template into a Report. You can also *email* others as soon as DbProtect Audit and Threat Management successfully generates the Report, attach the Report itself to an email, and more. Specifically, you must specify scheduling criteria in the following portions:

- **Job Frequency.** Use the **Task Frequency:** drop-down to select how often you want DbProtect Audit and Threat Management to generate the scheduled Report. Your choices are: **Once**, **Daily**, **Weekly**, and **Monthly**. For more information, see *Scheduling your Reports*.
- **Date Settings.** Enter the exact *dates* when the scheduled Report should begin and end in the **Start Date:** and **End Date:** fields, respectively. You must use the `mm/dd/yyyy` format (e.g., `01/01/2007`). Also enter the exact *time* when the scheduled Report should begin. You must use the 24 hour `HH:MM` format (e.g., `18:00` = 6 P.M.). For more information, see *Scheduling your Reports*.

- **Email.** This portion of the **Report Scheduling** page consists of the following:

  -**Notify via Email:**. Check this box to indicate you want DbProtect Audit and Threat Management to email the people in the **Recipients:** field as soon as DbProtect Audit and Threat Management successfully generates your Report.

  -**Recipients:**. Enter your comma-separated list of email addresses in this field, e.g., `jsmith@company.com`, `ajones@company.com`, etc.

Caution! Your list of email addresses **cannot** exceed 256 characters.

- **Subject:**. You **must** enter an email subject. The default subject text is: `DbProtect AppRadar generated Report now available: <Report Name Here>` where `<Report Name Here>` is the name of your Report template. You can overwrite this text.
- **Optional Message:**. Optionally, you can enter a message that will display in the body of the email to your recipients. The default message text is:

  ```
  The Report named, <Report Name Here>, has been generated by
  DbProtect AppRadar. Please find it attached here or you can log
  into DbProtect AppRadar and view it at:
  ```

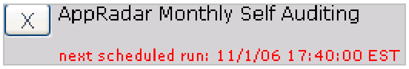
Note: DbProtect Audit and Threat Management automatically appends a Report link to this default message.

  `<Report Name Here>` is the name of your Report template. You can overwrite this text.

- **Link to Report (no attachment)**. Select to append a Report link to your email.
- **Attached PDF**. Select to attach the generated Report to your email as a PDF.
- **Attached CSV**. Select to attach the generated Report to your email as a comma-separated values (CSV) file.

4. When you're done, click the **Schedule** button at the bottom of the page.

The **Report Manager** re-displays. A message in red text displays below the scheduled Report template, i.e., next scheduled run: `<mm/dd/yy> <hh:mm:ss> <your time zone>`



AppRadar Monthly Self Auditing

next scheduled run: 11/1/06 17:40:00 EST

FIGURE: **Report Manager**

System Settings: Email Forwarding Rules, Forwarding Settings, Email Server Settings

This chapter consists of the following topics:

- *What are system settings?*
- *Understanding the System Settings page*
- *Email Forwarding Rules*
- *Forwarding Settings*
- *Email Server Settings.*

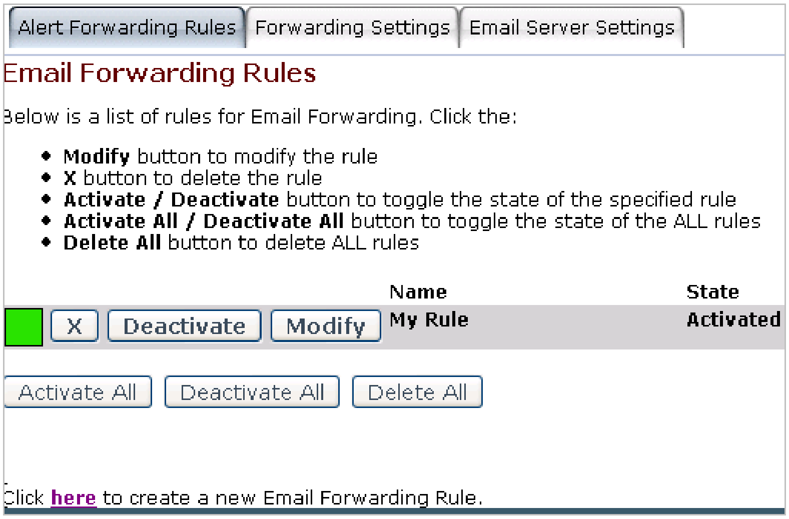
What are system settings?

System settings refer to the following:

- **Email Forwarding Rules**. Allow you to *email* Alerts instead of (or in addition to) using the SNMP trap, file, or Syslog methods specified during the configuration/deployment of an instance for a registered Sensor; for more information, see *Email Forwarding Rules*.
- **Forwarding Settings.** Allow you to specify the **polling frequency** (i.e., the interval between each successive check for Alerts to be forwarded via email) and the **maximum number of Alerts to handle** (i.e., if the number of Alerts is exceeded, Audit and Threat Management does **not** send an email); for more information, see *Forwarding Settings*.
- **Email Server Settings.** Allow you to configure email server properties (e.g., outbound SMTP server name and port number, maximum attachment size, etc.) to accommodate the forwarding of Alerts and Reports via email; for more information, see *Email Server Settings*.

Understanding the System Settings page

The **System Settings** page is shown below.



Email Forwarding Rules

Below is a list of rules for Email Forwarding. Click the:

- **Modify** button to modify the rule
- **X** button to delete the rule
- **Activate / Deactivate** button to toggle the state of the specified rule
- **Activate All / Deactivate All** button to toggle the state of the ALL rules
- **Delete All** button to delete ALL rules

				Name	State
🟩	X	Deactivate	Modify	**My Rule**	**Activated**

Activate All | Deactivate All | Delete All

Click **here** to create a new Email Forwarding Rule.

FIGURE: **System Settings** page

Different **System Settings** sub-pages display, depending on which tab you click. For example, if you click the **Email Forwarding Rules** tab, the **Email Forwarding Rules** sub-page displays.

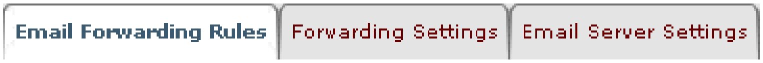


FIGURE: **System Settings** page tabs

These **System Settings** sub-pages allow you to configure Email Forwarding Rules, forwarding settings, and email server settings. For more information, see *What are system settings?*.

For specific information on configuring:

- **Email Forwarding Rules**, see *Email Forwarding Rules*
- **Forwarding Setting**, see *Forwarding Settings*
- **Email Server Settings**, see *Email Server Settings*.

Email Forwarding Rules

Email Forwarding Rules allow you to *email* Alerts, instead of (or in addition to) the SNMP trap, file, or Syslog methods specified during the configuration/deployment of an instance for a registered Sensor (for more information, see *Configuring a Sensor and deploying the configuration information*).

Each **Email Forwarding Rule** specifies user-defined criteria for forwarding Alerts via email. When the Email Forwarding Rule is activated, and these criteria are met, Audit and Threat Management emails the Alerts to your list of recipients (also specified in your Email Forwarding Rule).

Note: DbProtect Audit and Threat Management does **not** allow you to email forward Alerts with a risk level of **Info**. You must elevate the risk level of a rule in a Policy to **Low**, **Medium**, or **High** if you want to email forward Alerts. For more information, see *Editing a Policy* and *What do the risk levels mean?*

Important: Email Forwarding Rules work **only** works after you properly configure your email server; for more information, see *Email Server Settings*.

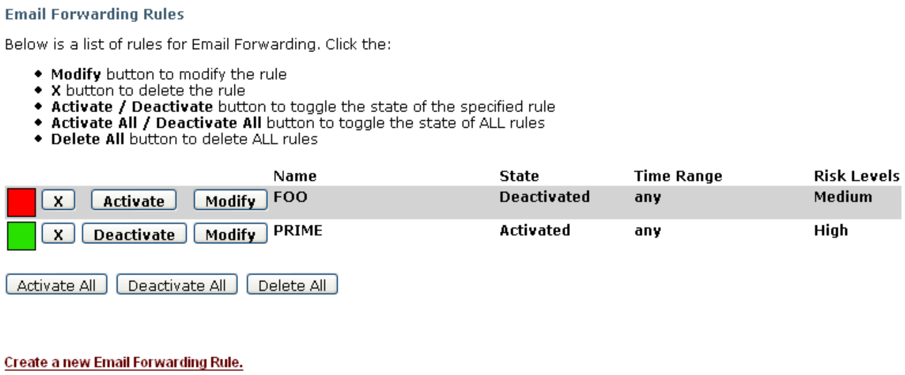
This topic assumes you understand Simple Mail Transfer Protocol (SMTP) server technology.

This topic consists of the following sub-topics:

- *Understanding the Email Forwarding Rules sub-page*
- *Creating a new Email Forwarding Rule*
- *Modifying an Email Forwarding Rule*
- *Deleting an Email Forwarding Rule*
- *Activating/deactivating an Email Forwarding Rule*.

UNDERSTANDING THE EMAIL FORWARDING RULES SUB-PAGE

The **Email Forwarding Rules** sub-page is shown below.



Email Forwarding Rules

Below is a list of rules for Email Forwarding. Click the:

- **Modify** button to modify the rule
- **X** button to delete the rule
- **Activate / Deactivate** button to toggle the state of the specified rule
- **Activate All / Deactivate All** button to toggle the state of ALL rules
- **Delete All** button to delete ALL rules

		Name	State	Time Range	Risk Levels
🟥	X Activate Modify	FOO	Deactivated	any	Medium
🟩	X Deactivate Modify	PRIME	Activated	any	High

Create a new Email Forwarding Rule.

FIGURE: **Email Forwarding Rules** sub-page

The **Email Forwarding Rules** sub-page displays your existing Email Forwarding Rules. Specifically, for each Rule, this sub-page displays the following attributes:

- the **Name** of the Email Forwarding Rule
- the **State** of the Email Forwarding Rule (i.e., **Activated** or **Deactivated**)

Hint: The color-coded icon to the left of each Email Forwarding Rules also indicate the state of the rule. Red means the Rule is **Inactive**. Green means the Rule is **Active**.

- the **Time Range** of the Email Forwarding Rule (you can configure an Email Forwarding Rule to take effect only during a specified time period, e.g., 10 P.M. to 6 A.M.)
- which **Risk Levels** the Email Forwarding Rule is configured to send emails about (i.e., High and/or Medium and/or Low).

Note: DbProtect Audit and Threat Management does **not** allow you to email forward Alerts with a risk level of **Info**. You must elevate the risk level of a rule in a Policy to **Low**, **Medium**, or **High** if you want to email forward Alerts. For more information, see *Editing a Policy* and *What do the risk levels mean?*

The **Email Forwarding Rules** sub-page allows you to:

- **create** a new Email Forwarding Rule; for more information, see *Creating a new Email Forwarding Rule*
- **modify** Email Forwarding Rules; for more information, see *Modifying an Email Forwarding Rule*
- **delete** Email Forwarding Rules; for more information, see *Deleting an Email Forwarding Rule*

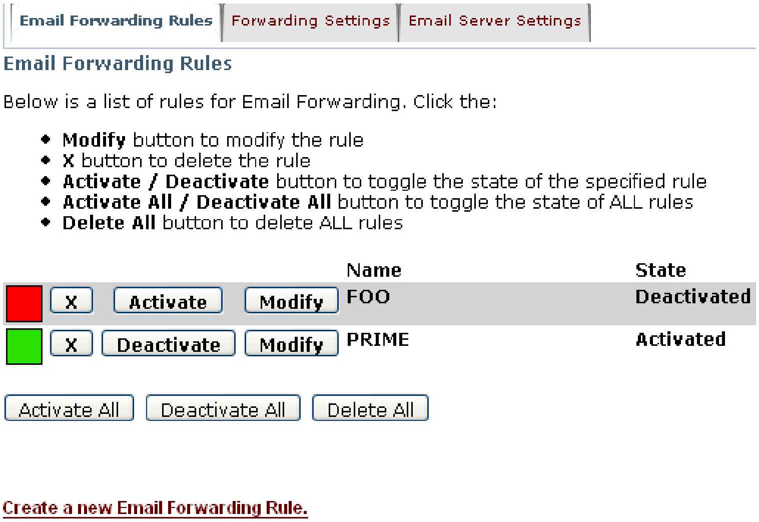
- **activate/deactivate** Email Forwarding Rules; for more information, see *Activating/deactivating an Email Forwarding Rule*.

CREATING A NEW EMAIL FORWARDING RULE

To create an Email Forwarding Rule:

1. Do the following to display the **Email Forwarding Rules** sub-page:

- Click the **System Settings** tab from any DbProtect Audit and Threat Management page to display the **System Settings** page (for more information, see *Understanding the System Settings page*).
- Click the **Email Forwarding Rules** tab.



Email Forwarding Rules

Below is a list of rules for Email Forwarding. Click the:

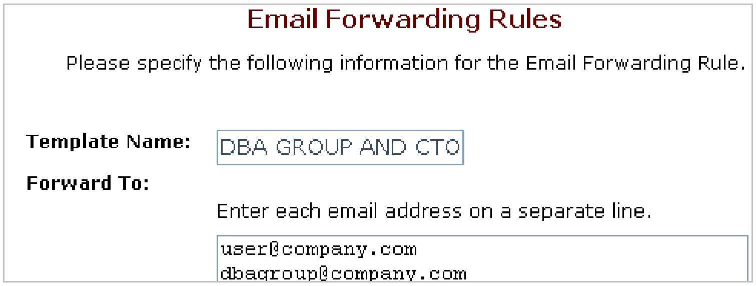
- **Modify** button to modify the rule
- **X** button to delete the rule
- **Activate / Deactivate** button to toggle the state of the specified rule
- **Activate All / Deactivate All** button to toggle the state of ALL rules
- **Delete All** button to delete ALL rules

				Name	State
🟥	X	Activate	Modify	FOO	Deactivated
🟩	X	Deactivate	Modify	PRIME	Activated

Create a new Email Forwarding Rule.

FIGURE: **Email Forwarding Rules** sub-page

2. Click the **Create a new Email Forwarding Rule** link at the bottom of the page to display the first **Email Forwarding Rules** page.



Email Forwarding Rules

Please specify the following information for the Email Forwarding Rule.

Template Name: DBA GROUP AND CTO

Forward To:

Enter each email address on a separate line.

```
user@company.com
dbagroup@company.com
```

FIGURE: First **Email Forwarding Rules** page

Note: If you have not created any Email Forwarding Rules, this page displays by default.

The first **Email Forwarding Rules** page allows you to specify an Email Forwarding Rule template name, and a list of email recipients.

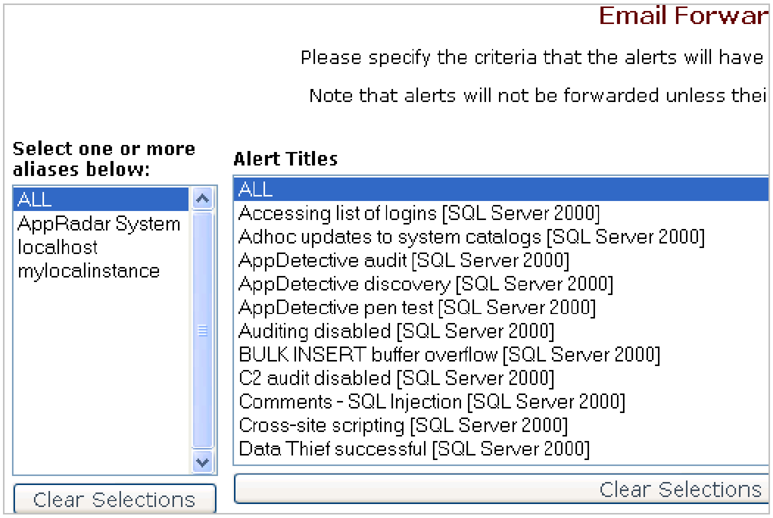
Enter the:

- name of your Email Forwarding Rule in the **Template Name:** field, e.g., `HIGH RISK ALERTS FOR DBA GROUP AND CTO`
- email addresses of your email recipients in the **Forward To:** field, e.g., `user@company.com`

Caution! You **must** enter each email address on a separate line. Do **not** separate the email addresses with commas.

3. Click the **Next** button.

The next **Email Forwarding Rules** page displays.



Email Forwar

Please specify the criteria that the alerts will have

Note that alerts will not be forwarded unless thei

Select one or more aliases below:

- ALL
- AppRadar System
- localhost
- mylocalinstance

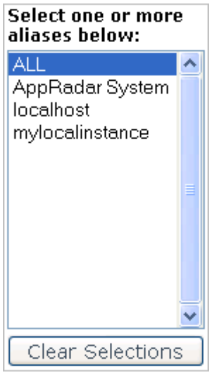
Alert Titles

- ALL
- Accessing list of logins [SQL Server 2000]
- Adhoc updates to system catalogs [SQL Server 2000]
- AppDetective audit [SQL Server 2000]
- AppDetective discovery [SQL Server 2000]
- AppDetective pen test [SQL Server 2000]
- Auditing disabled [SQL Server 2000]
- BULK INSERT buffer overflow [SQL Server 2000]
- C2 audit disabled [SQL Server 2000]
- Comments - SQL Injection [SQL Server 2000]
- Cross-site scripting [SQL Server 2000]
- Data Thief successful [SQL Server 2000]

FIGURE: Second **Email Forwarding Rules** page

4. In the **Select one or more aliases below:** portion of the second **Email Forwarding Rules** page, select the alias of the database instance where you registered a Sensor.

Only Alerts on this database instance will trigger your Email Forwarding Rule. You can select the default (**ALL**) if you want Alerts on all database instance aliases to trigger your Email Forwarding Rule.



Select one or more aliases below:

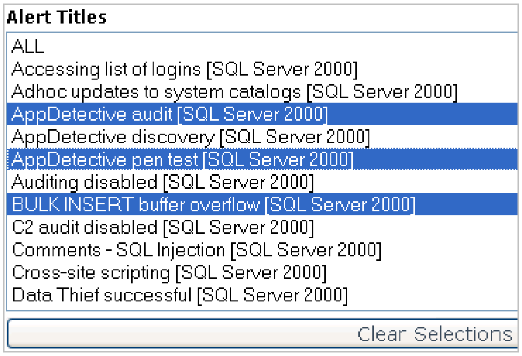
ALL
AppRadar System
localhost
mylocalinstance

FIGURE: **Select one or more aliases below:** portion

Hint: Press <SHIFT> to highlight multiple aliases. Press <CTRL> to highlight multiple non-consecutive aliases. Click the **Clear Selections** button to clear your alias selections.

For more information on configuring and deploying Sensors, see *Configuring a Sensor and deploying the configuration information*.

5. In the **Alert Titles** portion of the second **Email Forwarding Rules** page, select which Alerts will trigger your Email Forwarding Rule. Use the scroll-down box to highlight one or more Alerts. You can select the default (**ALL**) if you want all Alerts to trigger your Email Forwarding Rule.



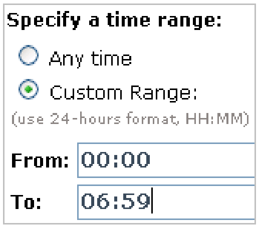
Alert Titles

ALL
Accessing list of logins [SQL Server 2000]
Adhoc updates to system catalogs [SQL Server 2000]
AppDetective audit [SQL Server 2000]
AppDetective discovery [SQL Server 2000]
AppDetective pen test [SQL Server 2000]
Auditing disabled [SQL Server 2000]
BULK INSERT buffer overflow [SQL Server 2000]
C2 audit disabled [SQL Server 2000]
Comments - SQL Injection [SQL Server 2000]
Cross-site scripting [SQL Server 2000]
Data Thief successful [SQL Server 2000]

FIGURE: **Alert Titles** portion

Hint: Press <SHIFT> to highlight multiple consecutive Alerts. Press <CTRL> to highlight multiple non-consecutive Alerts. Click the **Clear Selections** button to clear your Alert selections.

6. In the **Specify a time range:** portion of the second **Email Forwarding Rules** page, you can specify a **time range** for your Email Forwarding Rule. (For example, perhaps you only want Alerts that occur between the hours of midnight to 6:59 A.M. to trigger your Email Forwarding Rule.)



Specify a time range:

○ Any time

● Custom Range:

(use 24-hours format, HH:MM)

From: 00:00

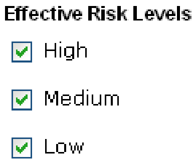
To: 06:59

FIGURE: **Specify a time range:** portion

If you select:

- **Any time**, then any Alerts specified in Step 6 will trigger your Email Forwarding Rule -- 24 hours a day
- **Custom range**, then enter a military time range in the **From:** and **To:** fields, using the format `hh:mm`. For example, if you only want Alerts that occur between the hours of midnight to 6:59 A.M. to trigger your Email Forwarding Rule, then enter `00:00` and `06:59` in the **From:** and **To:** fields, respectively.

7. In the **Effective Risk Levels** portion of the second **Email Forwarding Rules** page, you can specify which **Risk Levels** are associated with your Email Forwarding Rule.



Effective Risk Levels

☑ High

☑ Medium

☑ Low

FIGURE: **Effective Risk Levels** portion

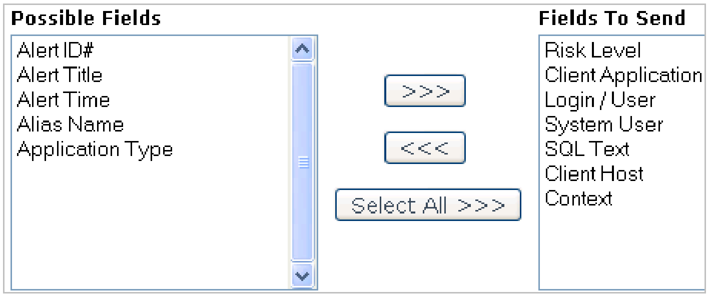
You can check one (minimum) or more of the following:

- **High**
- **Medium**
- **Low**.

Note: DbProtect Audit and Threat Management does **not** allow you to email forward Alerts with a risk level of **Info**. You must elevate the risk level of a rule in a Policy to **Low**, **Medium**, or **High** if you want to email forward Alerts; for more information, see *Editing a Policy* and *What do the risk levels mean?*

8. Click the **Next** button.

The third **Email Forwarding Rules** page displays.



Possible Fields

- Alert ID#
- Alert Title
- Alert Time
- Alias Name
- Application Type

Fields To Send

- Risk Level
- Client Application
- Login / User
- System User
- SQL Text
- Client Host
- Context

FIGURE: Third **Email Forwarding Rules** page

Two scroll-down boxes display: **Possible Fields** and **Fields To Send**. These scroll-down boxes allow you to select which Alert fields and values should display in each forwarded email Alert.

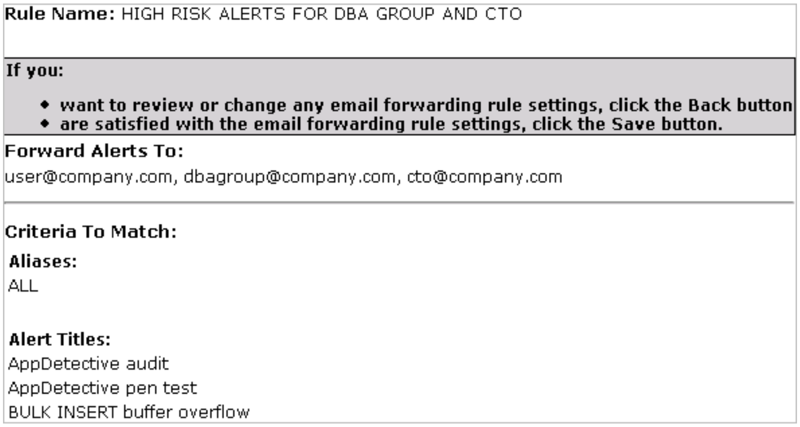
Note: Application Security, Inc. recommends that you include, at a minimum, the **Alert Title** and **Risk Level** fields in your forwarded email Alerts.

You can move fields from the **Possible Fields** scroll-down box to the **Fields To Send** scroll-down box, or vice versa, by highlighting the field name and clicking either the **<<<** or **>>>** button. Clicking the **>>>** button *adds* the highlighted Alert fields and values *to* the list of Alert fields and values to be displayed in an email Alert. Clicking the **<<<** button *removes* the highlighted Alert fields and values *from* the list of Alert fields and values to be displayed in an email Alert.

Note: Press <SHIFT> to highlight multiple consecutive fields. Press <CTRL> to highlight multiple non-consecutive fields. Click the Select All >>> button to move all fields in the Possible Fields scroll-down box to the Fields To Send scroll-down box.

9. Click the **Next** button.

The **Email Forwarding Rules** summary page displays.



Rule Name: HIGH RISK ALERTS FOR DBA GROUP AND CTO

If you:

- **want to review or change any email forwarding rule settings, click the Back button**
- **are satisfied with the email forwarding rule settings, click the Save button.**

Forward Alerts To:
user@company.com, dbagroup@company.com, cto@company.com

Criteria To Match:

Aliases:
ALL

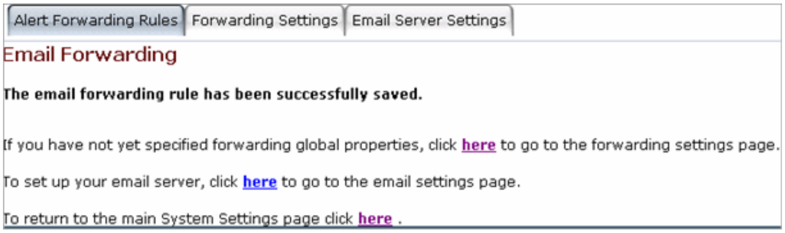
Alert Titles:
AppDetective audit
AppDetective pen test
BULK INSERT buffer overflow

FIGURE: **Email Forwarding Rules** summary page

If you:

- want to review or change any Email Forwarding Rule settings, you can click the **Back** button or any link that displays on the page
- are satisfied with your Email Forwarding Rule settings, click the **Save** button.

Your Email Forwarding Rule is saved. A confirmation page displays.



Email Forwarding

The email forwarding rule has been successfully saved.

If you have not yet specified forwarding global properties, click here to go to the forwarding settings page.

To set up your email server, click here to go to the email settings page.

To return to the main System Settings page click here .

FIGURE: **Email Forwarding Rules** confirmation page

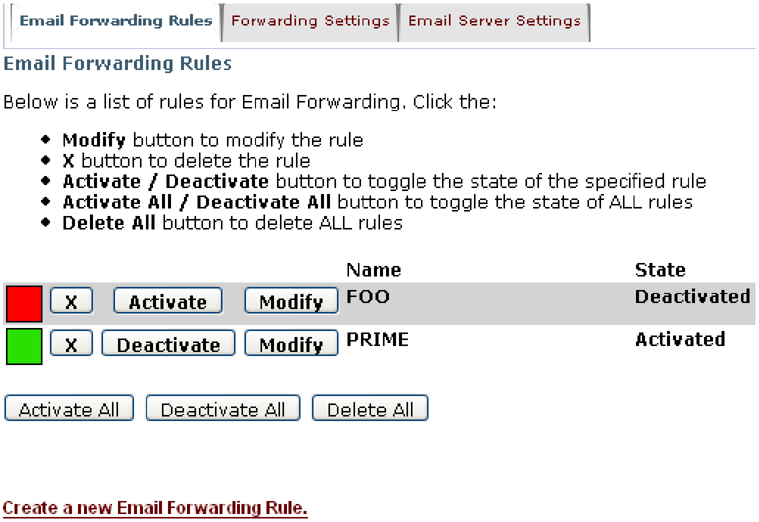
10. From the confirmation page, you can click the:

- first **here** link to display the **Global Properties** sub-page, which allows you to specify your **Forwarding Settings**; for more information, see *Forwarding Settings*
- second **here** link to display the **Email Server Settings** sub-page, which allows you to configure your email server to accommodate the forwarding of Alerts and Reports via email; for more information, see *Email Server Settings*
- third **here** link to display the first **Email Forwarding Rules** page.

MODIFYING AN EMAIL FORWARDING RULE

To modify an Email Forwarding Rule:

1. Do the following to display the **Email Forwarding Rules** sub-page:
   - Click the **System Settings** tab from any DbProtect Audit and Threat Management page to display the **System Settings** page (for more information, see *Understanding the System Settings page*).
   - Click the **Email Forwarding Rules** tab.



Email Forwarding Rules

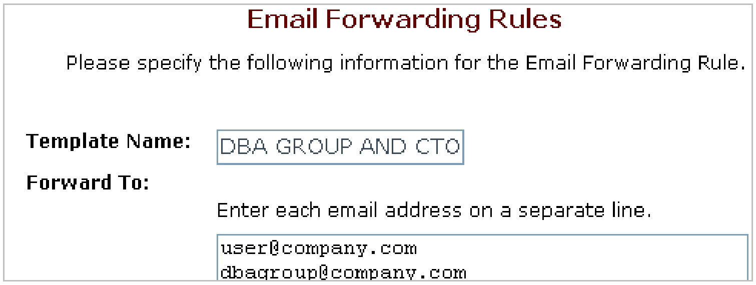
Below is a list of rules for Email Forwarding. Click the:

- **Modify** button to modify the rule
- **X** button to delete the rule
- **Activate / Deactivate** button to toggle the state of the specified rule
- **Activate All / Deactivate All** button to toggle the state of ALL rules
- **Delete All** button to delete ALL rules

				Name	State
🟥	X	Activate	Modify	FOO	Deactivated
🟩	X	Deactivate	Modify	PRIME	Activated

FIGURE: **Email Forwarding Rules** sub-page

2. Click the **Modify** button next to an existing Rule to display the first **Email Forwarding Rules** page.



Email Forwarding Rules

Please specify the following information for the Email Forwarding Rule.

Template Name: DBA GROUP AND CTO

Forward To:

Enter each email address on a separate line.

```
user@company.com
dbagroup@company.com
```

FIGURE: First **Email Forwarding Rules** page

The first **Email Forwarding Rules** page allows you to modify an Email Forwarding Rule template name, and a list of email recipients.

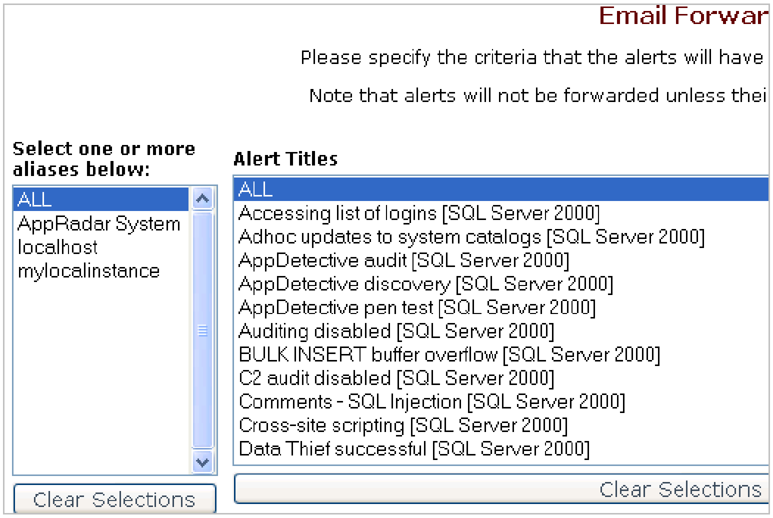
Modify the:

- name of your Email Forwarding Rule in the **Template Name:** field, e.g., `HIGH RISK ALERTS FOR DBA GROUP AND CTO`
- email addresses of your email recipients in the **Forward To:** field, e.g., `user@company.com`.

Caution! You **must** enter each email address on a separate line. Do **not** separate the email addresses with commas.

3. Click the **Next** button.

The second **Email Forwarding Rules** page displays.



Email Forwar

Please specify the criteria that the alerts will have

Note that alerts will not be forwarded unless thei

Select one or more aliases below:

- ALL
- AppRadar System
- localhost
- mylocalinstance

Alert Titles

- ALL
- Accessing list of logins [SQL Server 2000]
- Adhoc updates to system catalogs [SQL Server 2000]
- AppDetective audit [SQL Server 2000]
- AppDetective discovery [SQL Server 2000]
- AppDetective pen test [SQL Server 2000]
- Auditing disabled [SQL Server 2000]
- BULK INSERT buffer overflow [SQL Server 2000]
- C2 audit disabled [SQL Server 2000]
- Comments - SQL Injection [SQL Server 2000]
- Cross-site scripting [SQL Server 2000]
- Data Thief successful [SQL Server 2000]

FIGURE: Second **Email Forwarding Rules** page

4. In the **Select one or more aliases below:** portion of the second **Email Forwarding Rules** page, modify the alias of the database instance where you registered a Sensor.

Only Alerts on this database instance will trigger your Email Forwarding Rule. You can select the default (**ALL**) if you want Alerts on all database instance aliases to trigger your Email Forwarding Rule.

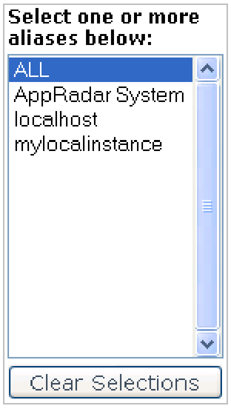
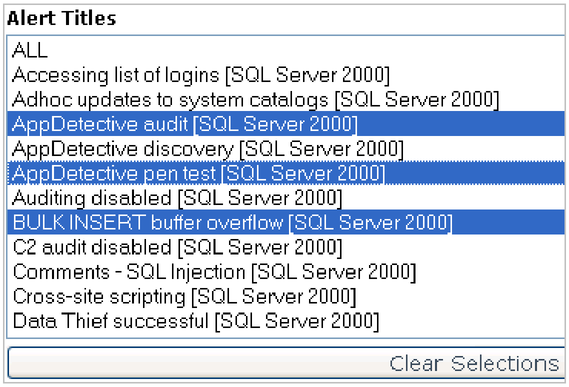


FIGURE: **Select one or more aliases below:** portion

Hint: Press <SHIFT> to highlight multiple aliases. Press <CTRL> to highlight multiple non-consecutive aliases. Click the **Clear Selections** button to clear your alias selections.

For more information on configuring and deploying Sensors, see *Configuring a Sensor and deploying the configuration information*.

5. In the **Alert Titles** portion of the second **Email Forwarding Rules** page, modify which Alerts will trigger your Email Forwarding Rule. Use the scroll-down box to highlight one or more Alerts. You can select the default (**ALL**) if you want all Alerts to trigger your Email Forwarding Rule.



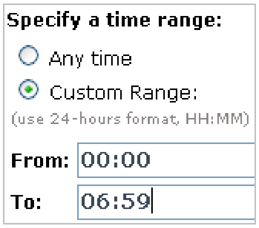
Alert Titles

ALL
Accessing list of logins [SQL Server 2000]
Adhoc updates to system catalogs [SQL Server 2000]
AppDetective audit [SQL Server 2000]
AppDetective discovery [SQL Server 2000]
AppDetective pen test [SQL Server 2000]
Auditing disabled [SQL Server 2000]
BULK INSERT buffer overflow [SQL Server 2000]
C2 audit disabled [SQL Server 2000]
Comments - SQL Injection [SQL Server 2000]
Cross-site scripting [SQL Server 2000]
Data Thief successful [SQL Server 2000]

FIGURE: **Alert Titles** portion

Hint: Press <SHIFT> to highlight multiple consecutive Alerts. Press <CTRL> to highlight multiple non-consecutive Alerts. Click the **Clear Selections** button to clear your Alert selections.

6. In the **Specify a time range:** portion of the second **Email Forwarding Rules** page, you can modify a **time range** for your Email Forwarding Rule. (For example, perhaps you only want Alerts that occur between the hours of midnight to 6:59 A.M. to trigger your Email Forwarding Rule.)



Specify a time range:

○ Any time
● Custom Range:
(use 24-hours format, HH:MM)

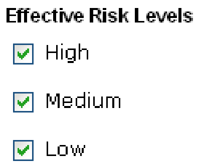
From: 00:00
To: 06:59

FIGURE: **Specify a time range:** portion

If you select:

- **Any time**, then any Alerts specified in Step 6 will trigger your Email Forwarding Rule -- 24 hours a day
- **Custom range**, then enter a military time range in the **From:** and **To:** fields, using the format `hh:mm`. For example, if you only want Alerts that occur between the hours of midnight to 6:59 A.M. to trigger your Email Forwarding Rule, then enter `00:00` and `06:59` in the **From:** and **To:** fields, respectively.

7. In the **Effective Risk Levels** portion of the second **Email Forwarding Rules** page, you can modify which **Risk Levels** are associated with your Email Forwarding Rule.



Effective Risk Levels

☑ High

☑ Medium

☑ Low

FIGURE: **Effective Risk Levels** portion

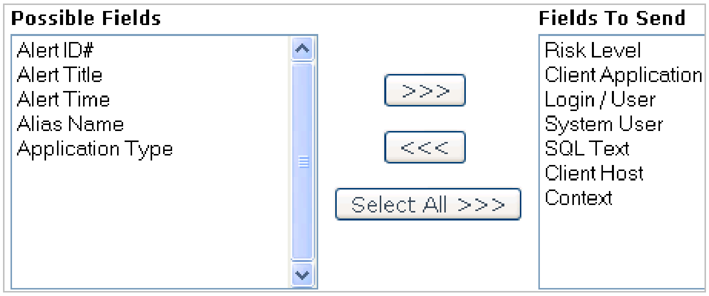
You can check one (minimum) or more of the following:

- **High**
- **Medium**
- **Low**.

Note: DbProtect Audit and Threat Management does **not** allow you to email forward Alerts with a risk level of **Info**. You must elevate the risk level of a rule in a Policy to **Low**, **Medium**, or **High** if you want to email forward Alerts; for more information, see *Editing a Policy* and *What do the risk levels mean?*

8. Click the **Next** button.

The third **Email Forwarding Rules** page displays.



Possible Fields

Alert ID#
Alert Title
Alert Time
Alias Name
Application Type

Fields To Send

Risk Level
Client Application
Login / User
System User
SQL Text
Client Host
Context

FIGURE: Third **Email Forwarding Rules** page

Two scroll-down boxes display: **Possible Fields** and **Fields To Send**. These scroll-down boxes allow you to modify which Alert fields and values should display in each forwarded email Alert.

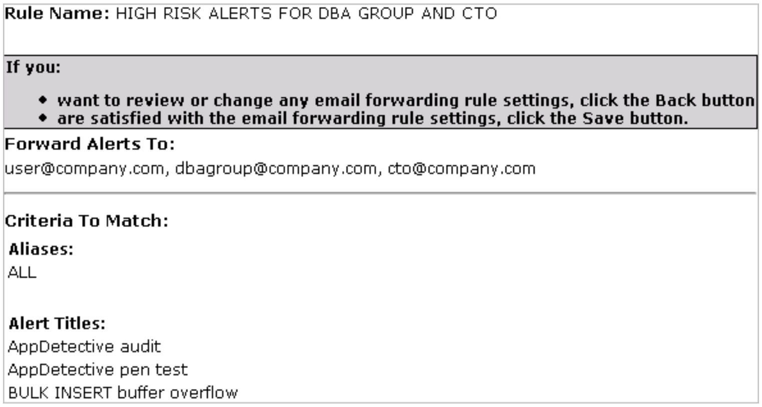
Note: Application Security, Inc. recommends that you include, at a minimum, the **Alert Title** and **Risk Level** fields in your forwarded email Alerts.

You can move fields from the **Possible Fields** scroll-down box to the **Fields To Send** scroll-down box, or vice versa, by highlighting the field name and clicking either the <<< or >>> button. Clicking the >>> button *adds* the highlighted Alert fields and values *to* the list of Alert fields and values to be displayed in an email Alert. Clicking the <<< button *removes* the highlighted Alert fields and values *from* the list of Alert fields and values to be displayed in an email Alert.

Note: Press <SHIFT> to highlight multiple consecutive fields. Press <CTRL> to highlight multiple non-consecutive fields. Click the Select All >>> button to move all fields in the Possible Fields scroll-down box to the Fields To Send scroll-down box.

9. Click the **Next** button.

The **Email Forwarding Rules** summary page displays.



Rule Name: HIGH RISK ALERTS FOR DBA GROUP AND CTO

If you:

- **want to review or change any email forwarding rule settings, click the Back button**
- **are satisfied with the email forwarding rule settings, click the Save button.**

Forward Alerts To:
user@company.com, dbagroup@company.com, cto@company.com

Criteria To Match:

Aliases:
ALL

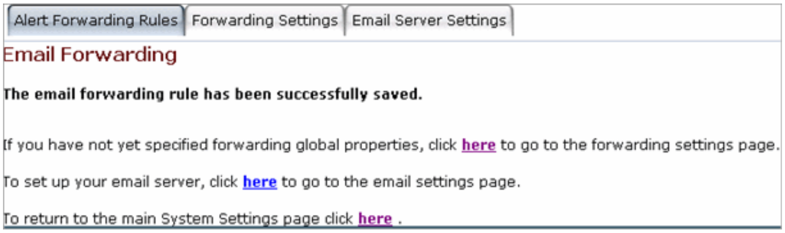
Alert Titles:
AppDetective audit
AppDetective pen test
BULK INSERT buffer overflow

FIGURE: **Email Forwarding Rules** summary page

If you:

- want to review or change any Email Forwarding Rule settings, you can click the **Back** button or any link that displays on the page
- are satisfied with your Email Forwarding Rule settings, click the **Save** button.

Your Email Forwarding Rule is saved. A confirmation page displays.



Email Forwarding

The email forwarding rule has been successfully saved.

If you have not yet specified forwarding global properties, click here to go to the forwarding settings page.

To set up your email server, click here to go to the email settings page.

To return to the main System Settings page click here .

FIGURE: **Email Forwarding Rules** confirmation page

10. From the confirmation page, you can click the:

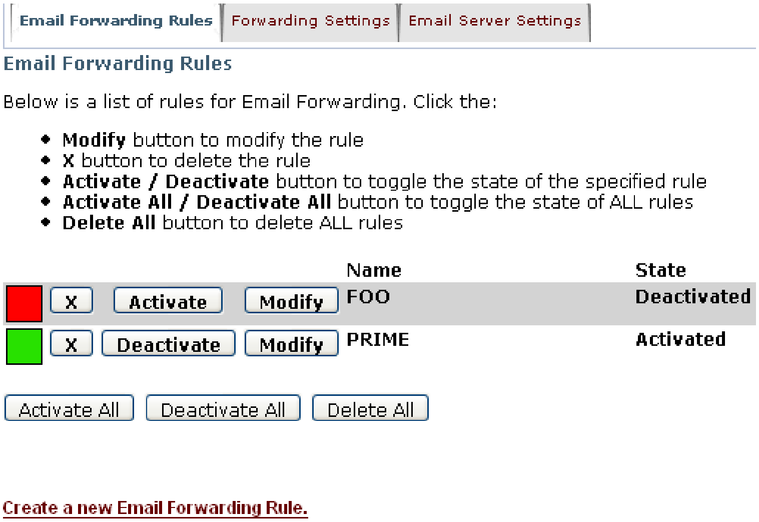
- first **here** link to display the **Global Properties** sub-page, which allows you to specify your **Forwarding Settings**; for more information, see *Forwarding Settings*
- second **here** link to display the **Email Server Settings** sub-page, which allows you to configure your email server to accommodate the forwarding of Alerts and Reports via email; for more information, see *Email Server Settings*
- third **here** link to display the first **Email Forwarding Rules** page.

DELETING AN EMAIL FORWARDING RULE

To **delete** an Email Forwarding Rule:

1. Do the following to display the **Email Forwarding Rules** sub-page:

- Click the **System Settings** tab from any DbProtect Audit and Threat Management page to display the **System Settings** page (for more information, see *Understanding the System Settings page*).
- Click the **Email Forwarding Rules** tab.



Email Forwarding Rules

Below is a list of rules for Email Forwarding. Click the:

- **Modify** button to modify the rule
- **X** button to delete the rule
- **Activate / Deactivate** button to toggle the state of the specified rule
- **Activate All / Deactivate All** button to toggle the state of ALL rules
- **Delete All** button to delete ALL rules

				Name	State
🟥	X	Activate	Modify	FOO	Deactivated
🟩	X	Deactivate	Modify	PRIME	Activated

Create a new Email Forwarding Rule.

FIGURE: **Email Forwarding Rules** sub-page

This sub-page lists your existing Email Forwarding Rules (whether active or inactive).

2. If you want to:

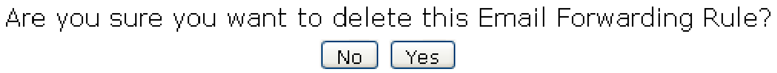
- delete an **individual** Email Forwarding Rule, go to Step 3
- delete **all** Email Forwarding Rules, go to Step 4.

3. Delete an individual Email Forwarding Rule.

From the **Email Forwarding Rules** sub-page, do the following:

- Click the **X** button next to the Email Forwarding Rule you want to delete.

  DbProtect Audit and Threat Management prompts you to confirm that you want to delete the Email Forwarding Rule.



Are you sure you want to delete this Email Forwarding Rule?

FIGURE: Confirm delete page (individual Email Forwarding Rule)

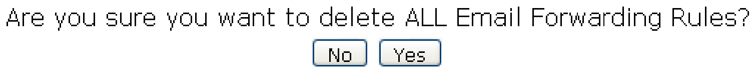
- Click the **Yes** button to delete the Rule.

4. Delete *all* Email Forwarding Rules.

From the **Email Forwarding Rules** sub-page, do the following:

- Click the **Delete All** button to delete **all** Email Forwarding Rules.

  DbProtect Audit and Threat Management prompts you to confirm that you want to delete the Email Forwarding Rule.



Are you sure you want to delete ALL Email Forwarding Rules?

FIGURE: Confirm delete (**all** Email Forwarding Rules)

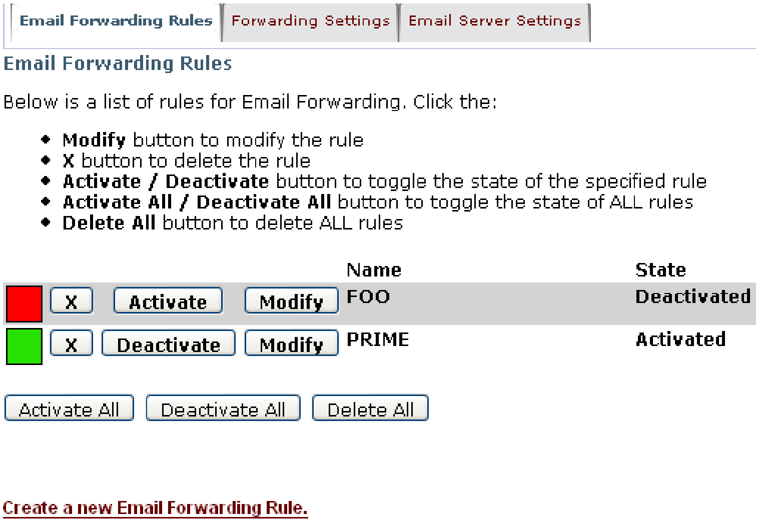
- Click the **Yes** button to delete all Rules.

ACTIVATING/DEACTIVATING AN EMAIL FORWARDING RULE

To **activate/deactivate** an Email Forwarding Rule:

1. Do the following to display the **Email Forwarding Rules** sub-page:

- Click the **System Settings** tab from any DbProtect Audit and Threat Management page to display the **System Settings** page (for more information, see *Understanding the System Settings page*).
- Click the **Email Forwarding Rules** tab.



Email Forwarding Rules

Below is a list of rules for Email Forwarding. Click the:

- **Modify** button to modify the rule
- **X** button to delete the rule
- **Activate / Deactivate** button to toggle the state of the specified rule
- **Activate All / Deactivate All** button to toggle the state of ALL rules
- **Delete All** button to delete ALL rules

				Name	State
🟥	X	Activate	Modify	FOO	Deactivated
🟩	X	Deactivate	Modify	PRIME	Activated

Create a new Email Forwarding Rule.

FIGURE: **Email Forwarding Rules** sub-page

This sub-page lists your existing Email Forwarding Rules (whether active or inactive).

2. If you want to:

- activate/deactivate an **individual** Email Forwarding Rule, go to Step 3
- activate/deactivate **all** Email Forwarding Rules, go to Step 4.

3. Activate/deactivate an individual Email Forwarding Rule.

From the **Email Forwarding Rules** sub-page, do the following:

- Click the **Activate** button to activate a corresponding (deactivated) Email Forwarding Rule.
- Click the **Deactivate** button to deactivate a corresponding (activated) Email Forwarding Rule.

4. Activate/deactivate *all* Email Forwarding Rules.

From the **Email Forwarding Rules** sub-page, do the following:

- Click the **Activate All** button to activate all (deactivated) Email Forwarding Rules.
- Click the **Deactivate All** button to deactivate all (activated) Email Forwarding Rules.

Forwarding Settings

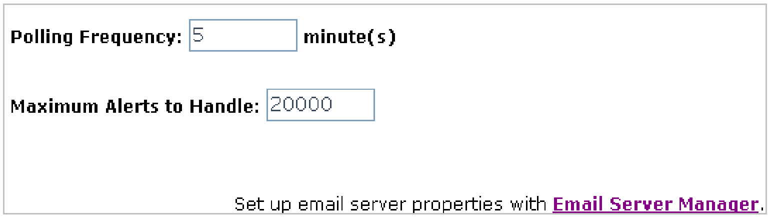
Forwarding Settings allow you to specify the:

- **polling frequency**, i.e., how often (in minutes) DbProtect Audit and Threat Management should check for new Alerts and email them to recipients identified in your *Email Forwarding Rules*).
- **maximum number of Alerts to handle**, i.e., the maximum number of Alerts you want DbProtect Audit and Threat Management to send in each email to your recipients (specified in your *Email Forwarding Rules*).

To configure your Forwarding Settings:

1. Do the following to display the **Global Properties** sub-page:

- Click the **System Settings** tab from any DbProtect Audit and Threat Management page to display the **System Settings** page (for more information, see *Understanding the System Settings page*).
- Click the **Forwarding Settings** tab.



Polling Frequency: 5 **minute(s)**

Maximum Alerts to Handle: 20000

Set up email server properties with **Email Server Manager**.

FIGURE: **Global Properties** sub-page

2. The **Global Properties** sub-page consists of the following fields:

- **Polling Frequency:** Enter the **polling frequency**, in minutes, for DbProtect Audit and Threat Management to check for new Alerts and email them to the recipients identified in your *Email Forwarding Rules*. The default polling frequency is `5` minutes.
- **Maximum Alerts to Handle:** Enter the **maximum number of Alerts** you want DbProtect Audit and Threat Management to send in each email to the recipients identified in your *Email Forwarding Rules*. The default value is `100` Alerts.

Email Server Settings

Email Server Settings allow you to configure your email server to accommodate the forwarding of Alerts and Reports via email.

The **Email Server Settings** sub-page allows you to:

- specify your **Outbound SMTP Server:** name and **Port:** number
- indicate whether you want to **Use Authentication** (for SMTP servers), and if so, which **login/password** pair to use; for more information, see *SMTP server authentication considerations*
- select whether to use a **Secure Connection:** (you can select **None** or **SSL**)
- enter the **From Address:** and **Reply To Address:** to display in your emailed Alerts
- specify the **Max Attachment Size:** (in megabytes) for attachments to your emailed Alerts
- send a **test email**.

This topic consists of the following sub-topics:

- *SMTP server authentication considerations*
- *Configuring your email server settings*.

SMTP SERVER AUTHENTICATION CONSIDERATIONS

Some **SMTP servers** require authentication in order to send email. Depending on what kind of SMTP server you are using, and how it is configured, this may or may not be the case. If your SMTP server requires authentication in order to send email, then you must enter a valid login/password pair, and check the **Use Authentication** checkbox in Step 2 of *Configuring your email server settings*, below. However, if you are not sure whether your SMTP server requires authentication, check with your mail administrator.

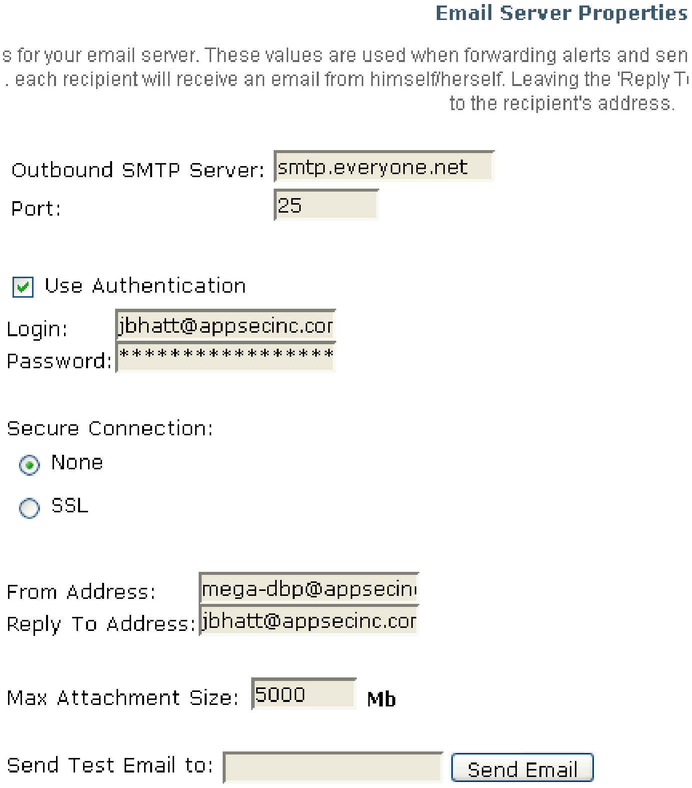
For more information on email authentication, see *http://en.wikipedia.org/wiki/Email_authentication*.

CONFIGURING YOUR EMAIL SERVER SETTINGS

To configure your Email Server Settings:

1. Do the following to display the **Email Server Properties** sub-page:

- Click the **System Settings** tab from any DbProtect Audit and Threat Management page to display the **System Settings** page (for more information, see *Understanding the System Settings page*).
- Click the **Email Server Settings** tab.



Email Server Properties

s for your email server. These values are used when forwarding alerts and sen
. each recipient will receive an email from himself/herself. Leaving the 'Reply T
to the recipient's address.

Outbound SMTP Server: smtp.everyone.net

Port: 25

☑ Use Authentication

Login: jbhatt@appsecinc.cor

Password: ****************

Secure Connection:

● None

○ SSL

From Address: mega-dbp@appsecin

Reply To Address: jbhatt@appsecinc.cor

Max Attachment Size: 5000 Mb

Send Test Email to:

FIGURE: **Email Server Settings** sub-page

2. In the:

- **Outbound SMTP Server:** field, enter the name of your outgoing SMTP server
- **Port** field, enter which port number (in the `1-65535` range) you want to use on your outgoing SMTP server.

3. Check the **Use Authentication** checkbox if your SMTP server requires authentication in order to send email.

Note: Some SMTP servers require authentication in order to send email. Depending on what kind of SMTP server you are using, and how it is configured, this may or may not be the case. If your SMTP server requires authentication in order to send email, then you must enter a valid login/ password pair, and check the Use Authentication checkbox. However, if you are not sure whether your SMTP server requires authentication, check with your mail administrator.

If you check the **Use Authentication** checkbox, you must **also** enter a valid:

- **Username:**
- **Password:**

4. In the **Secure Connection:** portion of the page, select:
   - **SSL** if you want to use Secure Sockets Layer (SSL) to encrypt your user name and credentials prior to transmission
   - **None** if you do not want to use SSL encryption.
5. Enter a:
   - "from" email address in the **From Address:** field (i.e., when DbProtect Audit and Threat Management sends an Alert email to the recipients identified in your *Email Forwarding Rules*, this is the "from" email address they will see)
   - "reply to" email address in the **Reply To Address:** field (i.e., when DbProtect Audit and Threat Management sends an Alert email to the recipients identified in your *Email Forwarding Rules*, this is the "reply to" email address they will see).
6. In the **Max Attachment Size:** field, specify a maximum attachment size in megabytes (`1-30`). The default value is `3` megabytes.

Note: When DbProtect Audit and Threat Management completes a Report, the generated email always includes link to the Report -- even if there is no attachment. In other words, even if the generated Report exceeds the maximum attachment size, your email recipients can still view the Report online.

7. Optionally, you can enter a valid email address in the **Send Test Email to:** field, and click the **Send Email** button, to send a test Alert email.
8. Review your Email Server Settings.
9. Click the **Save** button.

Compliance Packs

This section consists of the following chapters:

- *Understanding Compliance Packs*
- *Interpreting Your Generated Compliance Pack Dashboards, and Displaying/ Interpreting Your Generated Compliance Pack Reports*..

Understanding Compliance Packs

This chapter consists of the following topics:

- *What are Compliance Packs and Compliance Content Packs?*
- *Compliance Pack Prerequisite: DbProtect Analytics 1.3 or Greater*
- *Minimum Required Privileges for Compliance Pack Usage*
- *Available Compliance Packs*
- *Obtaining Your Compliance Content Packs*
- *Viewing Your Available Imported Compliance Content Packs*
- *Importing a Compliance Content Pack*
- *Understanding the Compliance Packs Page*
- *Generating Compliance Pack Dashboards and Reports*.

What are Compliance Packs and Compliance Content Packs?

Compliance packs are optional DbProtect add-ons that contain regulatory compliance-level views of your database environment designed to help you track, manage, and meet compliance requirements. **Compliance packs** work in conjunction with DbProtect Analytics (version 1.3 or higher), allowing you to review and analyze compliance progress with additional high-level Dashboards and report the results of testing of database security controls in the correct compliance language context (e.g., information assurance controls and identifiers).

Compliance packs simplify the mapping between established test controls and the automated methods and procedures within DbProtect, which helps to save a tremendous amount of analysis time. Moreover, content packs offer additional Policies, Dashboards, reports, export formats, and independent resource information where applicable.

In order to enable compliance packs within DbProtect, you must first obtain and import a **compliance content pack**, i.e., an Application Security, Inc.-provided `.zip` files that, when successfully imported into DbProtect, adds reports geared toward helping you achieve regulation-specific compliance (for example, DISA-STIG). Once you import a compliance content pack, a new **Compliance Packs** tab displays on the Console.

For more information on:

- obtaining compliance content packs, see *Obtaining Your Compliance Content Packs*
- importing compliance content packs, see *Importing a Compliance Content Pack*

- understanding the **Compliance Packs** page (created when you successfully import a compliance content pack), see *Understanding the Compliance Packs Page*
- running a compliance pack report, see *Generating Compliance Pack Dashboards and Reports*

For more information on how DbProtect can help your organization achieve regulatory compliance, please visit the Application Security, Inc. website at http://www.appsecinc.com/solutions/compliance/index.shtml. If you have any questions, don’t hesitate to contact an Application Security, Inc. *Customer Support* representative.

Compliance Pack Prerequisite: DbProtect Analytics 1.3 or Greater

In order to use compliance packs in DbProtect, you **must** have **DbProtect Analytics 1.3** or greater installed. For more information on DbProtect Analytics, see the *DbProtect Analytics Installation and User’s Guide*.

Minimum Required Privileges for Compliance Pack Usage

In order to work with compliance packs, your assigned User role **must** be one of the following:

- **DbProtect Admin**
- **DbProtect Super Admin**
- **Vulnerability Management Admin**
- **Audit and Threat Management Admin**.

For more information on User roles, and their inherent rights and privileges, see *DbProtect Organizations, Users, and User Roles*.

Available Compliance Packs

The current version of DbProtect supports the **DISA-STIG** compliance pack. Additional compliance packs -- for all supported regulations -- are in development and will be released soon.

For more information on:

- generating **DISA-STIG** compliance pack Dashboards and reports, see *Generating Compliance Pack Dashboards and Reports*
- interpreting generated **DISA-STIG** compliance pack Dashboards and reports, see *Interpreting Your Generated Compliance Pack Dashboards, and Displaying/Interpreting Your Generated Compliance Pack Reports*.

Obtaining Your Compliance Content Packs

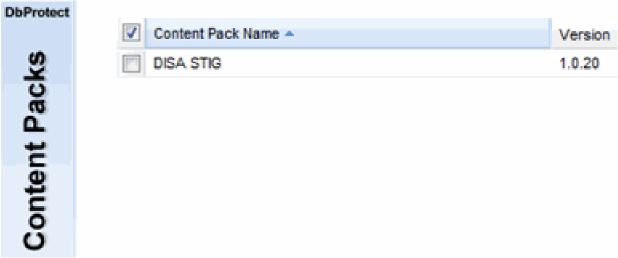
Once you purchase a regulation-specific content pack, an Application Security, Inc. representative will provide you with your compliance content pack in `.zip` file format (e.g., `DISA-STIG_1.0.20.cp.zip`). You must import this compliance content pack via the **Administration** page in order to start running compliance pack reports. For more information on:

- importing compliance content packs, see *Importing a Compliance Content Pack*
- running compliance pack reports, see *Generating Compliance Pack Dashboards and Reports*.

Viewing Your Available Imported Compliance Content Packs

To view your available imported compliance content packs:

1. Click the **Administration** tab to display the **Administration** page; for more information on the **Administration** page, see ***DbProtect Administration: Content/Compliance Packs, Data Sources, and System Information***.
2. Click the **Content Packs > View Content** link (in the navigation pane of the **Administration** page) to display content packs that you have already successfully imported (in the viewing pane).



☑	Content Pack Name ▲	Version
□	DISA STIG	1.0.20

FIGURE: Available imported content packs (in the **Administration** page viewing pane)

The navigation pane displays the name of the imported content pack (e.g., **DISA STIG**), as well as the version number (e.g., **1.0.20**).

Assuming you have already imported content packs, then you should see a **Compliance Packs** application tab on the DbProtect Console, which allows you to toggle to the **Compliance Packs** page and run compliance pack reports. For more information on:

- the **Compliance Packs** page, see *Understanding the Compliance Packs Page*
- running compliance pack reports, see *Generating Compliance Pack Dashboards and Reports*.

Importing a Compliance Content Pack

To import a compliance content pack:

1. Click the **Administration** tab to display the **Administration** page; for more information on the **Administration** page, see ***DbProtect Administration: Content/Compliance Packs, Data Sources, and System Information***.
2. Click the **Content Packs > Import Content** link (in the navigation pane of the **Administration** page) to import your Application Security, Inc.-provided, regulation-specific compliance content pack `.zip` file (e.g., `DISA-STIG_1.0.20.cp.zip`). You must import this compliance content pack via the **Administration** page in order to start running your compliance pack reports (explained in *Generating Compliance Pack Dashboards and Reports*).
3. Enter the full path location of your compliance content pack `.zip` file (stored on your local computer or network) in the **File:** field, or click the **Browse...** button to locate and upload the file.
4. Click the **Import** link.

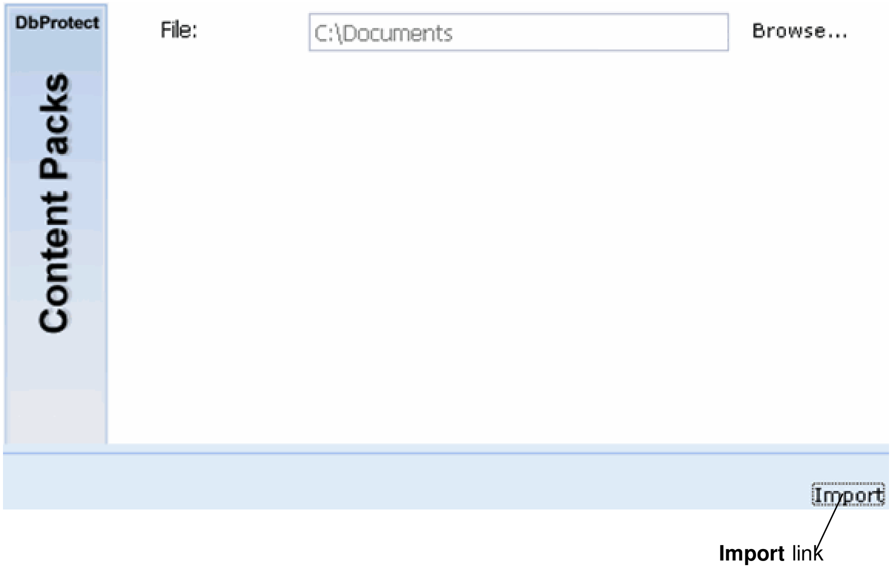


FIGURE: Compliance content pack import (in the **Administration** page viewing pane)

5. DbProtect imports your compliance content pack `.zip` file.

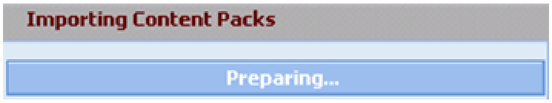


FIGURE: Compliance content pack import progress bar

DbProtect displays a success message upon completion.

Once you successfully import your compliance content pack into DbProtect, a new **Compliance Packs** application tab displays on the Console, allowing you to toggle to the newly-created **Compliance Packs** page and run compliance pack reports.

In addition, if you click the **Content Packs > View Content** link (in the navigation pane of the **Administration** page), you can display the content packs that you have already successfully imported (in the viewing pane).

For more information on:

- viewing the content packs that you have already imported, see *Viewing Your Available Imported Compliance Content Packs*
- the **Compliance Packs** page, see *Understanding the Compliance Packs Page*
- running compliance pack reports, see *Generating Compliance Pack Dashboards and Reports*.

Understanding the Compliance Packs Page

Once you have successfully imported a compliance content pack into DbProtect (as explained in *Importing a Compliance Content Pack*), the new **Compliance Packs** application tab displays on the Console, allowing you to toggle to the newly-created **Compliance Packs** page (shown below) and run compliance pack reports.

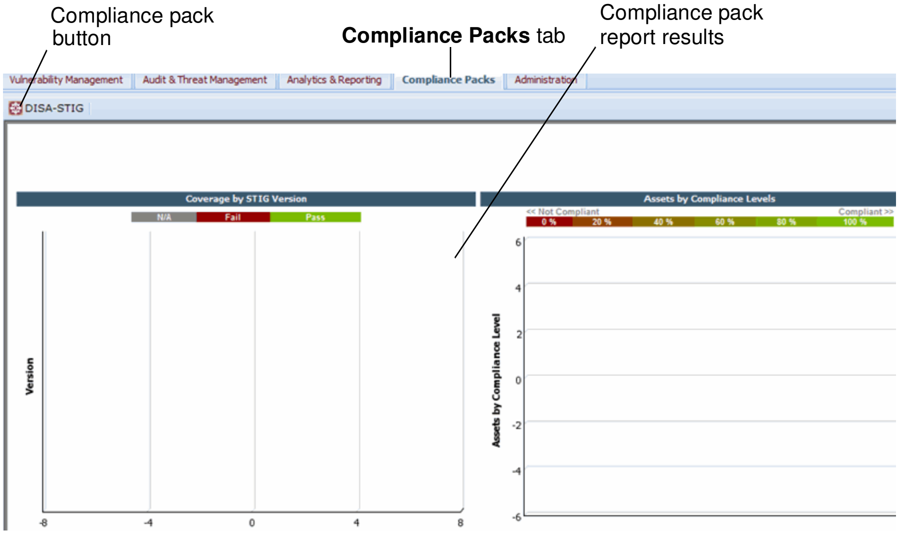


FIGURE: **Compliance Packs** page

The **Compliance Packs** page consists of:

- **Compliance pack buttons** -- one for each successfully-imported compliance content pack -- located in the upper-left portion of the page. Click this button to run a compliance pack report; for more information, see *Generating Compliance Pack Dashboards and Reports*.
- The **compliance pack report results** portion of the page, which displays your compliance pack report data.

Generating Compliance Pack Dashboards and Reports

There are **two** ways to generate compliance pack **reports** in DbProtect:

- from the **Compliance Packs** page (explained below)
- as a Report Job in DbProtect Vulnerability Management; for more information, see *Report Jobs*.

There is only one way, however, to generate high-level compliance pack **Dashboards** in DbProtect, however -- through from the **Compliance Packs** page (explained below).

To generate compliance pack Dashboards and reports from the **Compliance Packs** page:

1. Click the **Compliance Report** application tab to display the **Compliance Packs** page (shown below); for more information, see ***Understanding the Compliance Packs Page***.

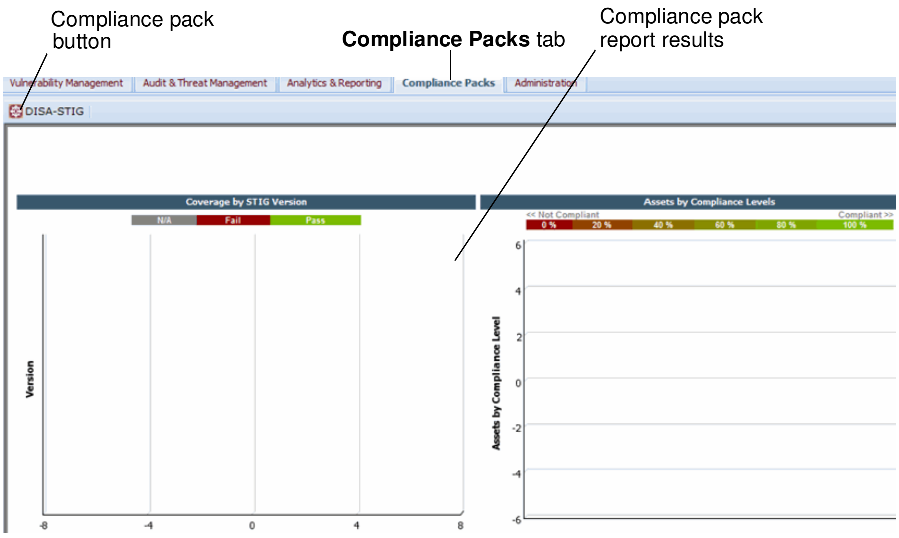


FIGURE: **Compliance Packs** page

2. Click a compliance pack button (one displays for each successfully-imported compliance content pack) located in the upper-left portion of the **Compliance Report** page.
3. DbProtect runs your compliance pack report, and displays the results in the compliance pack report data portion of the **Compliance Report** page.
4. For more information on:
   - the **Compliance Report** page, see *Understanding the Compliance Packs Page*
   - each available compliance pack report, see *Generating Compliance Pack Dashboards and Reports.*

Interpreting Your Generated Compliance Pack Dashboards, and Displaying/Interpreting Your Generated Compliance Pack Reports

There are **two** ways to generate compliance pack **reports** in DbProtect:

- from the **Compliance Packs** page; for more information, see *Generating Compliance Pack Dashboards and Reports*
- as a Report Job in DbProtect Vulnerability Management; for more information, see *Report Jobs*.

There is only one way, however, to generate high-level compliance pack **Dashboards** in DbProtect -- i.e., from the **Compliance Packs** page; for more information, see *Generating Compliance Pack Dashboards and Reports*.

What do you do with your compliance pack **Dashboard and report information once it's generated?** That's what this section explains.

Note: The current version of DbProtect supports the **DISA-STIG** compliance pack. Additional compliance packs -- for all supported regulations -- are in development and will be released soon. For more information on interpreting your generated **DISA-STIG** compliance pack Dashboards and reports, see *Interpreting Your Generated Compliance Pack Dashboards, and Displaying/Interpreting Your Generated Compliance Pack Reports*, below.

DISA-STIG Compliance Pack Dashboards and Reports

This topic consists of the following sub-topics:

- *What is DISA-STIG?*
- *Interpreting Your Generated DISA-STIG Compliance Pack Dashboards*
- *Displaying and Interpreting Your Generated DISA-STIG Compliance Pack Reports*

WHAT IS DISA-STIG?

Databases have become more frequent hacker targets leaving you vulnerable to disruption in operations, confidential information breaches, and national security risks. Application Security, Inc. empowers you with the security solutions to address the guidelines set forth by the *Defense Information Systems Agency's Database Security Technical Implementation Guide*.

The **Defense Information Systems Agency (DISA)** has responded to this threat with a new set of database security guidelines. The **Database Security Technical Implementation Guide (STIG)** presents the known security configuration items, vulnerabilities, and issues required to be addressed by DOD policy.

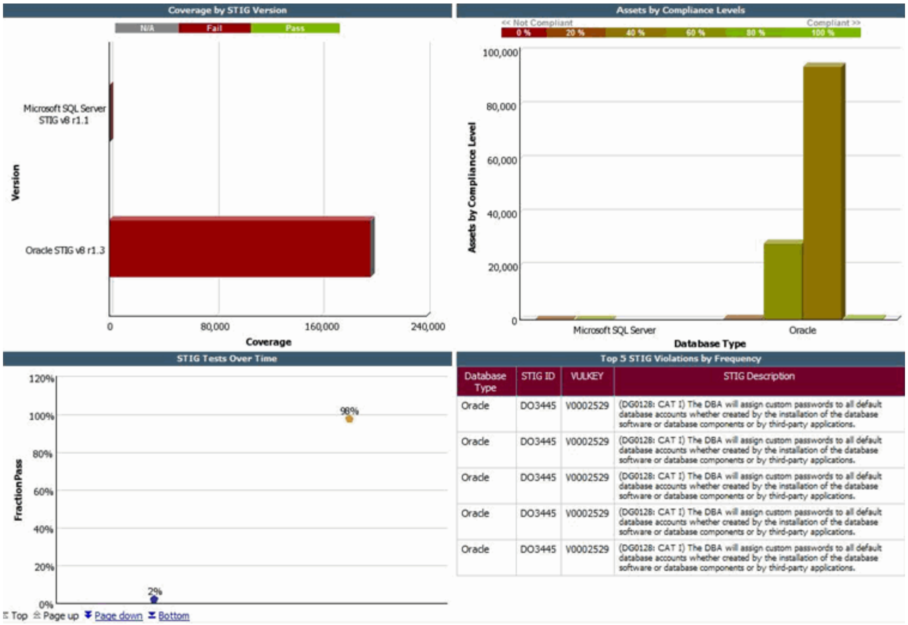
The STIG is provided under the authority of DOD Directive 8500.1. This directive requires that “all information assurance (IA) and IA-enabled IT products incorporated into DOD information systems shall be configured in accordance with DOD approved security configuration guidelines”. Implementing the recommendations and checklists outlined in the DISA-STIG will ensure DOD environments meet these security requirements and comply with this mandate.

Application Security, Inc. has created an automated policy for implementing the DISA-STIG requirements for database security. Using of the DISA-STIG Policy with the AppDetectivePro and DbProtect Vulnerability Management tools -- as well as the DISA-STIG compliance pack in DbProtect (explained herein) -- allows you to verify compliance with STIG checklist requirements and avoid the long, often painful, manual checklist process. This reduces implementation time by weeks, even months, and provides significant auditing information to satisfy compliance reporting requirements.

INTERPRETING YOUR GENERATED DISA-STIG COMPLIANCE PACK DASHBOARDS

After you import a DISA-STIG compliance pack (explained in *Importing a Compliance Content Pack*) you can generate your **DISA-STIG compliance pack Dashboards and reports** (explained in *Generating Compliance Pack Dashboards and Reports*).

The **DISA-STIG Compliance Pack Dashboards** are shown below.



Top 5 STIG Violations by Frequency

Database Type	STIG ID	VULKEY	STIG Description
Oracle	DO3445	V0002529	(DG0128: CAT I) The DBA will assign custom passwords to all default database accounts whether created by the installation of the database software or database components or by third-party applications.
Oracle	DO3445	V0002529	(DG0128: CAT I) The DBA will assign custom passwords to all default database accounts whether created by the installation of the database software or database components or by third-party applications.
Oracle	DO3445	V0002529	(DG0128: CAT I) The DBA will assign custom passwords to all default database accounts whether created by the installation of the database software or database components or by third-party applications.
Oracle	DO3445	V0002529	(DG0128: CAT I) The DBA will assign custom passwords to all default database accounts whether created by the installation of the database software or database components or by third-party applications.
Oracle	DO3445	V0002529	(DG0128: CAT I) The DBA will assign custom passwords to all default database accounts whether created by the installation of the database software or database components or by third-party applications.

FIGURE: DISA-STIG Compliance Pack Dashboards

DbProtect includes the following DISA-STIG compliance pack Dashboards:

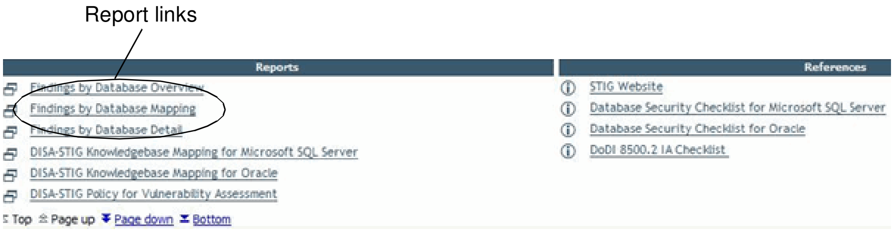
- **Coverage by STIG Version.** This Dashboard displays which STIG versions your scanned databases are compliant and not compliant with (i.e., **FAIL** or **PASS**).
- **Assets by Compliance Levels.** This Dashboard graphically displays what percentage of your scanned databases that have achieved (or not achieved) DISA-STIG compliance, by database type.
- **Coverage.** This Dashboard graphically displays STIG tests over time, and how well your organization has done with achieving) DISA-STIG compliance.
- **Database Type.** This Dashboard graphically the top five most frequent STIG violations that DbProtect has detected over time.

DISPLAYING AND INTERPRETING YOUR GENERATED DISA-STIG COMPLIANCE PACK REPORTS

After you import a DISA-STIG compliance pack (explained in *Importing a Compliance Content Pack*) you can generate your **DISA-STIG compliance pack Dashboards and reports** (explained in *Generating Compliance Pack Dashboards and Reports*).

Note: You can also run DISA-STIG Compliance Pack reports as Report Jobs in DbProtect Vulnerability Management; for more information, see *Report Jobs.*

The **DISA-STIG Compliance Pack report links** are labeled below.


Report links

Reports
Findings by Database Overview
Findings by Database Mapping
Findings by Database Detail
DISA-STIG Knowledgebase Mapping for Microsoft SQL Server
DISA-STIG Knowledgebase Mapping for Oracle
DISA-STIG Policy for Vulnerability Assessment
Top
Page up
Page down
Bottom
References
STIG Website
Database Security Checklist for Microsoft SQL Server
Database Security Checklist for Oracle
DoDI 8500.2 IA Checklist

FIGURE: DISA-STIG Compliance Pack report links

To **display** a DISA-STIG Compliance Pack report, click the appropriate link. The DISA-STIG Compliance Pack reports are:

- **STIG Findings by Database Overview.** This report shows a summary of STIG compliance broken down by results that pass, fail, and are not applicable (N/A) for automated verification.
- **STIG Findings by Database Mapping.** This report shows the findings summary mapped to STIG compliance.
- **STIG Findings by Database Detail.** This report shows the detailed findings mapped to STIG compliance.

Data Sources

This section consists of the following chapters:

- *Understanding Data Sources*
- *Working with Oracle Audit Vault as a DbProtect Data Source*.

Understanding Data Sources

This chapter consists of the following topics:

- *What are Data Sources?*
- *Available Data Sources*.

What are Data Sources?

Starting with version 6.0, DbProtect allows you to register and aggregate data from third-party data sources, such as Oracle Audit Vault, and include this data in certain DbProtect Analytics reports.

You must register properly-configured data sources in order to use them. For example, Oracle Audit Vault must be properly-configured and you must meet certain DbProtect suite and DbProtect Analytics minimum system requirements. Then you must register it as a data source. For more information, see *Working with Oracle Audit Vault as a DbProtect Data Source*.

Available Data Sources

The current version of DbProtect supports the Oracle Audit Vault data source. For more information on the Oracle Audit Vault data source, see *Working with Oracle Audit Vault as a DbProtect Data Source*.

Working with Oracle Audit Vault as a DbProtect Data Source

Starting with DbProtect 6.0 and DbProtect Analytics 1.4, you can configure **Oracle Audit Vault** as a DbProtect data source. This means you can include Oracle Audit Vault data in certain DbProtect Analytics reports. This section explains everything you should know about configuring Oracle Audit Vault as a DbProtect data source.

This chapter consists of the following topics:

- *Which DbProtect Analytics Reports Use Oracle Audit Vault Data?*
- *Minimum Requirements for Using Oracle Audit Vault as a DbProtect Data Source*
- *Roles and Privileges Required to Use Oracle Audit Vault as a DbProtect Data Source*
- *Registering Oracle Audit Vault as a DbProtect Data Source*
- *Unregistering Oracle Audit Vault as a DbProtect Data Source*
- *Troubleshooting Oracle Audit Vault (as a DbProtect Data Source) Issues*.

Which DbProtect Analytics Reports Use Oracle Audit Vault Data?

If you are using Oracle Audit Vault to audit your databases, then certain DbProtect Analytics reports can include Oracle Audit Vault data. The specific DbProtect Analytics Reports that include Oracle Audit Vault data are:

- *Failed Logins Review Report*
- *Privileged Activity Report*
- *Threat Detailed Review Report*
- *Threat Detailed Review Report (with Knowledgebase Articles)*
- *Sarbanes-Oxley (SOX) - Vulnerability Assessment Report*
- *Payment Card Industry Data Security Standard (PCI DSS) - Activity Monitoring Report*.

For information on each DbProtect Analytics Report, see the *DbProtect Analytics User's Guide*.

In order to include Oracle Audit Vault data in your DbProtect Analytics Reports, you must properly install Oracle Audit Vault and register Oracle Audit Vault within DbProtect prior to running any DbProtect Analytics Reports that support Oracle Audit Vault data (explained in this section).

Minimum Requirements for Using Oracle Audit Vault as a DbProtect Data Source

In order to use Oracle Audit Vault as a DbProtect data source, you require, at a minimum, the following:

- DbProtect 6.0 or greater
- DbProtect Analytics 1.4 or greater
- A properly configured Oracle Audit Vault environment with data.
- Oracle Instant Client for 10g/11g.

Roles and Privileges Required to Use Oracle Audit Vault as a DbProtect Data Source

When you register Oracle Audit Vault as a data source within DbProtect, you will need to provide a database user. You must also have at least the following roles and privileges in order to successfully connect to Oracle Audit Vault:

- At least `SELECT` privileges to the `AUDIT_EVENT_FACT` table, as well as the following dimension (`*_DIM`) tables, under the schema owner `AVSYS`:

  ```
  -CLIENT_HOST_DIM
  -CLIENT_TOOL_DIM
  -USER_DIM
  -TARGET_DIM
  -EVENT_DIM
  -TIME_DIM
  -CONTEXT_DIM
  -SOURCE_DIM
  -PRIVILEGES_DIM
  ```
- The role `AV_AGENT`, which manages collection agents and collectors by starting, stopping, and resetting them. A user is created and granted this role prior to a collection agent installation. The Oracle Audit Vault collection agent software uses this role at run time to query Oracle Audit Vault for configuration information. For more information on the `AV_AGENT` role, see `http://download.oracle.com/docs/cd/E11062_01/admin.1023/e11059/avadm_mng_security.htm`.

Registering Oracle Audit Vault as a DbProtect Data Source

To register Oracle Audit Vault as a DbProtect data source:

1. Install DbProtect 6.0 or greater and Analytics 1.4 (bundled with the DbProtect 6.0 installation bootstrapper); for more information, see the *DbProtect Installation Guide.*
2. Install Oracle Instance Client. Do the following:
   - Go to the Oracle website and download the Oracle Instant Client that matches your Oracle and operating system versions. Unzip the Oracle Instant Client anywhere on the same host as where DbProtect Analytics is installed. For example, use Oracle Instant Client Package - Basic Lite, version 11.1.0.7.0 (32-bit) or greater for Oracle 11g (on Windows 2003 32-bit).

Caution! Use a 32-bit driver even on 64-bit Windows. Some versions of Oracle Instance Client do not accept parenthesis in the path.

- Copy the ojdbc5.jar file from the unzip Oracle Instance Client folder to the DbProtect Analytics installation folder webapps.

  For example: If you unzip the client to folder: C:\Program Files\Oracle\instantclient_11_1, and DbProtect is installed on C:\Program Files\AppSecInc\DbProtect, copy ojdbc5.jar from C:\Program Files\Oracle\instance_11_1 to C:\Program Files\AppSecInc\DbProtect\Reporting\media\c8\webapps\p2pd\WEB-INF\lib (substitute your installation directory if it isn't the default)
- Add Oracle Instance Client to the system path. Do the following:

  -Open the Microsoft Windows Control Panel.

  -Select System to display the System Properties dialog box.

  -Click the Advanced tab.

  -Click the Environment Variables button to display the Environment Variables dialog box.

  -In the System Variables portion of the Environment Variables dialog box, locate the Path variable and click the Edit button to display the Edit System Variable dialog box.

  -Append (not replace) instantclient_11_1 to the end of the path, e.g., C:\Program Files\Oracle\instantclient_11_1.
- Run the command services.msc.
- Restart the Cognos8 service.

3. Register your Oracle Audit Vault data source within DbProtect. Do the following:

- Log into the DbProtect Console as a user that has DbProtect administrator privileges; for more information, see *Logging Into the DbProtect Console (and DbProtect Console Login Troubleshooting)*.
- Click the Administration tab to display the DbProtect Console Administration page; for more information on the *DbProtect Administration: Content/ Compliance Packs, Data Sources, and System Information*.
- Click the Data Sources > Audit Vault link in the navigation panel.
- Click the Register button.
- Specify the Oracle Audit Vault data source connection information:

  -Host or IP. Enter the name of the host or IP address where Oracle Audit Vault Server is installed and running. If the host is on a different domain than the machine where DbProtect is installed, you **must** provide a fully-qualified domain name.

  -Port. Enter the port where the Oracle Audit Vault is installed. The default port is 1521.

  -Service name. Enter the Oracle Audit Vault service name, which is defined in TNSNAMES.ORA.

Note: TNSNAMES.ORA is a SQL*Net configuration file that defines databases addresses for establishing connections to them. This file normally resides in the ORACLE HOME\NETWORK\ADMIN directory.

-**Username.** Enter the user created during the Oracle Audit Vault server installation. This user requires certain roles and privileges; for more information, see *Roles and Privileges Required to Use Oracle Audit Vault as a DbProtect Data Source*.

-**Password.** Specify the password for the user specified in the **Username** field.

Note: If you encounter problems registering Oracle Audit Vault as a DbProtect data source, see *Troubleshooting Oracle Audit Vault (as a DbProtect Data Source) Issues*.

-**Test Connection**. The **Test Connection** checkbox is checked by default. When this checkbox is checked, DbProtect automatically checks whether there is a valid connection between the DbProtect Console and your data source. However, as explained in *SID Defined TNSNAMES.ORA is Different From Service Name*, if the Oracle SID defined in your TNSNAMES.ORA file is different from the **Service name** (explained above), the test connection will fail. You must **uncheck** the **Test Connection** checkbox to proceed.

4. Click the **Next** button to complete the Oracle Audit Vault data source registration.

5. Run a DbProtect Analytics report that includes Oracle Audit Vault data; for more information, see *Which DbProtect Analytics Reports Use Oracle Audit Vault Data?* and the *DbProtect Analytics User's Guide*.

Unregistering Oracle Audit Vault as a DbProtect Data Source

To unregister a registered version of Oracle Audit Vault:

1. In the DbProtect Console, click the **Administration** tab to display the DbProtect Console **Administration** page; for more information, see ***Displaying, Understanding, and Navigating the DbProtect Administration Page***.
2. Click the **Data Sources > Audit Vault** link in the navigation panel.
3. Click the **Unregister** button.
4. Confirm the unregistration.

Troubleshooting Oracle Audit Vault (as a DbProtect Data Source) Issues

This topic explains some issues you may encounter when using Oracle Audit Vault as a DbProtect data source, and how to troubleshoot these issues. As a general rule, you should consult your Oracle Audit Vault administrator if you are not sure whether Oracle Audit Vault is running.

This topic consists of the following sub-topics:

- *DbProtect Suite is Installed on a Machine Where the Domain is Not the Same as the Domain Where Oracle Audit Vault is Installed*
- *SID Defined TNSNAMES.ORA is Different From Service Name*
- *If Oracle Audit Vault Registration Fails, Verify the Connection*
- *Starting Oracle Audit Vault Agents and Collectors*
- *Checking Whether Oracle Audit Vault is Running*
- *Starting Oracle Audit Vault*
- *Stopping Oracle Audit Vault.*

DBPROTECT SUITE IS INSTALLED ON A MACHINE WHERE THE DOMAIN IS NOT THE SAME AS THE DOMAIN WHERE ORACLE AUDIT VAULT IS INSTALLED

Upon registering your data source (or test connecting via the Cognos **Administration** tab), you may encounter an error message such as this: `"QE-DEF-0068 Unable to connect to at least one database"`.

This error may mean your Oracle client was not installed or not configured properly. However, it could also be related to a cross-domain environment issue. If you installed the DbProtect suite on a machine where the domain is **not** the same as the domain where Oracle Audit Vault is installed, you must run the `Cognos8` service with a user that can access the domain controller (e.g., a domain user, not a local system user). For more information, see the *DbProtect Installation Guide*.

SID DEFINED TNSNAMES.ORA IS DIFFERENT FROM SERVICE NAME

If the Oracle SID defined in your `TNSNAMES.ORA` file is different from the **Service name** (specified when you register Oracle Audit Vault as a DbProtect data source), the connection will fail. You must **uncheck** the **Test Connection** checkbox in the data source registration portion of the DbProtect Console **Administration** page in order to proceed; for more information, see *Registering Oracle Audit Vault as a DbProtect Data Source*.

IF ORACLE AUDIT VAULT REGISTRATION FAILS, VERIFY THE CONNECTION

If Oracle Audit Vault registration fails (as explained in *Registering Oracle Audit Vault as a DbProtect Data Source*), you should verify the connection between your DbProtect Console server and your Oracle Audit Vault server. To do so, run the following command `telnet auditvaulthost` *`port`*, e.g., `telnet myauditvault 1521`.

STARTING ORACLE AUDIT VAULT AGENTS AND COLLECTORS

Once Oracle Audit Vault is running, log in as an Oracle Audit Vault administrator (typically `avadmin`) and start the collectors manually via the **Collectors** tab. If the screen still shows a communication problem, select the **Agents** tab and confirm the problem. If it shows up in the **Agents** tab as well, you must manually fix the problem for each agent.

Once the agent is available you may see an icon of a "down arrrow". This means `oc4j` is up but the agent/collector is down. Start the agent via the Oracle Audit Vault user interface under the **Agents** tab. Once the agent is up (indicated by an up arrow), go to the **Collectors** tab and start the collector(s).

CHECKING WHETHER ORACLE AUDIT VAULT IS RUNNING

To check whether Oracle Audit Vault is running:

1. SSH to the host where Oracle Audit Vault is installed.
2. Check if Oracle Audit Vault is running by executing the command `avctl show_av_status`. Alternately, you can run the `command ps -ef | grep oracleav`. If the process `oracleav` displays, then Oracle Audit Vault is running. For example:

```
oracle   23906     1  0 Aug03 ?        00:03:45 oracleav (LOCAL=NO)
```

STARTING ORACLE AUDIT VAULT

To start Oracle Audit Vault:

1. SSH to the host where Oracle Audit Vault is installed.
2. Run the command `avctl start_av`.

   Sample output:

```
AVCTL started

Starting OC4J...

OC4J started successfully.

TZ set to US/PacificOracle Audit Vault 10g Database Control Release
10.2.3.1.0  Copyright (c) 1996, 2008 Oracle Corporation.  All rights
reserved.

http://auditvault1:5700/av

Oracle Audit Vault 10g is running.
```

STOPPING ORACLE AUDIT VAULT

To stop Oracle Audit Vault:

1. SSH to the host where Oracle Audit Vault is running.
2. Run the command: `avctl stop_av` to stop Oracle Audit Vault and the entire Oracle Application Server. This may take a while.

   Sample output:

   ```
   AVCTL started

   Stopping OC4J...

   OC4J stopped successfully.
   ```

Hint: If this command fails to stop Oracle Audit Vault, you may need to kill the processes one by one running the `kill -9 nnnn` (where `nnnn` is the process ID).

Asset Management

This section consists of the following chapters:

- *Understanding Asset Management*
- *Asset Search*.

Understanding Asset Management

This chapter consists of the following topics:

- *What is Asset Management?*
- *Displaying the Asset Management Page*.

What is Asset Management?

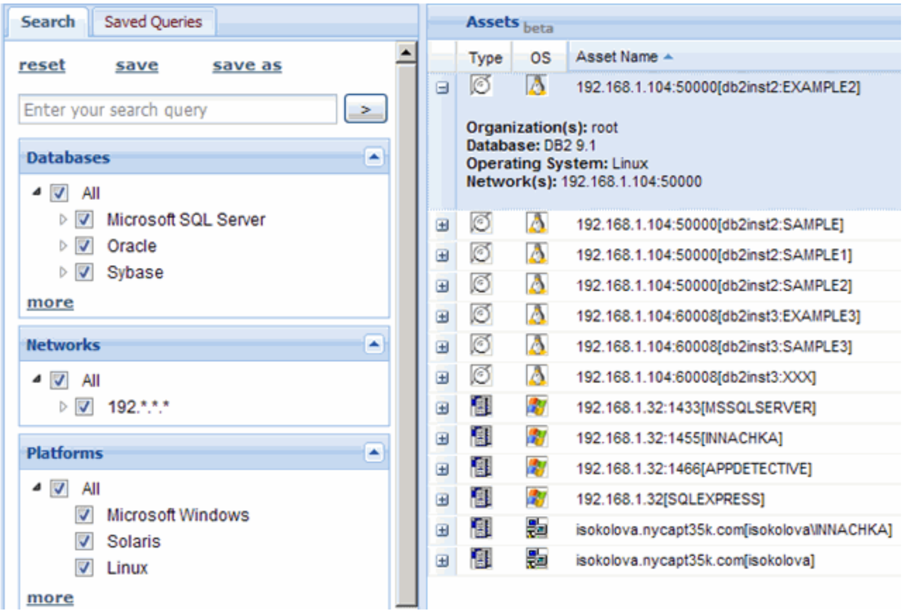
Starting with version 6.0, DbProtect includes a new beta feature called **Asset Management** which, in its current form, allows you to filter and query your database assets. A database **asset**, by definition, refers to any database in your enterprise that utilizes DbProtect's Vulnerability Management and DbProtect Audit and Threat Management technology. In other words, if your database has a Scan Engine or a Sensor installed, it's a manageable asset.

In future releases, Application Security, Inc. plans to expand the Asset Management feature to allow you to manage virtually **all** aspects of your asset inventory. For the time being, you must still conduct most Asset Management tasks using the Vulnerability Management tools and features described in the *Vulnerability Management* section of this guide.

The beta release of Asset Management includes **Asset Search** capabilities, which allow you to search your database assets based on specific filter and query criteria. You can save Asset Search queries for future use without having to repeat the process of re-configuring an Asset Search from scratch; for more information, see *Asset Search*.

Displaying the Asset Management Page

To display the **Asset Management** page, and access the Asset Management tools, click the **Asset Management** application tab from any DbProtect Console page; for more information on using the application tabs, see *Application Tabs*.



Databases
- ☑ All
  - ☑ Microsoft SQL Server
  - ☑ Oracle
  - ☑ Sybase

Networks
- ☑ All
  - ☑ 192.*.*.*

Platforms
- ☑ All
  - ☑ Microsoft Windows
  - ☑ Solaris
  - ☑ Linux

Type	OS	Asset Name
		192.168.1.104:50000[db2inst2:EXAMPLE2]

Organization(s): root
Database: DB2 9.1
Operating System: Linux
Network(s): 192.168.1.104:50000

Type	OS	Asset Name
		192.168.1.104:50000[db2inst2:SAMPLE]
		192.168.1.104:50000[db2inst2:SAMPLE1]
		192.168.1.104:50000[db2inst2:SAMPLE2]
		192.168.1.104:60008[db2inst3:EXAMPLE3]
		192.168.1.104:60008[db2inst3:SAMPLE3]
		192.168.1.104:60008[db2inst3:XXX]
		192.168.1.32:1433[MSSQLSERVER]
		192.168.1.32:1455[INNACHKA]
		192.168.1.32:1466[APPDETECTIVE]
		192.168.1.32[SQLEXPRESS]
		isokolova.nycapt35k.com[isokolova\INNACHKA]
		isokolova.nycapt35k.com[isokolova]

FIGURE: **Asset Management** page (default **Search** tab selected)

Currently, Asset Search is the only available Asset Management tool; for more information, see *Asset Search*.

Asset Search

This chapter consists of the following topics:

- *What is an Asset Search?*
- *Displaying the Asset Management Page*
- *Understanding the Components of Asset Search*
- *Performing an Asset Search*
- *Saving Your Asset Search as a Query*
- *Working with Saved Asset Search Queries*
- *Deleting a Saved Asset Search Query*.

What is an Asset Search?

Asset Search is an Asset Management tool that allows you to identify which database assets match specific Asset Search free-form query and/or filter tool criteria. Performing an Asset Search lets you quickly find out answers to questions like:

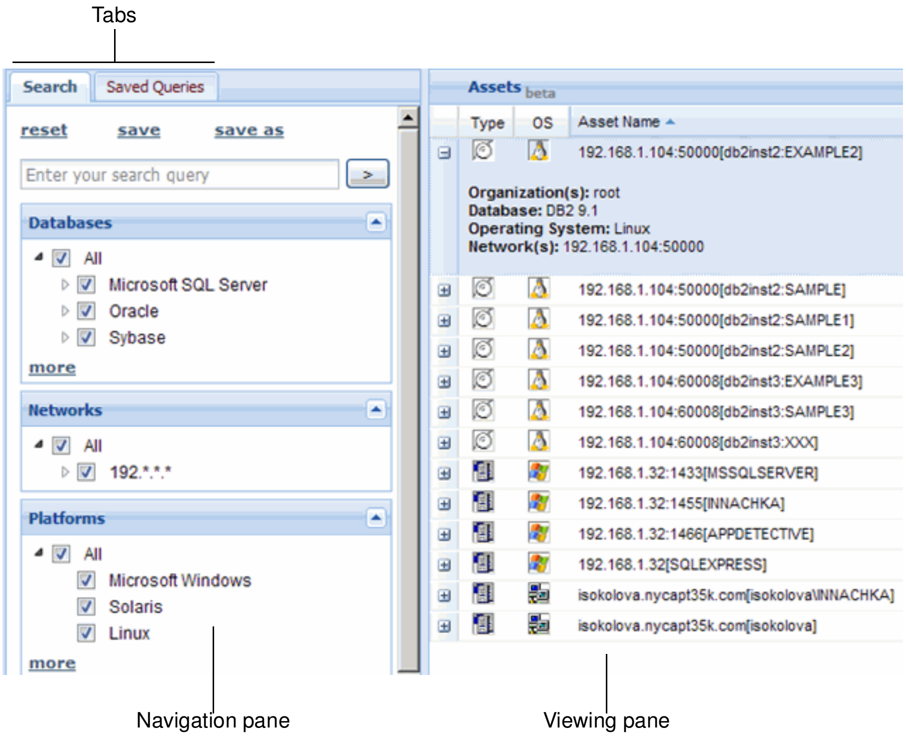
- *"How many Oracle database assets are in my enterprise?"*
- *"Which database assets with a network address starting with* `172` *are in my enterprise?"*
- *"How many database assets in my enterprise are running on Windows?"*
- *"Which database assets in my enterprise belong to a specific Organization?"*
- *"Which database assets in my enterprise have fired Alerts in the past month?"*
- *"Which database assets in my enterprise have weak passwords and patchable vulnerabilities?"*

Most Asset Searches consist of a **combination** of filter and search terms, e.g., *"How many Oracle databases on Windows have fired Alerts in the past month?"* Importantly, the Asset Search filter tools and the free-form query field are **not** mutually exclusive. In other words, for maximum efficiency you can perform your Asset Search using **both** the Asset Search filter tools and the free-form query field.

Understanding the Components of Asset Search

As explained in *Displaying the Asset Management Page*, you display the **Asset Management** page by clicking the **Asset Management** application tab from any DbProtect Console page; for more information. Currently, Asset Search is the only Asset Management tool that displays on the **Asset Management** page.

The **components** of Asset Search are labeled below.



Type	OS	Asset Name
		192.168.1.104:50000[db2inst2:EXAMPLE2]
		192.168.1.104:50000[db2inst2:SAMPLE]
		192.168.1.104:50000[db2inst2:SAMPLE1]
		192.168.1.104:50000[db2inst2:SAMPLE2]
		192.168.1.104:60008[db2inst3:EXAMPLE3]
		192.168.1.104:60008[db2inst3:SAMPLE3]
		192.168.1.104:60008[db2inst3:XXX]
		192.168.1.32:1433[MSSQLSERVER]
		192.168.1.32:1455[INNACHKA]
		192.168.1.32:1466[APPDETECTIVE]
		192.168.1.32[SQLEXPRESS]
		isokolova.nycapt35k.com[isokolova\INNACHKA]
		isokolova.nycapt35k.com[isokolova]

Organization(s): root
Database: DB2 9.1
Operating System: Linux
Network(s): 192.168.1.104:50000

FIGURE: Asset Search

This topic consists of the following sub-topics:

- *Understanding the Asset Search Tabs*
- *Understanding the Navigation and Viewing Panes*.

UNDERSTANDING THE ASSET SEARCH TABS

Asset Search consists of two **tabs**: the **Search** tab and the **Saved Queries** tab.

FIGURE: Asset Search tabs

When the default **Search** tab is selected, you can perform your Asset Search by entering valid search parameters in the free-form query field and/or by using the filter tools. For more information, see *Performing an Asset Search*. In addition, when the **Search** tab is selected, you can save your Asset Search as a query; for more information, see *Saving Your Asset Search as a Query*.

When the **Saved Queries** tab is selected, you can:

- retrieve your saved Asset Search queries; for more information, see *Working with Saved Asset Search Queries*
- delete a saved asset management query; for more information, see *Deleting a Saved Asset Search Query*.

UNDERSTANDING THE NAVIGATION AND VIEWING PANES

Regardless of which tab you select, Asset Search consists of two panes: the **navigation pane** (on the left) and the **viewing pane** (on the right). The actual contents of these panes depends on which Asset Search tab is selected.

When the **Search** tab is selected, the navigation pane displays the free-form query field and the Asset Search filter tools, which allow you to perform your Asset Search.

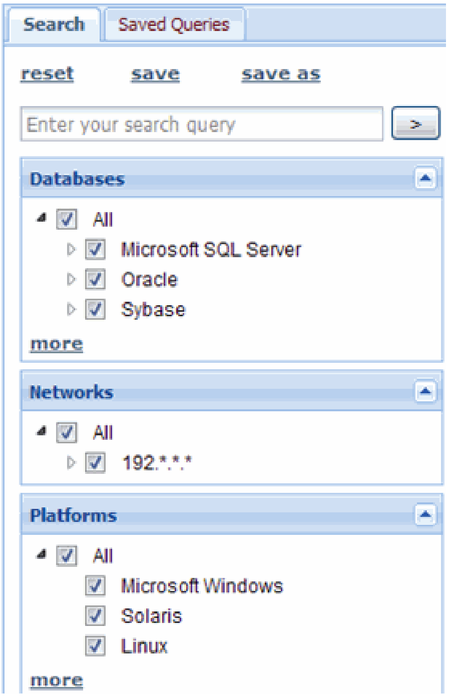
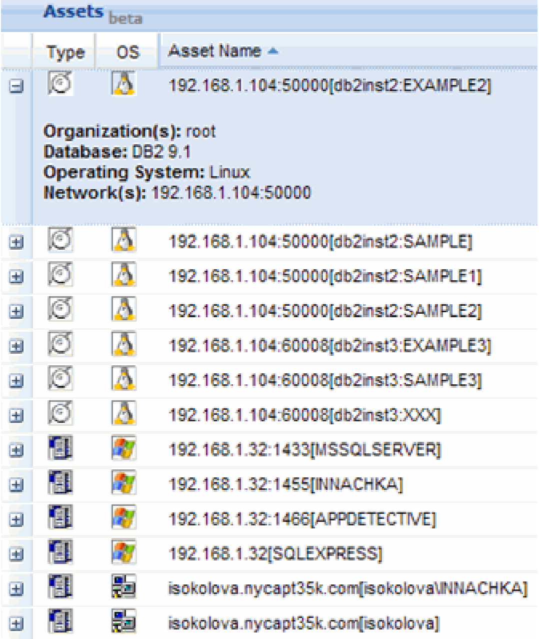


FIGURE: Navigation pane (**Search** tab selected)

After you perform your Asset Search, the **viewing pane** (shown below) displays your Asset Search results.



Assets beta

Type	OS	Asset Name
		192.168.1.104:50000[db2inst2:EXAMPLE2]

Organization(s): root
Database: DB2 9.1
Operating System: Linux
Network(s): 192.168.1.104:50000

Type	OS	Asset Name
		192.168.1.104:50000[db2inst2:SAMPLE]
		192.168.1.104:50000[db2inst2:SAMPLE1]
		192.168.1.104:50000[db2inst2:SAMPLE2]
		192.168.1.104:60008[db2inst3:EXAMPLE3]
		192.168.1.104:60008[db2inst3:SAMPLE3]
		192.168.1.104:60008[db2inst3:XXX]
		192.168.1.32:1433[MSSQLSERVER]
		192.168.1.32:1455[INNACHKA]
		192.168.1.32:1466[APPDETECTIVE]
		192.168.1.32[SQLEXPRESS]
		isokolova.nycapt35k.com[isokolova\INNACHKA]
		isokolova.nycapt35k.com[isokolova]

FIGURE: Viewing pane (Asset Search results)

Note: The columns of your Asset Search results (in the viewing pane) are sortable. To sort your Asset Search data, click a column header. For example, if you want to sort your Asset Search data by asset type, then click the **Type** column header.

For more information, see *Performing an Asset Search*.

On the other hand, when the **Saved Queries** tab is selected, the navigation pane displays any saved Asset Search queries.

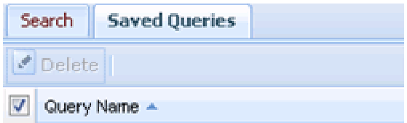


FIGURE: Viewing pane (**Saved Queries** tab selected)

You can select one or more saved Asset Search queries and:

- modify or run them; for more information, see *Working with Saved Asset Search Queries*
- delete them; for more information, see *Deleting a Saved Asset Search Query*.

Performing an Asset Search

When the **Search** tab is selected, you can configure your Asset Search using the:

- **free-form query field**, which allows you to enter query parameters; for more information, see *Understanding the Asset Search Free-Form Query Field*
- **filter tools**, which are broken down into categories; for more information, see *Understanding the Asset Search Filter Tools*.

As noted earlier, the Asset Search free-form query field and filter tools are **not** mutually exclusive. In other words, you can perform your Asset Search using **both** the free-form query field and the filter tools.

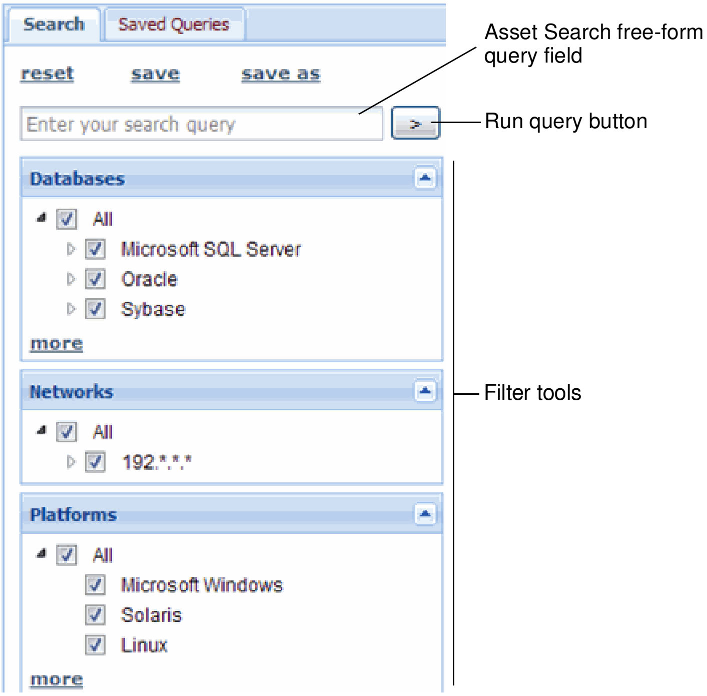


FIGURE: Free-form query field, filter tools, and the run query button

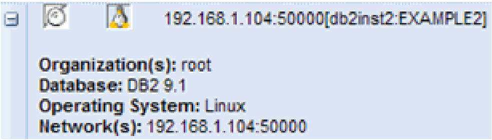
To run an Asset Search using the Asset Search free-form query field and/or filter tools, do the following:

1. Click the **Search** tab (in the upper-left portion of the **Asset Management** page).
2. In the navigation pane:
   - enter query terms in the free-form query field; for more information, see *Understanding the Asset Search Free-Form Query Field*
   - use the categorized Asset Search **filter tools** to fine-tune your Asset Search; for more information, see *Understanding the Asset Search Filter Tools*.
3. Click the **run query button** (next to the free-form query field) to run your query. Your Asset Management query results will display in the viewing pane; for more information, see *Understanding the Navigation and Viewing Panes*.

The results of your Asset Search display in the following sortable columns:

- **Type**
- **OS**
- **Asset Name**
- **Database**.

Furthermore, you can click the **+** icon next to any asset to expand individual assets (as shown below).



192.168.1.104:50000[db2inst2:EXAMPLE2]

Organization(s): root
Database: DB2 9.1
Operating System: Linux
Network(s): 192.168.1.104:50000

FIGURE: Viewing pane (expanded Asset Search results)

UNDERSTANDING THE ASSET SEARCH FREE-FORM QUERY FIELD

The Asset Search **free-form query field** in the navigation pane (shown below) allows you to fine-tune your Asset Search by entering specific query parameters.

Important: As noted earlier, the Asset Search free-form query field and filter tools are **not** mutually exclusive. In other words, you can perform your Asset Search using **both** the free-form query field and the filter tools.

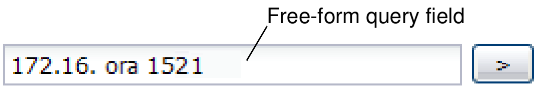


FIGURE: Free-form query field

When you enter query terms in the free-form query field, DbProtect searches your assets across the following attributes:

- **Asset name**
- **Database instance name**
- **Host address**
- **Port**.

Hint: You can click the **>reset** link to clear the free-form query field.

You can enter multiple query terms (separated by a space) to further narrow your Asset Search results. Asset Search only returns assets which have include each search term as part of **at least one** of its attributes (i.e., asset name, instance name, host address, or port number).

For example, if you enter the query terms `172.16 ora 1521` (as displayed above), Asset Search returns assets where:

- the **asset name** OR **instance name** OR **host address** OR **port number** contain `172.16`

  AND

- the **asset name** OR **instance name** OR **host address** OR **port number** contain `ora`

  AND

- the **asset name** OR **instance name** OR **host address** OR **port number** contain `1521`

Hint: You **cannot** use `*` wildcards in the free-form query field. Use partial query terms instead (which works the same as using a `*` wildcard).

UNDERSTANDING THE ASSET SEARCH FILTER TOOLS

The Asset Search **filter tools** in the navigation pane are broken down into **categories** (e.g., **Databases**, **Networks**, **Platforms**, etc.).

Each Asset Search filter tool category is comprised of **facets** (and sub-facets) of searchable data attributes. The filter tools allow you to fine-tune your Asset Search according to broad (or narrow) search parameters.

Important: As noted earlier, the Asset Search free-form query field and filter tools are **not** mutually exclusive. In other words, you can perform your Asset Search using **both** the free-form query field and the filter tools.

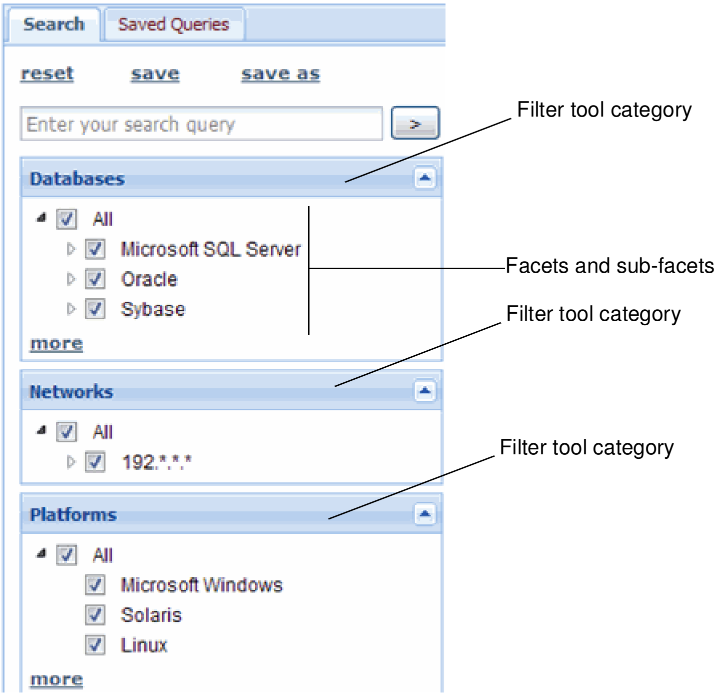
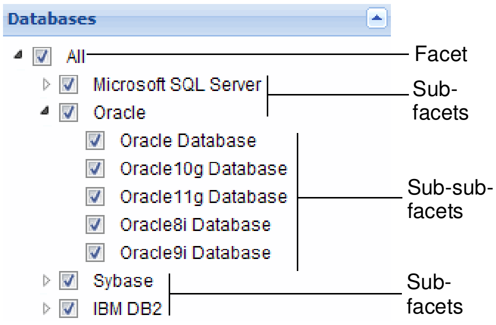


FIGURE: Filter tools

Initially, the navigation pane displays four *open* filter tool categories (i.e., **Databases**, **Networks**, **Platforms**, and **Organizations**) and two *closed* filter tool categories (i.e., **Findings** and **Threats**).

The following table explains each available filter tool link and icon, and how facets and sub-facets work within Asset Search.

Filter tool link/icon	Description
more link more	Click the **more** link to display more filter tool options.
less link less	Click the **less** link to display fewer filter tool options.
up arrow icon ▲	Click the **up arrow icon** to open a filter tool.
down arrow icon ▼	Click the **down arrow icon** to close a filter tool.

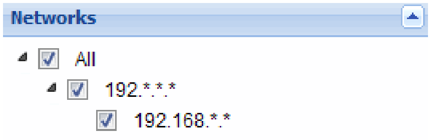
Filter tool link/icon	Description
facet/sub-facet arrow icons ▷ ◢  Databases All Microsoft SQL Server Oracle Oracle Database Oracle10g Database Oracle11g Database Oracle8i Database Oracle9i Database Sybase IBM DB2 Facet Sub-facets Sub-sub-facets Sub-facets	All filter tool categories employ **facets** and **sub-facets** to reduce the volume of displayed data. A facet is an attribute within a given filter tool category. For example, **All** is a facet within the **Databases** category, i.e., all databases. A sub-facet is an attribute that is logically related to its parent facet (for example, **Oracle**, **Sybase**, and **IBM DB2** are sub-facets of the parent facet **All** databases). In some cases, you can "drill down" to the sub-sub-facet level. For example, the sub-facet **Oracle** contains Oracle version sub-sub-facets, i.e., **Oracle 10g Database**, **Oracle 11g Database**, etc. When an **arrow icon** displays next to a facet, you know the facet contains sub-facets. Likewise, when an arrow icon displays next to a sub-facet, you know the sub-facet contains sub-sub-facets. Click the arrow icons to expand (and contract) the facets and sub-facets beneath.

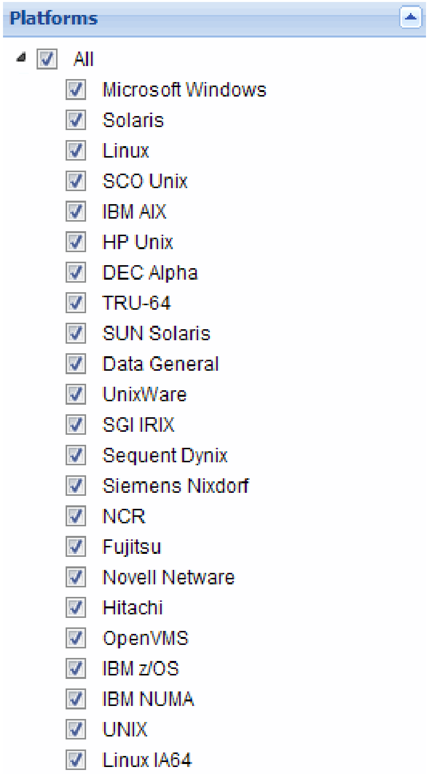
When a filter tool category is initially closed, Asset Search does **not** apply a filter condition for that category. For example, if you don't open the **Threats** filter tool category, Asset Search does **not** consider the **Threats** filter tool category during the Asset Search. In other words, it will return assets whether or not they are being monitored and whether or not Alerts have been received for those assets.

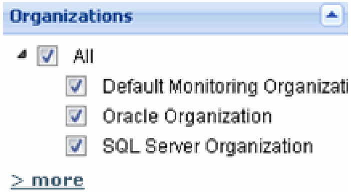
Note: If you open a filter tool category, make selections, and then close the filter tool category, your selections will be applied to the Asset Search despite the filter tool category is closed.

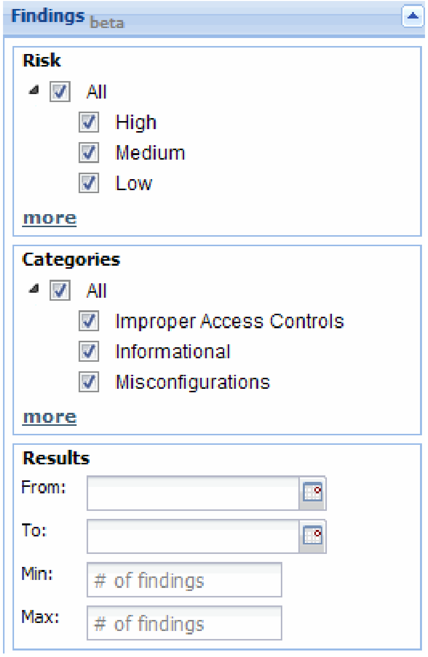
Similarly, if you check the **All** facet checkbox, then Asset Search does **not** apply a filter condition for a given filter tool category. For example, if you check the **All** facet checkbox in the **Platforms** filter tool category, then DbProtect will perform an Asset Search on **all** platforms. On the other hand, if you uncheck the **All** facet checkbox (in the Platforms filter tool category) and, instead, only check the **Microsoft Windows** sub-facet checkbox, then DbProtect will only return assets that run on Microsoft Windows.

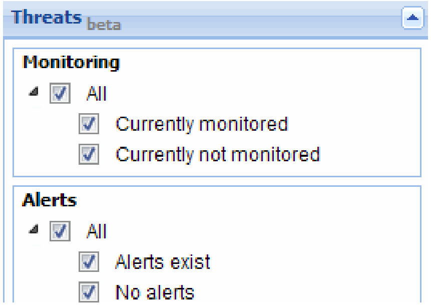
The following table lists each filter tool category.

Asset Search filter tool category	Description
Networks  Networks ☑ All ☑ 192.*.*.* ☑ 192.168.*.*	This filter tool category allows you to run a query against assets in your enterprise according to specific network IP addresses. For example, if you want to know which assets in your enterprise have a network address starting with `172`, you would only check the **192.*.*.*** sub-facet checkbox in the **Networks** filter tool category. You can check the **All** facet checkbox to run a query against **all** network IP addresses, or you can uncheck the **All** facet checkbox and, instead, select individual network IP address prefixes (where assets have been detected).

Asset Search filter tool category	Description
Platforms  Platforms ☑ All ☑ Microsoft Windows ☑ Solaris ☑ Linux ☑ SCO Unix ☑ IBM AIX ☑ HP Unix ☑ DEC Alpha ☑ TRU-64 ☑ SUN Solaris ☑ Data General ☑ UnixWare ☑ SGI IRIX ☑ Sequent Dynix ☑ Siemens Nixdorf ☑ NCR ☑ Fujitsu ☑ Novell Netware ☑ Hitachi ☑ OpenVMS ☑ IBM z/OS ☑ IBM NUMA ☑ UNIX ☑ Linux IA64	This filter tool category allows you to run a query against assets in your enterprise according to specific operating systems. For example, if you want to know which assets in your enterprise run on **HP UX Itanium 32** and **HP UX Itanium 64**, you would only check the **HP UX Itanium 32** and **HP UX Itanium 64** sub-facet checkboxes in **Platforms** filter tool category. You can check the **All** facet checkbox to run a query against all platforms, or you can uncheck the **All** facet checkbox and, instead, select individual platforms (e.g., **Microsoft Windows**, **Solaris**, **Linux**, etc.).

Asset Search filter tool category	Description
Organizations  Organizations All Default Monitoring Organizati Oracle Organization SQL Server Organization > more	This filter tool category allows you to run a query against assets in your enterprise according to specific Organizations. For example, if you want to know which assets are associated with your **Default Monitoring Organization**, you would only check the **Default Monitoring Organization** sub-facet checkbox in the **Organizations** filter tool category. You can check the **All** facet checkbox to run a query against all Organizations, or you can uncheck the **All** facet checkbox and, instead, select individual Organizations. Unlike other filter tools that include pre-configured facets, the Organizations that display in the **Organizations** Asset Search filter tool category depend on the Organizations you have created for your enterprise; for more information, see *DbProtect Organizations, Users, and User Roles*.

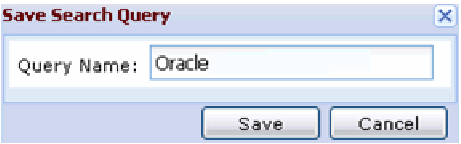
Asset Search filter tool category	Description
Findings  Findings beta Risk ☑ All ☑ High ☑ Medium ☑ Low more Categories ☑ All ☑ Improper Access Controls ☑ Informational ☑ Misconfigurations more Results From: To: Min: # of findings Max: # of findings	This filter tool category consists of the following sub-categories: • **Risk.** This sub-category allows you to perform an Asset Search according to the risk levels of detected findings. You can check the **All** facet checkbox to perform an Asset Search against all checks where findings (of any Risk level) have been reported. Or uncheck the **All** facet checkbox and, instead, select one or more of the following finding Risk levels: **High**, **Medium**, **Low**, or **Informational**. • **Categories.** This sub-category allows you to perform an Asset Search according to a specific category of detected findings. For example, maybe you only want to know which assets contain Sensors that have detected **High** risk level findings. In this case, you would only check the **High** facet checkbox. • **Results**. This sub-category allows you to perform an Asset Search against your assets according to checks (in all Policies deployed to your Scan Engines) that yielded findings within a specified date range. You can also set a minimum and maximum number of checks with findings. For example, let's say you want to know which assets yielded findings against a minimum of 10 different checks in the month of January 2010. To do so, you would specify the **From:** and **To:** date facet fields (`01/01/10` and `01/31/10`, respectively). Next, you would specify a **Min:** number of findings (`10`). Hint: You can enter the **From:** and **To:** dates manually using the `MM/DD/YYYY` format, or you can click the calendar icons to display a calendar and select your **From:** and **To:** dates.

Asset Search filter tool category	Description
Threats  Threats beta Monitoring ☑ All ☑ Currently monitored ☑ Currently not monitored Alerts ☑ All ☑ Alerts exist ☑ No alerts	This filter tool category consists of the following sub-categories: • **Monitoring.** This sub-category allows you to search which assets currently have Sensors that are monitoring (or Sensors that are **not** monitoring) threats using DbProtect Audit and Threat Management technology. For example, assume you only want to know which assets are currently being monitored. In this case, you would check the **Currently monitored** sub-facet checkbox, and uncheck the **Currently not monitored** checkbox. For more information, see *Audit and Threat Management*. • **Alerts.** This sub-category allows you to search which assets (with Sensors installed on them) currently contain Alerts, and/or which assets (with Sensors installed on them) currently contain no Alerts. For example, assume you only want to know which assets (with Sensors installed on them) currently contain Alerts. In this case, you would check the **Alerts exist** sub-facet checkbox (and uncheck the **No alerts** sub-facet checkbox).

Saving Your Asset Search as a Query

To save an Asset Search as a query:

1. With the **Search** tab (in the upper-left portion of the **Asset Management** page) selected, click the **> save** link in the navigation pane to display the **Save Search Query** pop up.


Save Search Query

Query Name: Oracle

FIGURE: **Save Search Query** pop up

2. Enter the name of your Asset Search query in the **Query Name:** field.
3. Click the **Save** button to save your Asset Search query. Your saved Asset Search query will now display in the navigation pane of the **Asset Management** page when you click the **Saved Queries** tab; for more information, see *Working with Saved Asset Search Queries*.

Working with Saved Asset Search Queries

When the **Saved Queries** tab is selected, your saved Asset Search queries will display in the navigation pane. The viewing pane will display the results of your saved Asset Search queries (when you run them).

To select and run a saved Asset Search query:

1. Click the **Saved Queries** tab to display your saved queries in the navigation pane.

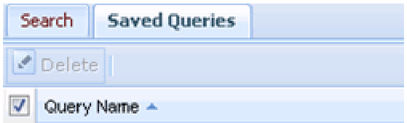


FIGURE: Navigation pane (**Saved Queries** tab selected)

2. Select which saved Asset Search query you want to run, and it will run automatically. The **Search** tab is automatically selected, and your Asset Search query results display in the viewing pane.

Hint: You can check the **Query Name** checkbox to select all saved queries.

Deleting a Saved Asset Search Query

When the **Saved Queries** tab is selected, your saved Asset Search queries display in the navigation pane. You can delete one or more saved Asset Search queries.

To delete one or more saved Asset Search queries:

1. Click the **Saved Queries** tab to display your saved queries in the navigation pane.

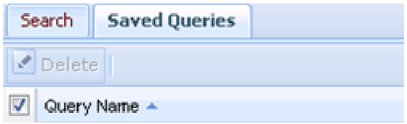


FIGURE: Navigation pane (**Saved Queries** tab selected)

2. Select which saved Asset Search query (or queries) you want to delete.

Hint: You can check the **Query Name** checkbox to select all saved queries.

3. Click the **Delete** button.
4. A pop up prompts you to confirm the delete.
5. Click the **Yes** button to delete your selected saved Asset Search query/ queries.

DbProtect Analytics

This section explains how to use **DbProtect Analytics**, and provides an overview of the Dashboard and Report elements. It also includes DbProtect Analytics troubleshooting help.

This section consists of the following chapters:

- *Understanding DbProtect Analytics*
- *DbProtect Analytics Dashboards*
- *DbProtect Analytics Reports*
- *DbProtect Analytics Troubleshooting.*

Understanding DbProtect Analytics

This chapter consists of the following topics:

- *What is DbProtect Analytics?*
- *DbProtect Analytics and Compliance Reporting*
- *Starting DbProtect Analytics*
- *Using the Toolbar Buttons to Navigate DbProtect Analytics*
- *Understanding Compliance Scores in DbProtect Analytics*.

What is DbProtect Analytics?

DbProtect Analytics is an essential component of the DbProtect suite of products. DbProtect Analytics includes new executive-level **Dashboards** for security, compliance, and operations, and a collection of **Reports** (including new compliance Reports for NIST 800-53, SOX, PCI DSS, HIPAA and DISA-STIG, and more).

DbProtect Analytics provides a global view of your enterprise's database security posture. This content is designed for executives, security risk managers, IT administration, and any personnel involved in the enforcement of regulatory/ corporate compliance policies and database patch administration.

DbProtect Analytics provides a convenient set of executive level Dashboards and key Reports that draw data from DbProtect's Vulnerability Management and Audit and Threat Management components.

DbProtect Analytics Dashboards provide better security and compliance transparency to executives and management. Dashboards are designed to support adhoc investigation with drill-through technology, combining assessment and monitoring data.

DbProtect Analytics and Compliance Reporting

The DbProtect Analytics **Compliance** Dashboard charts the compliance posture across your inventory of databases assessed and/or monitored by the DbProtect suite of products. In addition, DbProtect Analytics includes a set of Reports which displays vulnerability and threat data mapped using DbProtect's regulatory compliance mappings. Some key DbProtect Analytics compliance Reports include:

- Healthcare Services (HIPAA)
- Sarbanes-Oxley Act (SOX)
- Payment Card Industry (PCI) Data Security Standards
- National Institute of Standards and Technology (NIST).

Starting DbProtect Analytics

DbProtect Analytics is part of DbProtect suite. When you sign into the DbProtect Console, you will be able to access DbProtect Analytics via the **Analytics & Reporting** tab. For more information on logging into the DbProtect Console, see *Logging Into the DbProtect Console (and DbProtect Console Login Troubleshooting).*

DbProtect Analytics consists of Dashboards and Reports that span your entire organization's assets. The data displayed in the DbProtect Analytics Dashboards and drill-down reports is filtered by the "effective" Organization of the logged-in user.

Using the Toolbar Buttons to Navigate DbProtect Analytics

When you click the **Analytics & Reporting** tab (available on every DbProtect Console page) to display DbProtect Analytics, you will notice a group of **toolbar buttons**.

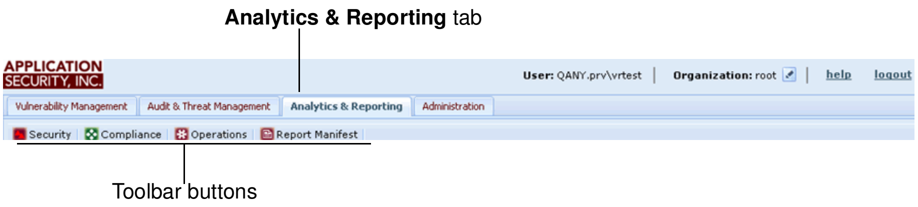


FIGURE: DbProtect Analytics toolbar buttons

There are two types of DbProtect Analytics toolbar buttons. They are:

- The **Dashboard** toolbar buttons (i.e., **Security**, **Compliance**, and **Operations**); for more information, see *DbProtect Analytics Dashboards*
- The **Report Manifest** toolbar button, which allows you to access DbProtect Analytics Reports; for more information, see *DbProtect Analytics Reports*

Understanding Compliance Scores in DbProtect Analytics

Several DbProtect Analytics reports and Dashboards display compliance score information as percentages. There are six levels of compliance, described below.

- **100%.** The asset was scanned and no vulnerabilities were found.
- **80%.** The asset was scanned at least one **Informational** vulnerability was found.
- **60%.** The asset was scanned at least one **Low** vulnerability was found.
- **40%.** The asset was scanned and at least one **Medium** vulnerability was found.
- **20%.** The asset was scanned and at least one **High** vulnerability was found.
- **0%.** The asset was **not** scanned.

DbProtect Analytics Dashboards

This chapter consists of the following topics:

- *What are DbProtect Analytics Dashboards?*
- *The Security Dashboard*
- *The Compliance Dashboard*
- *The Operations Dashboard*.

What are DbProtect Analytics Dashboards?

DbProtect Analytics provides executive **Dashboards** which contain information targeted toward specific areas of interest in most organizations. When you click the **Analytics & Reporting** tab (available on every DbProtect Console page) to display DbProtect Analytics, you will notice a group of **toolbar buttons**.

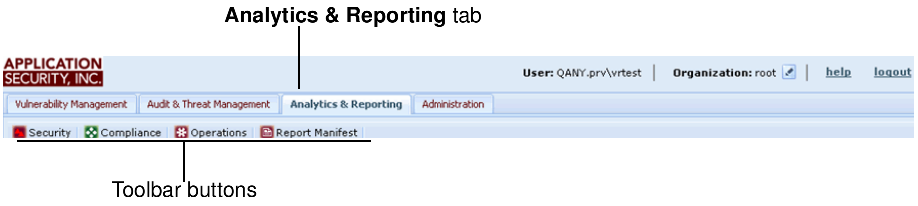


FIGURE: DbProtect Analytics toolbar buttons

The **Dashboard** toolbar buttons (i.e., **Security**, **Compliance**, and **Operations**) allow you to display the DbProtect Analytics Dashboards (i.e., the **Security**, **Compliance**, and **Operations** Dashboards, respectively).

Alternately, you can click the **Reports Manifest** link to display the Reports section, which contains up-to-the-minute DbProtect Analytics report data; for more information, see *DbProtect Analytics Reports*.

Starting with version 1.4, DbProtect Analytics Dashboards are Organization aware. Meaning, the dates displayed by the DbProtect Analytics Dashboards are filtered based on the "effective" Organization of the logged-in user, which is displayed on every page of the DbProtect Console; for more information, see *User ID and Associated "Effective" Organization*. If you change your "effective" Organization (as explained in *Setting Your "Effective" Organization*), the DbProtect Analytics Dashboards will refresh with the date associated with your new "effective" Organization.

For all Organizations (other than root), the DbProtect Analytics Dashboard data that displays is only for the current "effective" Organization, and does not drill down to children Organizations. For the root Organization, however, the DbProtect Analytics Dashboards allow you to drill down the entire Organizational structure, encompassing all assets across all Organizations. DbProtect Analytics Dashboards and Reports display the Organizational filtering structure in the upper left portion of each Dashboard and Report page.

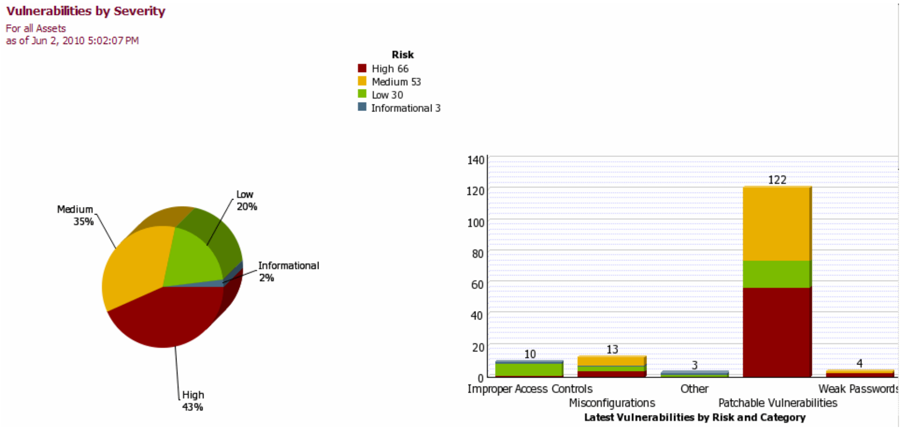
The Security Dashboard

The **Security Dashboard** consists of the following elements:

- *Vulnerabilities by Severity*
- *Threats by Severity.*

VULNERABILITIES BY SEVERITY

The **Vulnerabilities by Severity** Dashboard element computes the most recent result for any assessment test that was run within the scope of the associated Report. If the test revealed a vulnerability, it is aggregated into this Dashboard according to its severity and category. For tests that return a list of objects in violation (such as accounts with weak passwords, or objects with inappropriate privilege grants), the test result only counts as one violation.



Vulnerabilities by Severity

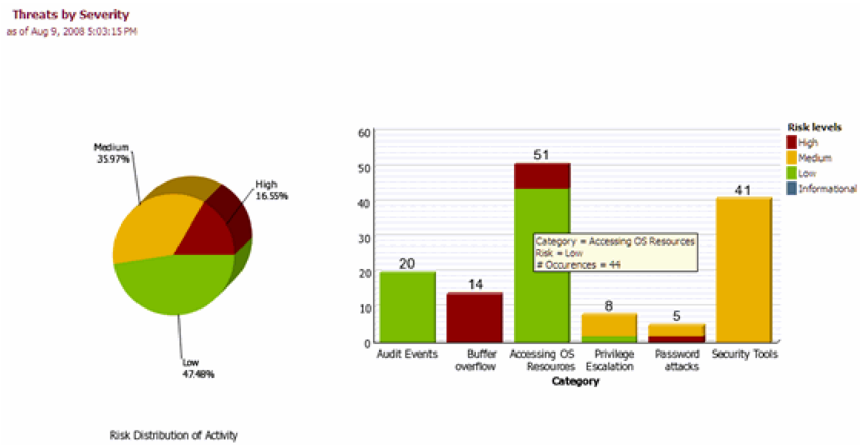
For all Assets

as of Jun 2, 2010 5:02:07 PM

FIGURE: Vulnerabilities by Severity Dashboard element

THREATS BY SEVERITY

The **Threats by Severity** Dashboard element computes the distribution of monitored security events aggregated by severity and category. The Dashboard shows no informational events or internal system audit events since they are not considered security events.


Threats by Severity
as of Aug 9, 2008 5:03:15 PM

Category = Accessing OS Resources
Risk = Low
Occurences = 44

FIGURE: Threats by Severity Dashboard element

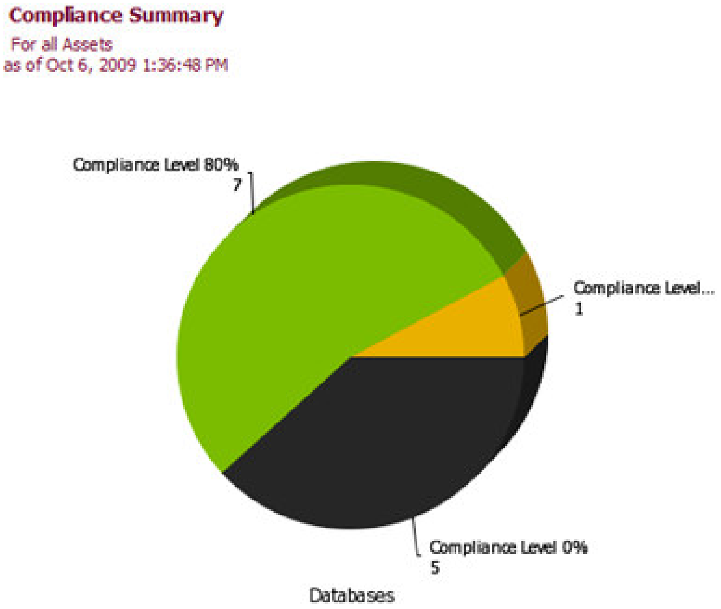
The Compliance Dashboard

The **Compliance Dashboard** consists of the following elements:

- *Compliance Summary*
- *Compliance by Database*
- *Aging Scan Activity*
- *Compensating Controls.*

COMPLIANCE SUMMARY

The **Compliance Summary** Dashboard element provides a view of the managed databases that meet a set of criteria. This Dashboard displays compliance score information as percentages. There are six levels of compliance, as described in *Understanding Compliance Scores in DbProtect Analytics*.



Compliance Summary Dashboard element

COMPLIANCE BY DATABASE

The **Compliance by Database** Dashboard element provides a view of the managed databases that meet a set of criteria. This Dashboard displays compliance score information as percentages. There are six levels of compliance, as described in *Understanding Compliance Scores in DbProtect Analytics*.

In this Dashboard element, DbProtect Analytics charts each database type separately, displaying the proportion of compliant assets within each database type.

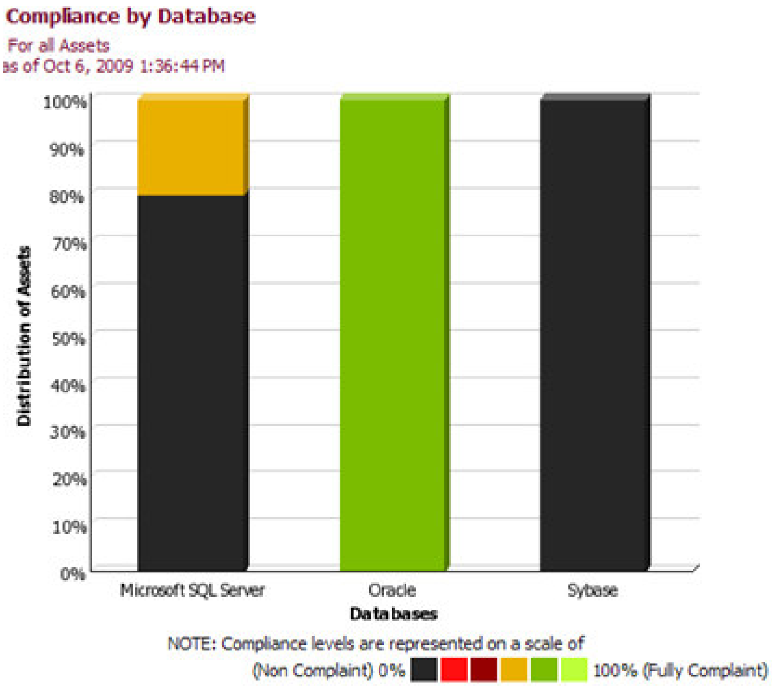


FIGURE: Compliance by Database Dashboard element

AGING SCAN ACTIVITY

The **Aging Scan Activity** Dashboard element shows the number of assets distributed across the age of the most recent scan data recorded for those assets. The complete inventory of databases is categorized into buckets of scan ranges (such as 0-30 days, 30-60 days, etc.). The assets that fall into each range are then aggregated by type (such as Oracle, IBM DB2, etc.) and scan ranges. These are shown as a set of stacked points (one for each database type) plotted along a time axis (scan ranges). You should be able to discern your average scan age by looking for the median scan age in this plot with the highest number of assets.

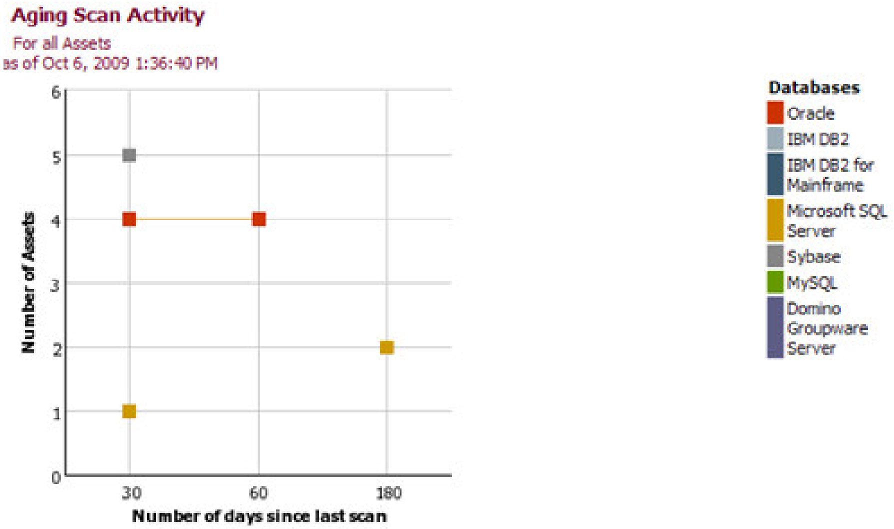


FIGURE: Aging Scan Activity Dashboard element

COMPENSATING CONTROLS

The **Compensating Controls** Dashboard element shows a distribution of database assets that have DbProtect Audit and Threat Management turned on. All other assets are classified with a monitoring status of **None/Unknown**.

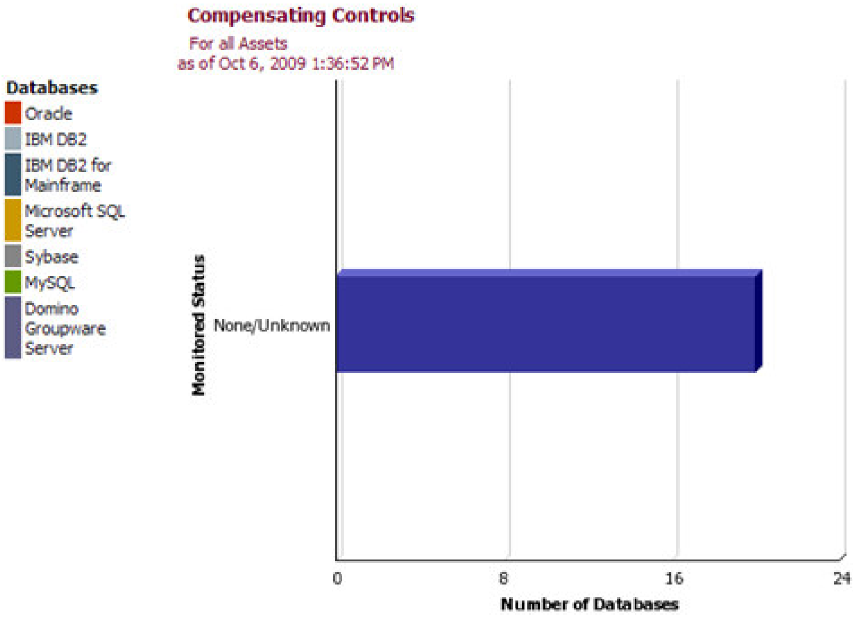


FIGURE: Compensating Controls Dashboard element

The Operations Dashboard

The **Operations Dashboard** consists of the following elements:

- *Database Distribution*
- *Recent Scan Jobs*
- *Scan Policy Usage*
- *Inactivity Trends.*

DATABASE DISTRIBUTION

The **Database Distribution** Dashboard element shows all discovered database instances aggregated by the type of asset (such as Oracle, IBM DB2, etc.). This inventory data does **not** include supplemental services such as Oracle listeners or Microsoft SQL Redirectors.

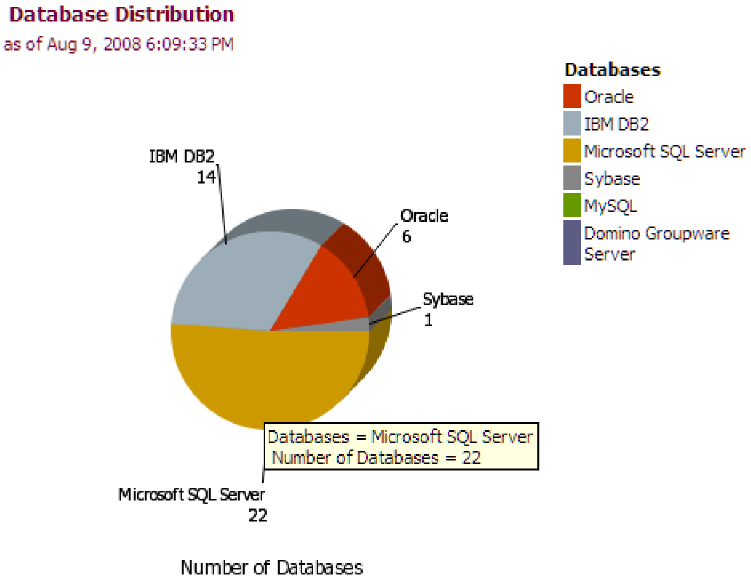
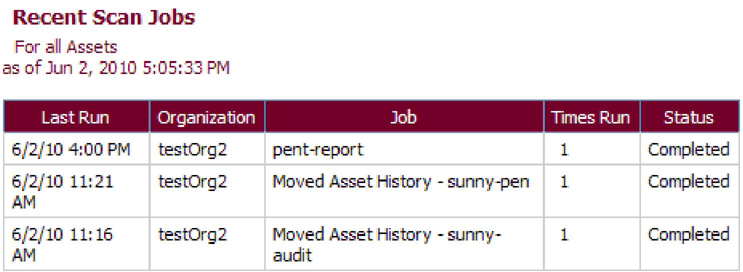


FIGURE: Database Distribution Dashboard element

RECENT SCAN JOBS

The **Recent Scan Jobs** Dashboard element shows a list of the 15 most recent scan jobs. It serves as a quick snapshot of what jobs are being run, how often, status of the job, and the organization from which the job was executed.



Recent Scan Jobs

For all Assets
as of Jun 2, 2010 5:05:33 PM

Last Run	Organization	Job	Times Run	Status
6/2/10 4:00 PM	testOrg2	pent-report	1	Completed
6/2/10 11:21 AM	testOrg2	Moved Asset History - sunny-pen	1	Completed
6/2/10 11:16 AM	testOrg2	Moved Asset History - sunny-audit	1	Completed

FIGURE: Recent Scan Jobs Dashboard element

SCAN POLICY USAGE

The **Scan Usage Policy** Dashboard element displays the aggregated usage counts for Vulnerability Management Policies. Since these Policies are categorized as Penetration Test and Audit Policies, the Dashboard aggregates the usage along the same categories. Within each category, the proportion of individual Policy usage is stacked to show the relative use. This serves as an easy reference point to determine whether Policies are being used for assessment which deviate from corporate mandates.

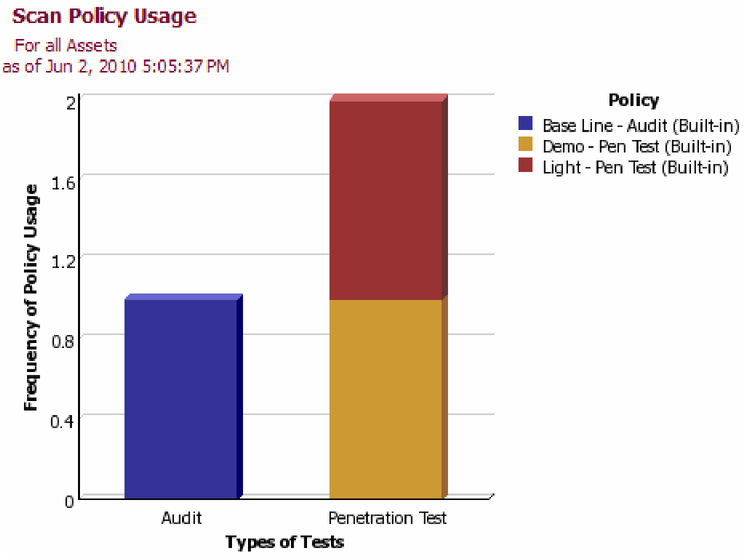


FIGURE: Scan Policy Usage Dashboard element

INACTIVITY TRENDS

The **Inactivity Trends** Dashboard element provides an aggregation of inactivity alerts over the last twelve months system wide. It is a very high-level view of overall levels of detected inactivity. This allows you to easily identfiy database assets that might be offline (or network unreachable), or have unusual usage patterns over time.

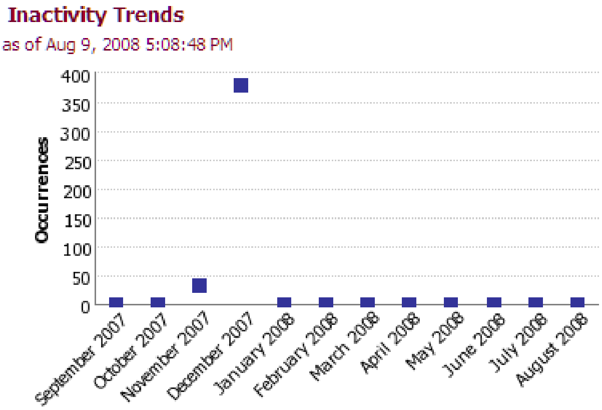


FIGURE: Inactivity Trends Dashboard element

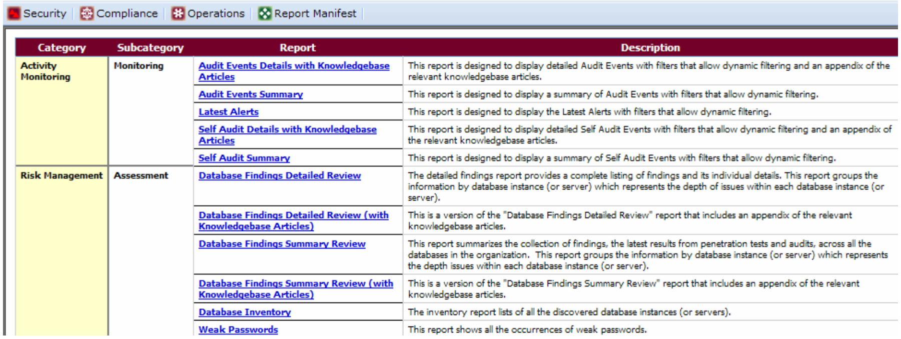
DbProtect Analytics Reports

This chapter consists of the following topics:

- *Navigating to the Reports*
- *Running and Viewing Reports*
- *Understanding the Reports.*

Navigating to the Reports

You can click the **Report Manifest** toolbar button to access DbProtect Analytics Reports. The **Report Manifest** page is shown below.



Category	Subcategory	Report	Description
Activity Monitoring	Monitoring	Audit Events Details with Knowledgebase Articles	This report is designed to display detailed Audit Events with filters that allow dynamic filtering and an appendix of the relevant knowledgebase articles.
		Audit Events Summary	This report is designed to display a summary of Audit Events with filters that allow dynamic filtering.
		Latest Alerts	This report is designed to display the Latest Alerts with filters that allow dynamic filtering.
		Self Audit Details with Knowledgebase Articles	This report is designed to display detailed Self Audit Events with filters that allow dynamic filtering and an appendix of the relevant knowledgebase articles.
		Self Audit Summary	This report is designed to display a summary of Self Audit Events with filters that allow dynamic filtering.
Risk Management	Assessment	Database Findings Detailed Review	The detailed findings report provides a complete listing of findings and its individual details. This report groups the information by database instance (or server) which represents the depth of issues within each database instance (or server).
		Database Findings Detailed Review (with Knowledgebase Articles)	This is a version of the "Database Findings Detailed Review" report that includes an appendix of the relevant knowledgebase articles.
		Database Findings Summary Review	This report summarizes the collection of findings, the latest results from penetration tests and audits, across all the databases in the organization. This report groups the information by database instance (or server) which represents the depth issues within each database instance (or server).
		Database Findings Summary Review (with Knowledgebase Articles)	This is a version of the "Database Findings Summary Review" report that includes an appendix of the relevant knowledgebase articles.
		Database Inventory	The inventory report lists of all the discovered database instances (or servers).
		Weak Passwords	This report shows all the occurrences of weak passwords.

FIGURE: **Report Manifest** page

Available DbProtect Analytics Reports are organized by category (e.g., **Risk Management**) and subcategory (e.g., **Assessment**), with a clickable link to generate each Report.

Running and Viewing Reports

This sections explains what you need to know about *Running a Report* and *Viewing a Report*.

RUNNING A REPORT

To run a DbProtect Analytics Report, click the Report description (e.g., **Database Findings Detailed Review**) on the **Report Manifest** page. The Report runs, and displays in a separate window.

VIEWING A REPORT

Each DbProtect Analytics Report contains a drop-down icon in the upper right portion of the Report window. When you click the drop-down icon, the Report viewing options menu displays (shown below).

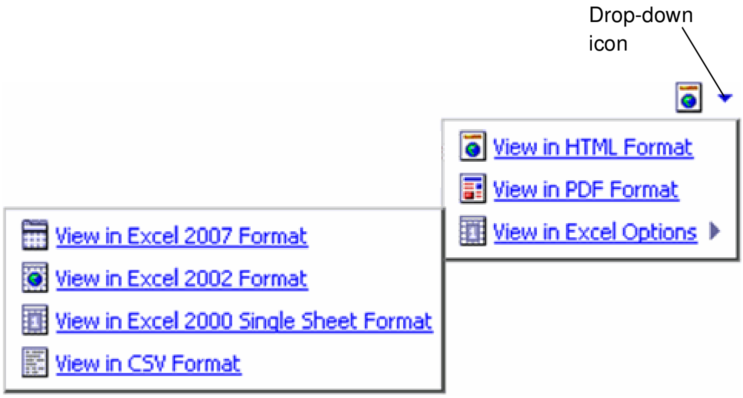


FIGURE: Report viewing options menu

You can click **View in HTML Format, View in PDF Format**, or **View in Excel Options** to view your Report in HTML, PDF, or Excel formats, respectively.

Understanding the Reports

This section provides a description of each DbProtect Analytics Report. It consists of the following topics:

- *DbProtect Analytics Reports At-a-Glance*
- *Which DbProtect Analytics Reports Include Oracle Audit Vault Data?*
- *Risk Management*
- *Standards and Compliance*
- *System Information.*

DBPROTECT ANALYTICS REPORTS AT-A-GLANCE

The following table lists each available DbProtect Analytics Report (organized by category and subcategory), and provides a link to the Report detail.

Category	Subcategory	Report
Activity Monitoring	*Activity Monitoring - Monitoring*	*Audit Events Details with Knowledgebase Articles Report*
		Audit Events Summary Report
		Latest Alerts Report
		Self Audit Details with Knowledgebase Articles Report
		Self Audit Summary Report

Category	Subcategory	Report
Risk Management	*Risk Management - Assessment*	*Database Findings Detailed Review Report*
		Database Findings Detailed Review Report (with Knowledgebase Articles)
		Database Findings Summary Review Report
		Database Findings Summary Review Report (with Knowledgebase Articles)
		Database Inventory Report
		Job Findings Detailed Review Report (with Knowledgebase Articles)
		Job Findings Summary Review Report
		Weak Passwords Report
	RIsk Management - Monitoring	*Failed Logins Review Report*
		Privileged Activity Report
		Threat Detailed Review Report
		Threat Detailed Review Report (with Knowledgebase Articles)
		Threat Summary Review Report
		Threat Summary Review Report (with Knowledgebase Articles)
		User Activity Report
	Risk Management - Policy Management	*Available Policies Report*
		Knowledgebase Detail Report
		Monitoring Configuration Report

Category	Subcategory	Report
Standards and Compliance	*Standards and Compliance - Assessment*	*Compliance Report Wizard*
		Health Insurance Portability and Accountability Act (HIPAA) - Vulnerability Assessment Report
		NIST 800-53 Report
		Payment Card Industry Data Security Standard (PCI DSS) - Vulnerability Assessment Report
		Sarbanes-Oxley (SOX) - Audit and Threat Management Report
	Standards and Compliance - Monitoring	*Payment Card Industry Data Security Standard (PCI DSS) - Audit and Threat Management Report*
		Sarbanes-Oxley (SOX) - Audit and Threat Management Report
System Information	*System Information - Diagnostics*	*Inactivity Alerts Report*

WHICH DBPROTECT ANALYTICS REPORTS INCLUDE ORACLE AUDIT VAULT DATA?

If you are using Oracle Audit Vault to audit your databases, then certain DbProtect Analytics Reports may include Oracle Audit Vault data. The specific DbProtect Analytics Reports that may include Oracle Audit Vault data are:

- *Failed Logins Review Report*
- *Privileged Activity Report*
- *Threat Detailed Review Report*
- *Threat Detailed Review Report (with Knowledgebase Articles)*
- *Sarbanes-Oxley (SOX) - Audit and Threat Management Report*
- *Payment Card Industry Data Security Standard (PCI DSS) - Audit and Threat Management Report.*

In order to include Oracle Audit Vault data in your DbProtect Analytics Reports, you must properly install Oracle Audit Vault and register Oracle Audit Vault within DbProtect. For more information, see *Minimum Requirements for Using Oracle Audit Vault as a DbProtect Data Source* in the *DbProtect User's Guide*.

Activity Monitoring

This topic explains the DbProtect Analytics **Risk Management** Reports, and its one current sub-category:

- *Activity Monitoring - Monitoring*

ACTIVITY MONITORING - MONITORING

Audit Events Details with Knowledgebase Articles Report

This report is designed to display detailed Audit Events with filters that allow dynamic filtering and an appendix of the relevant knowledgebase articles.

Audit Events Summary Report

This report is designed to display a summary of Audit Events with filters that allow dynamic filtering.

Latest Alerts Report

This report is designed to display the Latest Alerts with filters that allow dynamic filtering.

Self Audit Details with Knowledgebase Articles Report

This report is designed to display detailed Self Audit Events with filters that allow dynamic filtering and an appendix of the relevant knowledgebase articles.

Self Audit Summary Report

This report is designed to display a summary of Self Audit Events with filters that allow dynamic filtering.

Risk Management

This topic explains the DbProtect Analytics **Risk Management** Reports, organized in the following sub-categories:

- *Risk Management - Assessment*
- *RIsk Management - Monitoring*
- *Risk Management - Policy Management*.

RISK MANAGEMENT - ASSESSMENT

Database Findings Detailed Review Report

This Report provides a complete and detailed listing of the latest outside-in (Penetration) and inside-out (Audit) tests across all organizations. This Report groups the information by database instance providing deep visibility of issues within each database. The data and graph can be used to determine general trends, strengths and weaknesses of your database security.

Database Findings Detailed Review Report (with Knowledgebase Articles)

This Report provides a complete summary of the latest outside-in (Penetration) and inside-out (Audit) tests across all organizations. This Report groups the information by database instance providing deep visibility of issues within each database. The data and graph can be used to determine general trends, strengths and weaknesses of your database security. The last section of this Report includes an appendix of knowledgebase articles that correspond to the findings.

Database Findings Summary Review Report

This Report summarizes the collection of findings, the latest results from penetration tests and audits, across all the databases in the organization. This Report groups the information by database instance (or server) which represents the depth issues within each database instance (or server).

Database Findings Summary Review Report (with Knowledgebase Articles)

This Report provides a complete and detailed listing of the latest outside-in (Penetration) and inside-out (Audit) tests across all organizations. This Report groups the information by database instance providing deep visibility of issues within each database. The data and graph can be used to determine general trends, strengths and weaknesses of your database security. The last section of this Report includes an appendix of knowledgebase articles that correspond to the findings.

Database Inventory Report

This Report lists of all the discovered database instances (or servers). The network was inventoried by either an inventory import or by conducting a network sweep of IP addresses and investigating the responsive ports for the existence of applications using DbProtect AppDetective. This inventory information should be reviewed periodically to reconcile the systems against their business context. It is also important to evaluate the system versions and patch levels to ensure they are up to corporate standard.

Job Findings Detailed Review Report (with Knowledgebase Articles)

This Report provides a complete and detailed listing of the latest outside-in (penetration) and inside-out (audit) tests for a selected job in a given organization. You can use the data and graphic to determine general trends, strengths and weaknesses of your database security. The last section of this report includes an appendix of knowledgebase articles that correspond to the findings.

Job Findings Summary Review Report

This Report summarizes the collection of findings, the latest results from penetration tests and audits, across all the databases in the organization. It also summarizes the most recent information which represents the job execution initiated by administrator(s) of the organization.

Weak Passwords Report

This Report shows all the occurrences of weak passwords. Weak passwords are vulnerabilities that have the potential for exploitation. They are much sought-after by hackers and can put your entire organization at risk. Weak passwords are easily guessable by a human or a computer within a finite timeframe. The longer the lifespan of a password, the weaker it becomes. Best practices suggest that regular password modifications combined with strong passwords helps to thwart the weak password threat.

RISK MANAGEMENT - MONITORING

Failed Logins Review Report

This activity Report provides a comprehensive history of failed database connection attempts. This Report should be reviewed periodically to examine whether an unauthorized threat existed or to investigate past incidents. Excessive login failures, patterned login failures, failures with non-existing accounts and default accounts, are some indicators of possible break-in attempts and should be cause for concern.

Note: If you are using Oracle Audit Vault to audit your databases, and you registered Oracle Audit Vault within DbProtect, this report will include Oracle Audit Vault data. For more information, see *Working with Oracle Audit Vault as a DbProtect Data Source*.

Privileged Activity Report

This activity Report provides an audit trail of activity that is classified as privileged--schema modifications, authorization changes, and administrative actions. This represents the privileged activity performed according to the active policy during the time of the recorded events. Regular reviews of privileged activity help to reduce the propagation of bad behavior and support the ability to thwart ongoing malicious activity. This can also be used in incident investigation. The authorized privileged activity can generally be matched to some change control reference, if your organization actively uses one.

Note: If you are using Oracle Audit Vault to audit your databases, and you registered Oracle Audit Vault within DbProtect, this report will include Oracle Audit Vault data. For more information, see *Working with Oracle Audit Vault as a DbProtect Data Source*.

Threat Detailed Review Report

This threat Report provides a detailed view of all the security alerts that were generated across the organization. This is designed to provide the complete event details for the selected risk-events. Security Alerts are events that are classified with risk levels of **High**, **Medium**, and **Low**. These events should occur irregularly and be addressed in a timely manner. Any regularity of events should be questioned; it should become a candidate for policy change or process change.

Note: If you are using Oracle Audit Vault to audit your databases, and you registered Oracle Audit Vault within DbProtect, this report will include Oracle Audit Vault data. For more information, see *Working with Oracle Audit Vault as a DbProtect Data Source*.

Threat Detailed Review Report (with Knowledgebase Articles)

This threat Report provides a complete detailed view of all the security alerts that were generated across the organization. This depth of information can be used to investigate issues raised by the **Threat Summary Review** Report. Security Alerts are events that are classified with risk levels of **High**, **Medium**, and **Low**. These events should occur irregularly and be addressed in a timely manner. Any regularity of events should be questioned; it should become a candidate for policy change or process change. The last section of this Report includes an appendix of knowledgebase articles that correspond to the findings.

Note: If you are using Oracle Audit Vault to audit your databases, and you registered Oracle Audit Vault within DbProtect, this report will include Oracle Audit Vault data. For more information, see *Working with Oracle Audit Vault as a DbProtect Data Source*.

Threat Summary Review Report

This threat Report provides a summarized view of all the security alerts that were generated across the organization. This is designed to support high-level analysis of the risk-events that occurred within the environment. This summarized information can be used as a starting point for deeper investigation. Security Alerts are events that are classified with risk levels of **High**, **Medium**, and **Low**. These events should occur irregularly and be addressed in a timely manner. Any regularity of events should be questioned; it should become a candidate for policy change or process change.

Threat Summary Review Report (with Knowledgebase Articles)

This is a version of the **Threat Summary Review Report** that includes an appendix of the relevant knowledgebase articles.

User Activity Report

This activity Report provides an audit trail of user activity. This report provides activity details limited to a selection of users, or can provide full details on all user activity.

RISK MANAGEMENT - POLICY MANAGEMENT

Available Policies Report

This displays a listing of all policies that are available for use in the system. Policies are divided into three distinctive categories: 1) Penetration Tests; 2) Audits; and 3) Audit and Threat Management. The three Policy types are used to perform separate functions.

Knowledgebase Detail Report

This Report shows knowledgebase articles for a selection of database types.

Monitoring Configuration Report

This Report lists all of the database instances that have Audit and Threat Management turned on with their corresponding monitoring policy. The chart represents the distribution of active policies across all the monitored databases.

Standards and Compliance

This topic explains the DbProtect Analytics **Risk Management** Reports, organized in the following sub-categories:

- *Standards and Compliance - Assessment*
- *Standards and Compliance - Monitoring.*

STANDARDS AND COMPLIANCE - ASSESSMENT

Compliance Report Wizard

This is a Report that presents the results as it maps to your selected compliance policy. Use this wizard to generate details that meet the compliance standards described by your policies.

Health Insurance Portability and Accountability Act (HIPAA) - Vulnerability Assessment Report

This Report is an indicator of compliance with Health Insurance Portability and Accountability Act (HIPAA). This Report is based on the out-of-the-box policy that maps regulatory standards to the appropriate vulnerability checks. Use this Report as a gauge of compliance with regulatory compliance.

NIST 800-53 Report

This Report is an indicator of compliance with NIST 800-53. NIST 800-53 is the recommended guideline for security controls for a federal information system. This is applicable to all federal agencies and any government entity that follows the NIST standard. The NIST 800-53 guideline breaks down security controls into six categories: Access Control (AC), Audit and Accountability (AU), Identification and Authentication (IA), Configuration Management (CM), System and Communications Protection (SC), and System and Information Integrity (SI). This Report provides the results of vulnerability findings mapped to the six security control categories.

Payment Card Industry Data Security Standard (PCI DSS) - Vulnerability Assessment Report

This Report is an indicator of compliance with Payment Card Industry Data Security Standard (PCI DSS). This Report is based on the out-of-the-box policy that maps regulatory standards to the appropriate vulnerability checks. Use this Report as a gauge of compliance with regulatory compliance.

Note: If you are using Oracle Audit Vault to audit your databases, and you registered Oracle Audit Vault within DbProtect, this report will include Oracle Audit Vault data. For more information, see *Working with Oracle Audit Vault as a DbProtect Data Source.*

STANDARDS AND COMPLIANCE - MONITORING

Payment Card Industry Data Security Standard (PCI DSS) - Audit and Threat Management Report

This Report highlights database activity that pertains to Payment Card Industry Data Security Standard (PCI DSS) compliance. This Report is based on an out-of-the-box policy that maps regulatory standards to the appropriate Audit and Threat Management rules. Use this Report to summarize activity that may compromise compliance with this regulatory standard.

Sarbanes-Oxley (SOX) - Audit and Threat Management Report

This Report is an indicator of compliance with Sarbanes-Oxley (SOX). This Report is based on the out-of-the-box policy that maps regulatory standards to the appropriate vulnerability checks. Use this Report as a gauge of compliance with regulatory compliance.

Note: If you are using Oracle Audit Vault to audit your databases, and you registered Oracle Audit Vault within DbProtect, this report will include Oracle Audit Vault data. For more information, see *Working with Oracle Audit Vault as a DbProtect Data Source*.

System Information

This topic explains the DbProtect Analytics **System Information** Report (i.e., the *Inactivity Alerts Report*), which belongs to the sub-category *System Information - Diagnostics*.

SYSTEM INFORMATION - DIAGNOSTICS

Inactivity Alerts Report

Inactivity alerts are special diagnostic events that a Sensor sends when it does not detect any database activity for a pre-determined period of time. That period is configurable and should be evaluated for each environment to determine its appropriate value. Inactivity alerts can also be shut off. Inactivity at the database may or may not be considered normal behavior depending on its usage. Peak and Off-peak hours, weekend and holidays, business hours are all factors that contribute to normal occurrences of inactivity alerts. However, if the profile of the inactivity alerts change, then there is reasonable cause to investigate its shift. Under normal circumstances, you should be able associate shifts to an environmental change. Otherwise, this is an indicator that the monitoring system has been modified or is experiencing difficulty.

DbProtect Analytics Troubleshooting

This chapter consists of the following topics:

- *Resolving Problems Quickly*
- *Key Issues*
- *Troubleshooting Installation Errors*
- *Troubleshooting Runtime Errors*.

Resolving Problems Quickly

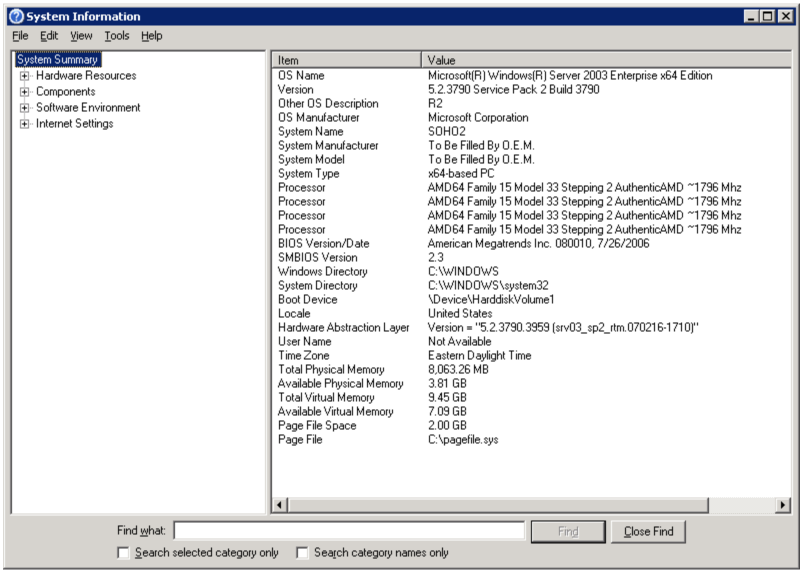
This section provides a list of items you should gather before you contact Application Security, Inc. Support (`support@appsecinc.com`). This information allows us to rapidly identify the source of a problem, and provide a quick resolution. Key information elements include:

- *Operating System Characteristics*
- *Log File to Troubleshoot Installation Problems*
- *Key Configuration and Log Files*.

OPERATING SYSTEM CHARACTERISTICS

It is beneficial to find out your hardware and software system characteristics in order to help determine if they are causing the issues you are experiencing. One easy way to obtain this information is to run the built-in system information utility from Microsoft.

Do the following:

<table>
<tr><th>Step</th><th>Action</th></tr>
<tr><td>1</td><td>Choose <b>Start</b> &gt; <b>Run</b> &gt; <b>msinfo32.exe</b>. A window similar to the one below displays.


<table>
<tr><th>Item</th><th>Value</th></tr>
<tr><td>OS Name</td><td>Microsoft(R) Windows(R) Server 2003 Enterprise x64 Edition</td></tr>
<tr><td>Version</td><td>5.2.3790 Service Pack 2 Build 3790</td></tr>
<tr><td>Other OS Description</td><td>R2</td></tr>
<tr><td>OS Manufacturer</td><td>Microsoft Corporation</td></tr>
<tr><td>System Name</td><td>SOHO2</td></tr>
<tr><td>System Manufacturer</td><td>To Be Filled By O.E.M.</td></tr>
<tr><td>System Model</td><td>To Be Filled By O.E.M.</td></tr>
<tr><td>System Type</td><td>x64-based PC</td></tr>
<tr><td>Processor</td><td>AMD64 Family 15 Model 33 Stepping 2 AuthenticAMD ~1796 Mhz</td></tr>
<tr><td>Processor</td><td>AMD64 Family 15 Model 33 Stepping 2 AuthenticAMD ~1796 Mhz</td></tr>
<tr><td>Processor</td><td>AMD64 Family 15 Model 33 Stepping 2 AuthenticAMD ~1796 Mhz</td></tr>
<tr><td>Processor</td><td>AMD64 Family 15 Model 33 Stepping 2 AuthenticAMD ~1796 Mhz</td></tr>
<tr><td>BIOS Version/Date</td><td>American Megatrends Inc. 080010, 7/26/2006</td></tr>
<tr><td>SMBIOS Version</td><td>2.3</td></tr>
<tr><td>Windows Directory</td><td>C:\WINDOWS</td></tr>
<tr><td>System Directory</td><td>C:\WINDOWS\system32</td></tr>
<tr><td>Boot Device</td><td>\Device\HarddiskVolume1</td></tr>
<tr><td>Locale</td><td>United States</td></tr>
<tr><td>Hardware Abstraction Layer</td><td>Version = "5.2.3790.3959 (srv03_sp2_rtm.070216-1710)"</td></tr>
<tr><td>User Name</td><td>Not Available</td></tr>
<tr><td>Time Zone</td><td>Eastern Daylight Time</td></tr>
<tr><td>Total Physical Memory</td><td>8,063.26 MB</td></tr>
<tr><td>Available Physical Memory</td><td>3.81 GB</td></tr>
<tr><td>Total Virtual Memory</td><td>9.45 GB</td></tr>
<tr><td>Available Virtual Memory</td><td>7.09 GB</td></tr>
<tr><td>Page File Space</td><td>2.00 GB</td></tr>
<tr><td>Page File</td><td>C:\pagefile.sys</td></tr>
</table>
FIGURE: <b>System Information</b> window
Key information elements here for Application Security, Inc. Support are:
• <b>Total / Available Physical Memory</b>
• <b>Total / Available Virtual Memory</b>
• <b>Page File Space</b>
• <b>OS Name</b>
• <b>Version</b>
• <b>Locale</b>.</td></tr>
</table>

LOG FILE TO TROUBLESHOOT INSTALLATION PROBLEMS

During normal installation of the DbProtect suite components, log files are generated and placed in a temporary directory. You can access this directory by entering `%temp%` in Windows Explorer. Application Security, Inc. Customer Support will ask you to send these files if you contact them.

Caution! Since this is a technical "dump" of your install process, sometimes there may be credential information recorded in this manually generated log file. Review the contents of this log to remove any sensitive credential information before sending it to any Application Security, Inc. Customer Support professionals.

KEY CONFIGURATION AND LOG FILES

Sometimes it may be necessary for Support personnel to investigate a problem in more detail. In order to help us in this process, it is beneficial to collect the following files/directories with key information.

```
<DbProtect Installation Root>/Reporting/media/c8/logs
```

```
<DbProtect Installation Root>/Reporting/media/c8/configuration/
cogstartup.xml
```

```
<DbProtect Installation Root>/GUI/logs
```

```
<DbProtect Installation Root>/GUI/tomcat/conf/wrapper.conf
```

```
<DbProtect Installation Root>/GUI/tomcat/conf/Catalina/localhost
```

```
<DbProtect Installation Root>/GUI/tomcat/logs
```

In addition to these, it is also useful to record how the DbProtect Console and Analytics services are run. To verify this, do the following:

- Choose **Start > Control Panel > Administrative Tools > Services**.
- Locate the services `DbProtect Console`, `DbProtect Analytics`, and `Cognos 8`.
- Right-click the service name and select **Properties** to display the **Properties** dialog box.
- Click the **Log On** tab.

Record the current selection for **Local System Account**, or the account specified under **This account**.

Key Issues

This section consists of the following topics:

- *Installation, Uninstallation, and Repair*
- *Credential Management*
- *Service Creation*
- *Reports*.

INSTALLATION, UNINSTALLATION, AND REPAIR

- To uninstall DbProtect Analytics via the Start Menu (recommended), choose: **Start > Program Files > AppSecInc > DbProtect > Uninstall Analytics**.
- When you uninstall DbProtect Analytics -- either from the Start Menu or the Control Panel -- you **must** manually address some intentional cleanup items. The following steps need to be completed in order to cleanly remove all artifacts from a DbProtect Analytics installation:

  -Remove the `DbPAnalytics` database (created at time of installation on the same database instance as the DbProtect Console Data Repository). You may do this from any of the Microsoft SQL Server tools (such as Microsoft SQL Management Studio or Query Analyzer). Do the following: 1.) Log in to the Microsoft SQL Server instance with appropriate privileges allowing you to drop databases. 2.) Locate the database `DbPAnalytics` in the Object Explorer. 3.) Right click the database `DbPAnalytics` and select **Delete**.

  -Remove any files and folders that remain in the `<DbProtect Console Root>/Reporting` folder. You may also remove the `Reporting` folder.
- Uninstall fails if any DbProtect Console browser windows are open. Ensure all DbProtect Console browser windows are closed prior to uninstalling.

CREDENTIAL MANAGEMENT

DbProtect Analytics allows for both SQL and Windows authentication modes. If you are using SQL authentication, there is currently no UI for credential management. Contact the Application Security, Inc. Support team to obtain a specific utility and instructions to affect this type of credential change.

SERVICE CREATION

The DbProtect Analytics installer prompts the user for service log on credentials. If a user is specified but not domain-qualified (such as domain\user). For local users, use the host name instead of the domain), the service credential setting is reverted to **Log On as Local System**. Open the **Services** dialog box (choose **Start > Control Panel > Administrative Tools > Services**) and set the appropriate account credentials from the Log On tab, after you complete the installation.

REPORTS

DbProtect Analytics includes a set of export options that allows you to save report data in a number of XLS/CSV formats. If you see a flash, but do not successfully export any content when you select one of these options, ensure the following:

- You do not have an active pop up blocker that is closing the window.

  OR

- Your browser's security settings allow the DbProtect Console site to open windows and download file content. You may need to add the DbProtect Console site to your list of trusted sites.

  OR

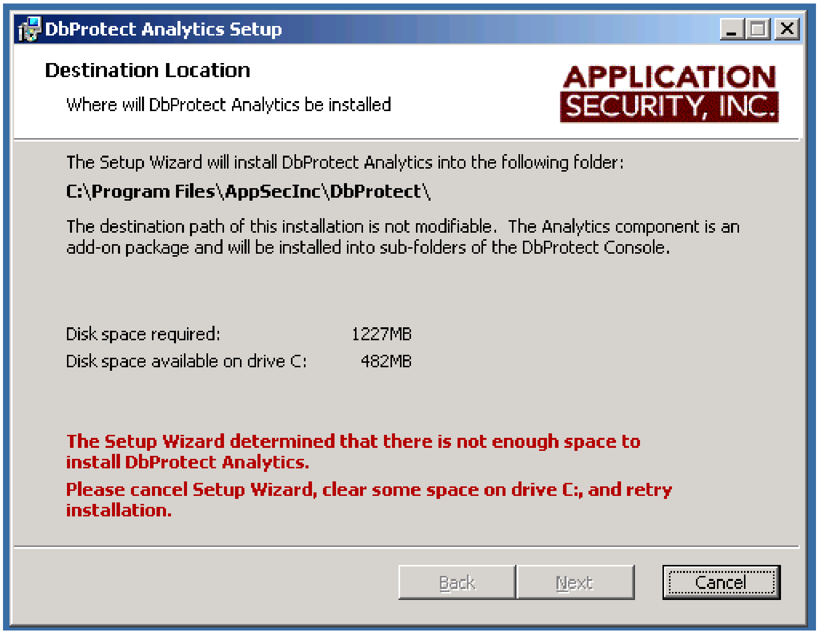
- In the case of generating an Excel spreadsheet (XLS) report, make sure you have enabled **Automatic prompting for file downloads** within Internet Explorer. To do so, choose: **Internet Options** > **Security Tab** > **Custom Level** > **Downloads** > **Automatic prompting for file downloads** > **Enable**.

Troubleshooting Installation Errors

This section explains how to troubleshoot common DbProtect Analytics **installation** errors. It consists of the following topics:

- *"The Setup Wizard determined that this is not enough space to install DbProtect Analytics"*
- *"Your machine has XXX MB of physical memory; at least YYY GB is required to install DbProtect Analytics"*
- *"Your machine has XXX MB of physical memory; at least YYY GB is recommended to install DbProtect Analytics"*
- *"This account does not have logon as service right or account privileges could not be obtained"*
- *"DbProtect Analytics Setup Wizard was interrupted"*
- *"DbProtect Analytics Setup Wizard ended prematurely"*.

"THE SETUP WIZARD DETERMINED THAT THIS IS NOT ENOUGH SPACE TO INSTALL DBPROTECT ANALYTICS"



DbProtect Analytics Setup
Destination Location
Where will DbProtect Analytics be installed
APPLICATION SECURITY, INC.

The Setup Wizard will install DbProtect Analytics into the following folder:

C:\Program Files\AppSecInc\DbProtect\

The destination path of this installation is not modifiable. The Analytics component is an add-on package and will be installed into sub-folders of the DbProtect Console.

```
Disk space required:              1227MB
Disk space available on drive C:   482MB
```

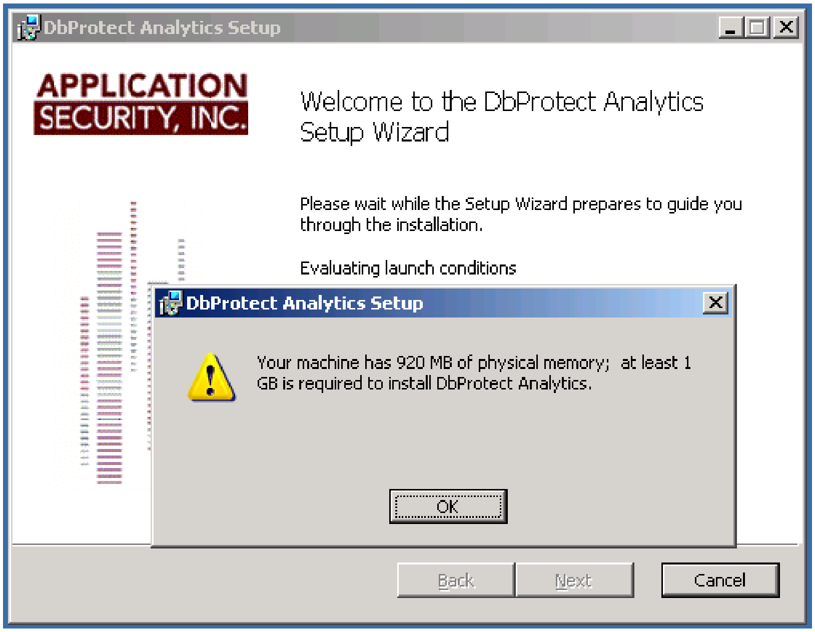
The Setup Wizard determined that there is not enough space to install DbProtect Analytics.

Please cancel Setup Wizard, clear some space on drive C:, and retry installation.

FIGURE: "The Setup Wizard determined that this is not enough space to install DbProtect Analytics" error message

DbProtect Analytics is installed as an add-on component to DbProtect Console, in the same drive location as the DbProtect Console. For more information, see the *DbProtect Installation Guide*.

"YOUR MACHINE HAS XXX MB OF PHYSICAL MEMORY; AT LEAST YYY GB IS REQUIRED TO INSTALL DBPROTECT ANALYTICS"


DbProtect Analytics Setup
APPLICATION SECURITY, INC.
Back
Next
Cancel
DbProtect Analytics Setup
OK

Welcome to the DbProtect Analytics Setup Wizard

Please wait while the Setup Wizard prepares to guide you through the installation.

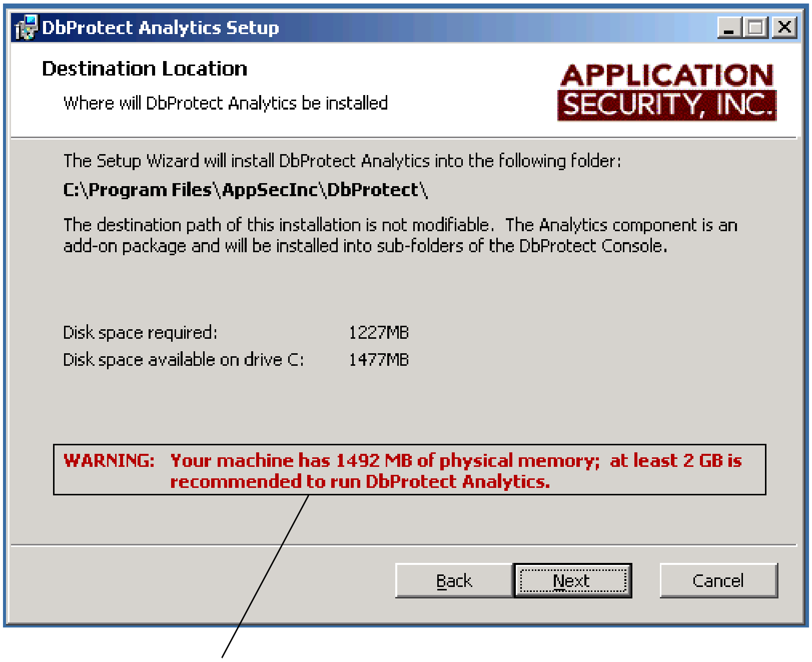
Evaluating launch conditions

Your machine has 920 MB of physical memory; at least 1 GB is required to install DbProtect Analytics.

FIGURE: "Your machine has XXX MB of physical memory; at least YYY GB is required to install DbProtect Analytics" error message

DbProtect Analytics enforces that at least 1 GB of RAM is present to complete the installation. This allows you to complete the installation process, but may yield poor performance except with very small data sets. Make sure you meet all the physical hardware requirements before you install. For more information, see the *DbProtect Installation Guide*.

"YOUR MACHINE HAS XXX MB OF PHYSICAL MEMORY; AT LEAST YYY GB IS RECOMMENDED TO INSTALL DBPROTECT ANALYTICS"



Destination Location

Where will DbProtect Analytics be installed

The Setup Wizard will install DbProtect Analytics into the following folder:

C:\Program Files\AppSecInc\DbProtect\

The destination path of this installation is not modifiable. The Analytics component is an add-on package and will be installed into sub-folders of the DbProtect Console.

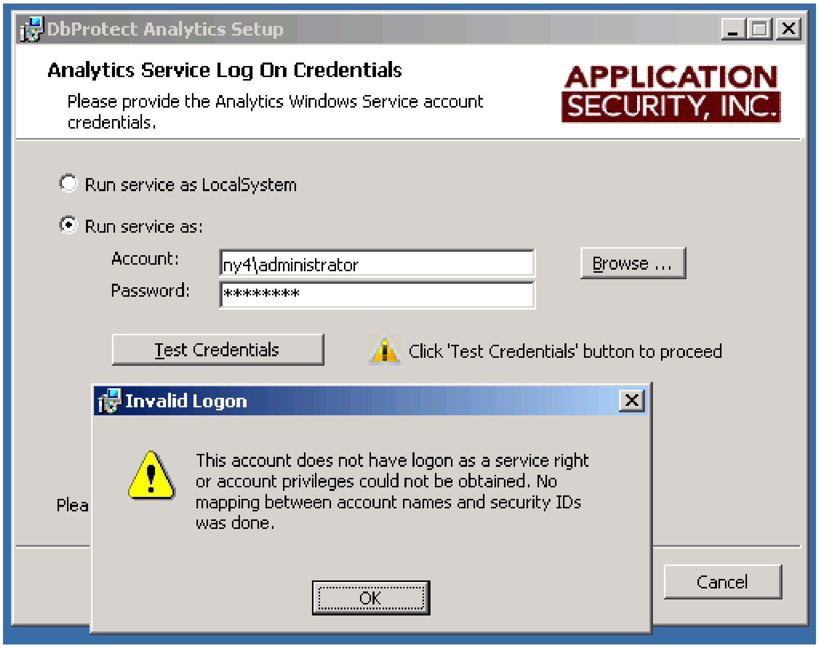
Disk space required:	1227MB
Disk space available on drive C:	1477MB

WARNING: Your machine has 1492 MB of physical memory; at least 2 GB is recommended to run DbProtect Analytics.

FIGURE: "Your machine has XXX MB of physical memory; at least YYY GB is recommended to install DbProtect Analytics" error message

There is enough memory to proceed with the installation; however, it is below the recommended hardware configuration. Please make sure you meet all the physical hardware requirements before you install. For more information, see the *DbProtect Installation Guide*.

"THIS ACCOUNT DOES NOT HAVE LOGON AS SERVICE RIGHT OR ACCOUNT PRIVILEGES COULD NOT BE OBTAINED”



Analytics Service Log On Credentials

Please provide the Analytics Windows Service account credentials.

○ Run service as LocalSystem

● Run service as:

Account: ny4\administrator

Password: *********

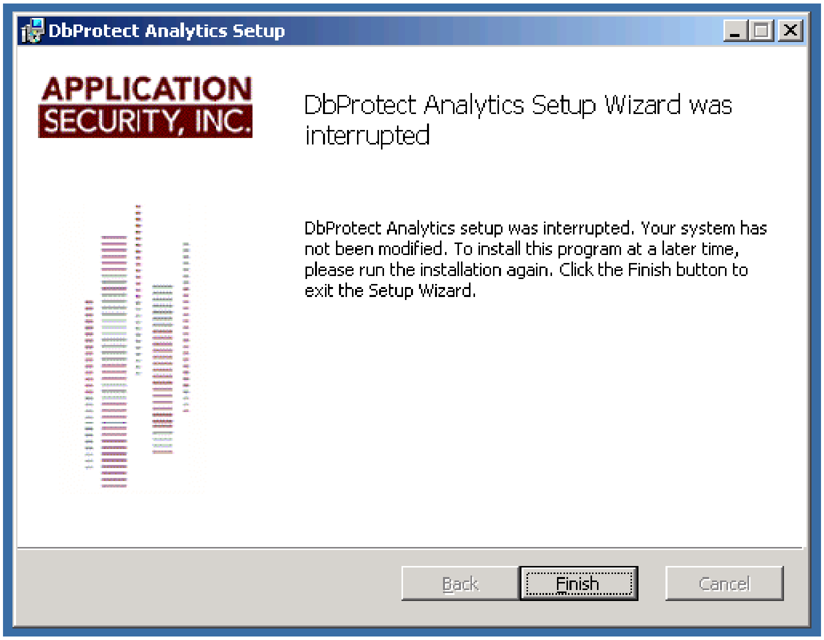
Click 'Test Credentials' button to proceed

This account does not have logon as a service right or account privileges could not be obtained. No mapping between account names and security IDs was done.

FIGURE: "This account does not have logon as service right or account privileges could not be obtained” error message

DbProtect Analytics runs as two services: `DbProtect Analytics` and `Cognos 8`. The credentials you enter into the installer for a runtime user are used to run this service. The account you are using to run the installer needs to have the necessary privileges to check for the **Log on as a service** rights. The specified runtime user needs to have these rights granted to them. Make sure you have the necessary privileges and accounts listed in *What You Will Need.*

"DBPROTECT ANALYTICS SETUP WIZARD WAS INTERRUPTED”



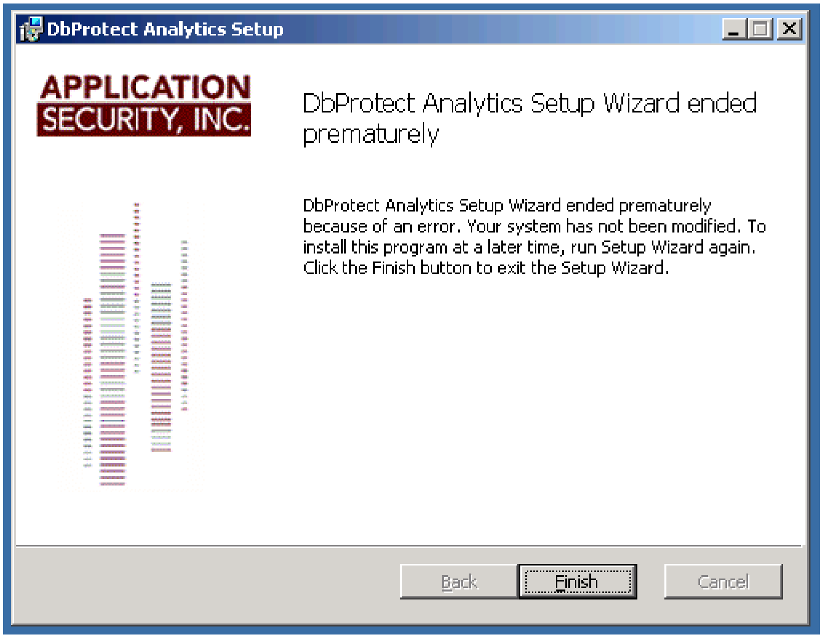
DbProtect Analytics Setup Wizard was interrupted

DbProtect Analytics setup was interrupted. Your system has not been modified. To install this program at a later time, please run the installation again. Click the Finish button to exit the Setup Wizard.

FIGURE: "DbProtect Analytics Setup Wizard was interrupted” error message

This screen confirms that you have aborted an in-progress DbProtect Analytics installation. If you received this unexpectedly, click the **Finish** button, then confirm the installation has exited by checking the **Task Manager**. Once the installer process has exited, you may restart the installation.

"DBPROTECT ANALYTICS SETUP WIZARD ENDED PREMATURELY"



DbProtect Analytics Setup Wizard ended prematurely

DbProtect Analytics Setup Wizard ended prematurely because of an error. Your system has not been modified. To install this program at a later time, run Setup Wizard again. Click the Finish button to exit the Setup Wizard.

FIGURE: "DbProtect Analytics Setup Wizard ended prematurely" error message

This screen confirms that the DbProtect Analytics installation has failed. There are many environmental factors that might lead to a failure. Typically, these failures are related to login rights (either for the database instance, or on the host), or to lack of hardware resources on the host. Please make sure you have the necessary privileges and accounts enumerated in the section *What You Will Need*.

Troubleshooting Runtime Errors

This section explains how to troubleshoot common DbProtect Analytics **runtime** errors. It consists of the following topics:

- *The Analytics & Reporting Tab is Disabled/Grayed Out*
- *The Message "CAM-AAA-1079 The 3rd party provider returned an unrecoverable exception" Displays When You Navigate to the Analytics tab, from DbProtect Console*
- *Upon Navigating to the Analytics Tab Within DbProtect Console, the Message "The Cognos gateway is unable to connect to the Cognos BI server" Displays*
- *The "Your report is running, please wait …" Page Displays for a Long Time*
- *The Message "RSV-XXX-XXXX The request 'asynchWait_Request' failed because the Conversation was already canceled" Appears in Place of a Report or Dashboard*
- *The Message "RSV-XXX-XXXX The absolute affinity request 'asynchWait_Request' failed, the requested session does not exist" Displays in Place of a Report or Dashboard*
- *Excel Spreadsheet Report Generation Fails With a DPR-ERR-2079 Firewall Security Rejection Error Message*

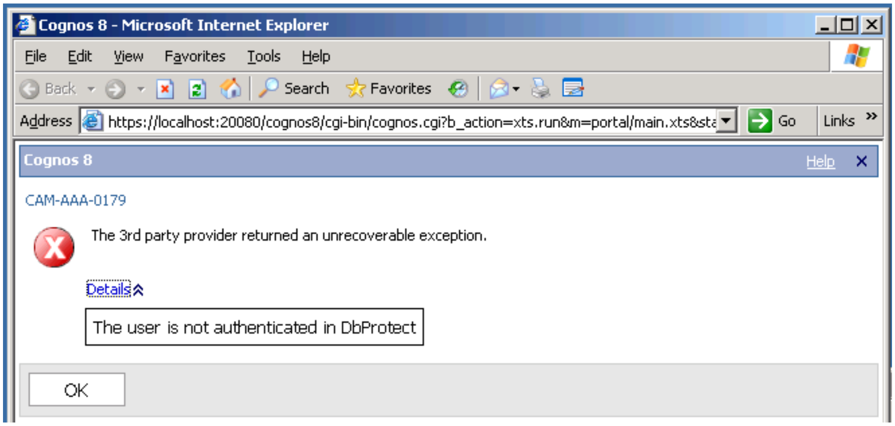
THE ANALYTICS & REPORTING TAB IS DISABLED/GRAYED OUT

The DbProtect Console connects to and identifes the `DbProtect Analytics` service during startup. If the DbProtect Console is unable to detect whether DbProtect Analytics was installed, the **Analytics & Reporting** tab in the DbProtect Console is disabled.

In some cases (especially when a server has less than the minimum hardware specifications, as explained in the *DbProtect Installation Guide*), the DbProtect Console might start up, without DbProtect Analytics starting.

Make sure DbProtect Analytics was installed successfully, and verify that both the `DbProtect Analytics` and `Cognos 8` services are up and running on your server. Then restart the `DbProtect Console` service.

THE MESSAGE “CAM-AAA-1079 THE 3RD PARTY PROVIDER RETURNED AN UNRECOVERABLE EXCEPTION” DISPLAYS WHEN YOU NAVIGATE TO THE ANALYTICS TAB, FROM DBPROTECT CONSOLE


Cognos 8 - Microsoft Internet Explorer

Address https://localhost:20080/cognos8/cgi-bin/cognos.cgi?b_action=xts.run&m=portal/main.xts&sta

Cognos 8

CAM-AAA-0179

The 3rd party provider returned an unrecoverable exception.

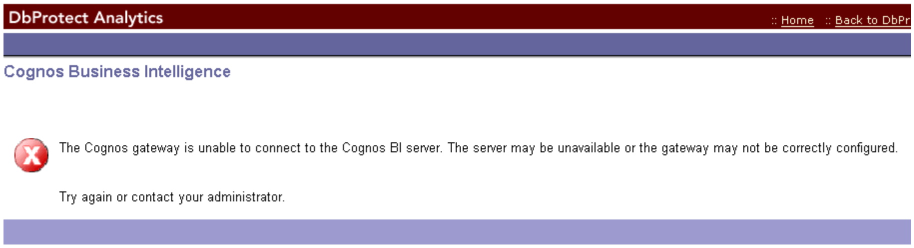
Details

The user is not authenticated in DbProtect

FIGURE: “CAM-AAA-1079 The 3rd party provider returned an unrecoverable exception” error message

This error typically confirms that you have tried to navigate to DbProtect Analytics without first authenticating to DbProtect Console. Since DbProtect Analytics is an add-on portal within DbProtect Console, only authenticated users are allowed to access the Analytics portal. Please identify a suitable user and authenticate to DbProtect Console as that user. Then select the **Analytics** tab to navigate to DbProtect Analytics. For more information, see *Navigating the DbProtect Analytics Portal*.

UPON NAVIGATING TO THE ANALYTICS TAB WITHIN DBPROTECT CONSOLE, THE MESSAGE “THE COGNOS GATEWAY IS UNABLE TO CONNECT TO THE COGNOS BI SERVER” DISPLAYS


DbProtect Analytics

Cognos Business Intelligence

The Cognos gateway is unable to connect to the Cognos BI server. The server may be unavailable or the gateway may not be correctly configured.

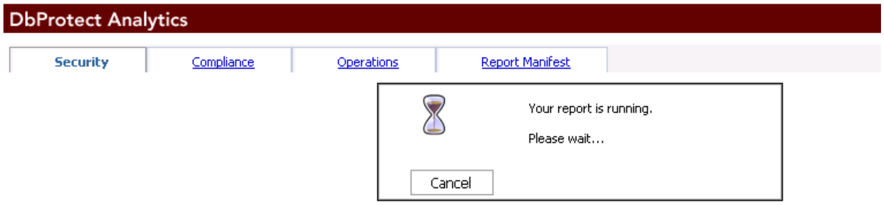
Try again or contact your administrator.

FIGURE: “The Cognos gateway is unable to connect to the Cognos BI server” error message

If the error message **"The Cognos gateway is unable to connect to the Cognos BI server"** displays, the server may be unavailable or the gateway may not be correctly configured. Try again or contact your administrator.

This error typically confirms that the DbProtect Analytics service (`Cognos 8`) is not running. This may be because it was not set to start up automatically, or the service user did not have the necessary rights. Start the service, exit, log back in to DbProtect Console, and navigate to DbProtect Analytics. If you need to validate the runtime user's privileges, see *What You Will Need*.

THE "YOUR REPORT IS RUNNING, PLEASE WAIT ..." PAGE DISPLAYS FOR A LONG TIME



Your report is running.

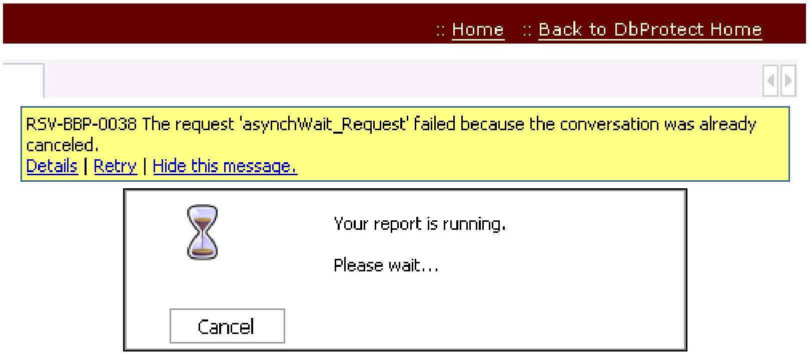
Please wait...

FIGURE: "Your report is running, please wait" page

This page displays when DbProtect Analytics is preparing a Report or computing a Dashboard.

If this message displays for a long time on your Reports and Dashboards, you should verify your hardware configuration; for more information, see the *DbProtect Installation Guide*.

THE MESSAGE "RSV-XXX-XXXX THE REQUEST 'ASYNCHWAIT_REQUEST' FAILED BECAUSE THE CONVERSATION WAS ALREADY CANCELED" APPEARS IN PLACE OF A REPORT OR DASHBOARD


:: Home :: Back to DbProtect Home
Details | Retry | Hide this message.
Cancel

RSV-BBP-0038 The request 'asynchWait_Request' failed because the conversation was already canceled.

Your report is running.

Please wait...

FIGURE: "RSV-XXX-XXXX The request 'asynchWait_Request' failed because the Conversation was already canceled" error message

This message often displays when the host running DbProtect Console and DbProtect Analytics is starved of resources, or the SQL Server database repository is slow or non-responsive.

If this is a sporadic problem, click on the **Retry** link. This re-issues the request and the element or page should repaint normally. If this is a regular problem, consider whether your hardware environment continues to be within the recommended parameters. If you are operating on large data sets, it is important you have enough processor and memory resources, both on the host running DbProtect Analytics as well as the host running SQL Server. You should verify your hardware configuration; for more information, see the *DbProtect Installation Guide*.

THE MESSAGE "RSV-XXX-XXXX THE ABSOLUTE AFFINITY REQUEST 'ASYNCHWAIT_REQUEST' FAILED, THE REQUESTED SESSION DOES NOT EXIST" DISPLAYS IN PLACE OF A REPORT OR DASHBOARD

This message displays when the browser's session with DbProtect Analytics has timed out. Your browser may have been idle for a long time, or you may have participated in navigation that caused the DbProtect Analytics session to be abandoned. Close the browser, or locate a valid DbProtect Console browser session, and navigate to DbProtect Analytics; for more information, see *Navigating the DbProtect Analytics Portal*.

EXCEL SPREADSHEET REPORT GENERATION FAILS WITH A DPR-ERR-2079 FIREWALL SECURITY REJECTION ERROR MESSAGE

This message displays if you are trying to generate an Excel spreadsheet (XLS) report, and you have **not** enabled **Automatic prompting for file downloads** within Internet Explorer.

To do so, choose: **Internet Options** > **Security Tab** > **Custom Level** > **Downloads** > **Automatic prompting for file downloads** > **Enable**.

Appendices

What you will find in this chapter:

Appendix A: Creating a User Credentials File

This appendix consists of the following topics:

- *What is a User Credentials File?*
- *Converting to the .xml file format from the legacy flat file format*
- *Current User Credentials File format (.xml file)*
- *Legacy User Credentials File format (flat file).*

What is a User Credentials File?

The **User Credentials File** includes the administration user's operating system user name, operating system password, system privileges, database username, and database password.

You **must** provide database and operation system authentication credentials in order to run an Audit Job. If you don't use a Credential Profile (see *Working with Credential Profiles and User Credential Files*), you can import a properly-formatted User Credentials File (explained below).

All users (except View Users) can **import** a User Credentials File from an `.xml` file. This file **must** be properly-formatted or the import will fail, and the credentials will remain unchanged.

Note: Super Admin users can also **export** a User Credentials File.

For more information on:

- importing a User Credentials File, see *Importing a User Credentials File*
- exporting a User Credentials File, see *Exporting a User Credentials File*.

Note: If you have multiple database instances installed on a single host, and you want to Audit them all, you can enter separate credentials for each instance. However, you can only enter a single (per AppDetective Scan Engine) global listener password in order to Discover Oracle database instances. For more information, see *Creating an Audit Job*.

Converting to the .xml file format from the legacy flat file format

Past versions of DbProtect AppDetective allowed you to import credentials from a flat file. **The flat file format is not recommended.**

The `.xml` format developed by Application Security, Inc. allows for better readability of the credentials file, as well as encryption of application passwords. The `.xml` format is now considered the standard.

However, Application Security, Inc. has **not** disabled the importing of the flat files for backwards compatibility. If you are currently using a flat file to import credentials, Application Security, Inc. **strongly encourages** you to switch to the new, standard, and vastly superior `.xml` format. To do so, you must first import the flat file, then export it. DbProtect AppDetective automatically converts the flat file to the proper format.

For more information on:

- importing a User Credentials File, see *Importing a User Credentials File*
- exporting a User Credentials File, see *Exporting a User Credentials File*.

Current User Credentials File format (.xml file)

The `.xml` file is simple to create manually, assuming you have basic `.xml` skills. Please refer to the schema provided below for this. If you have exported a file with encryption, and you want to add a new credential set, this can be done by editing the file. It is allowed for some of the credentials in the file to be encrypted, while others are not.

Caution! If you select the option to encrypt the application passwords, a number of elements and attributes will be added to support encryption (`encryption`, `encryptionUsed`, `verificationString`, `salt`, `encrypted`). It is highly discouraged that the user add, remove, or change values of these elements and attributes, as this will likely lead to an unreadable `.xml` file.

Importing does **not** change the file it imports, and exporting overwrites an existing file, so be careful that all the credentials you want to export were correctly imported into the current set of subnets and applications.

For example, it is possible to import a credential file with a dozen nodes, although you have only selected one node with the **Application Picker** tool. In this case, exporting the credentials with only one node selected will only export the credentials for the one application. If you overwrite the existing credential file, you will lose the other 11 credentials.

Below is the current User Credentials File format schema, written in RelaxNG format:

```
<?xml version="1.0"?>

<grammar xmlns="http://relaxng.org/ns/structure/1.0"
datatypeLibrary="http://www.w3.org/2001/XMLSchema-datatypes">


<start>
```

```
<element name="credentials">
<optional>
<ref name="encryptElement"/>
<!-- This element must only be used if any of the passwords in the file
are encrypted. -->
</optional>
<interleave>
<optional>
<ref name="networkElement"/>
</optional>
<zeroOrMore>
<ref name="subnetElement"/>
</zeroOrMore>
<zeroOrMore>
<ref name="hostElement"/>
</zeroOrMore>
<zeroOrMore>
<ref name="appElement"/>
</zeroOrMore>
</interleave>
</element>

</start>

<define name="encryptElement">
<element name="encryption">
<attribute name="encryptionUsed"><text/></attribute>
<attribute name="verificationString"><text/></attribute>
<ref name="saltAttribute"/>
</element>
</define>

<define name="networkElement">
<element name="network">
<zeroOrMore>
<ref name="pairElement"/>
</zeroOrMore>
</element>
</define>

<define name="subnetElement">
<element name="subnet">
<ref name="ipAttribute"/>
<zeroOrMore>
<ref name="pairElement"/>
</zeroOrMore>
</element>
```

```
</define>

<define name="hostElement">
<element name="host">
<choice>
<ref name="ipAttribute"/>
<ref name="hostnameAttribute"/>
</choice>
<zeroOrMore>
<ref name="pairElement"/>
</zeroOrMore>
</element>
</define>

<define name="appElement">
<element name="app">
<choice>
<ref name="ipAttribute"/>
<ref name="hostnameAttribute"/>
</choice>
<ref name="portAttribute"/>
<attribute name="instance"><text/></attribute>
<ref name="pairElement"/>
</element>
</define>


<define name="pairElement">
<element name="pair">
<interleave>
<optional>
<ref name="osElement"/>
</optional>
<ref name="dbElement"/>
</interleave>
</element>
</define>


<define name="osElement">
<choice>
<element name="windows">
<interleave>
<ref name="credentialSet"/>
<optional>
<element name="usescanenginecred"><data type="boolean"/></element>
</optional>
```

```
</interleave>
</element>
<element name="unix">
<interleave>
<ref name="credentialSet"/>
<ref name="protocolElement"/>
<ref name="portElement"/>
<optional>
<element name="useoscredfordb"><data type="boolean"/></element>
</optional>
</interleave>
</element>
</choice>
</define>


<define name="dbElement">
<choice>
<element name="mssql">
<interleave>
<ref name="credentialSet"/>
<element name="windowsauth"><data type="boolean"/></element>
</interleave>
</element>
<element name="oracle">
<interleave>
<ref name="credentialSet"/>
<element name="privilege">
    <choice>
    <value>sysdba</value>
    <value>normal</value>
    <value>sysoper</value>
    </choice>
</element>
</interleave>
</element>
<element name="otherdb">
<attribute name="application">
<choice>
<value>Microsoft SQL Server</value>
    <value>Oracle Database</value>
    <value>Sybase Adaptive Server Enterprise</value>
    <value>IBM DB2 Universal Database</value>
    <value>MySQL</value>
    <value>HTTP Web Server</value>
    <value>Lotus Domino</value>
    <value>Lotus Application Server</value>
    <value>Oracle All Components</value>
    <value>Microsoft Exchange Server</value>
    <value>IBM WebSphere Application Server</value>
    <value>IBM DB2 For Mainframe</value>
    <value>Bea WebLogic</value>
    <value>Bea Webservices</value>
    </choice>
</attribute>
<ref name="credentialSet"/>
</element>
</choice>
</define>


<define name="credentialSet">
<interleave>
<element name="username">
<text/>
</element>
<element name="password">
<optional>
<!-- if the encrypted attribute has a value of true, the password is assumed to be encrypted -->
<attribute name="encrypted"><data type="boolean"/></attribute>
<ref name="saltAttribute"/>
</optional>
<text/>
</element>
</interleave>
</define>


<define name="protocolElement">
<element name="protocol">
<choice>
<value>ssh</value>
<value>telnet</value>
</choice>
</element>
</define>

<define name="portElement">
<element name="port">
<data type="integer">
<param name="minInclusive">0</param>
<param name="maxInclusive">65535</param>
</data>
```

```
</element>
</define>

<define name="portAttribute">
<attribute name="port">
<data type="integer">
<param name="minInclusive">0</param>
<param name="maxInclusive">65535</param>
</data>
</attribute>
</define>

<define name="ipAttribute">
<attribute name="ip">
<data type="string">
<param name="maxLength">15</param>
</data>
</attribute>
</define>

<define name="hostnameAttribute">
<attribute name="hostname">
<text/>
</attribute>
</define>

<define name="saltAttribute">
<attribute name="salt"><text/></attribute>
</define>

</grammar>
```

Legacy User Credentials File format (flat file)

The legacy, flat file User Credentials File format is:

```
ipaddress,port,"database instance name","dbuser","dbpwd” [,
sysprivileges, “osusrname” , “ospwd] “
```

where: `[]` indicates **optional** parameters.

EXAMPLES:

Oracle:

```
192.168.1.73,1521,"ORCL","sys","admin123",normal,"oracle","admin123"
```

```
10.9.0.34,1521,"ORCL","sys","admin123",sysdba
```

DB2:

```
192.168.1.106,50000,"db2inst1:SAMPLE","admin","admin123", normal,
"alamo", "alamo123"
```

```
192.168.1.106,50000,"db2inst1:SAMPLE","admin","admin123", normal
```

SQL Server:

```
192.168.1.18,1433,"MSSQLSERVER","sa","admin123",normal, “alamo”,
“alamo123”
```

```
192.168.1.18,1433,"MSSQLSERVER","sa","admin123",normal
```

Sybase:

```
192.168.1.233,5000,"sbse_sql","sys","admin123
```

Appendix B: Monitoring Oracle Databases in an Oracle Fail Safe Environment: Sensor and Cluster Configuration Steps

This appendix explains how to configure a host-based Sensor for Oracle (on Windows) in an Oracle Fail Safe environment. It also explains how to configure your Oracle Fail Safe cluster, once you have properly configured your Sensor.

In this appendix:

- *About Oracle Fail Safe*
- *Oracle Fail Safe vs. Oracle RAC*
- *Sensor configuration steps (Oracle Fail Safe)*
- *Cluster configuration steps (Oracle Fail Safe).*

About Oracle Fail Safe

Oracle Fail Safe, a type of Oracle cluster, is a core feature included with every Oracle 11g, Oracle 10g and Oracle9i license for Microsoft Windows 2000 and Microsoft Windows 2003. Oracle Fail Safe is integrated with Microsoft Cluster Server to allow you to configure and verify Microsoft Windows clusters and to automatically fail over Oracle databases and applications.

Oracle Fail Safe is essentially a Microsoft Clustering Services (MSCS) plug-in. In an MSCS architecture, two systems share the same disk, which only one system controls at a time. In the event of a failure (determined by the heartbeat mechanism), the standby system replaces the instance currently running the Oracle instance (and controlling the storage).

Oracle Fail Safe vs. Oracle RAC

Oracle Fail Safe differs in several ways from Oracle Real Application Cluster (RAC); for more information on installing and configuring a host-based Sensor for Oracle (on Windows) to monitor Oracle databases on a RAC, see *Appendix C: Installing and Configuring a Host-Based Sensor for Oracle to Monitor Oracle Databases on an Oracle RAC*.

Oracle Fail Safe is generally considered easier to implement and administer than RAC. Most organizations that run applications on Microsoft Windows have already implemented MSCS and are familiar with it. In addition, Oracle Fail Safe is a core feature of Oracle9i and Oracle10g for Windows, so you won't need additional licenses.

Another key difference: unlike Oracle RAC (which can run in a Microsoft Windows or on a *nix-based platform), Oracle Fail Safe runs on Microsoft Windows only. Thus, this appendix is only relevant if you are configuring a host-based Sensor for Oracle (on Windows); for more information, see *Configuring a host-based Sensor to monitor Oracle SIDs and services and deploying the configuration information (when Sensor is installed on Windows)*.

Sensor configuration steps (Oracle Fail Safe)

To monitor Oracle databases in an Oracle Fail Safe environment, first complete the following host-based **Sensor** for Oracle (on Windows) **configuration** steps:

1. **Install** your host-based **Sensor** for Oracle (on Windows); for more information, see *Host-based Sensor for Oracle (on Windows) - installation steps* in the *DbProtect Installation Guide*.
2. **Register** your host-based **Sensor** for Oracle (on Windows); for more information, see *Registering a Sensor*.
3. **Configure and deploy** your host-based **Sensor** for Oracle (on Windows). Pay special attention to:
   - **Step 5** of *Configuring a host-based Sensor to monitor Oracle SIDs and services and deploying the configuration information (when Sensor is installed on Windows)*, where you **must** select a network adapter that is associated with a real IP address (where the network traffic can sniff packets). Make sure this is **not** the cluster heartbeat card, because cluster heartbeat cards do not detect network traffic.
   - **Step 10** of *Configuring a host-based Sensor to monitor Oracle SIDs and services and deploying the configuration information (when Sensor is installed on Windows)*, where you must configure your network adapter for the cluster's virtual IP address. If this is not already populated in the **IP Address:** field, then you must enter it manually.
4. Complete the remaining **configuration** steps described in *Configuring a host-based Sensor to monitor Oracle SIDs and services and deploying the configuration information (when Sensor is installed on Windows)*, and **deploy** the configured instance to your host-based **Sensor** for Oracle (on Windows).
5. Next, configure your Oracle Fail Safe cluster; for more information, see *Cluster configuration steps (Oracle Fail Safe)*.

Cluster configuration steps (Oracle Fail Safe)

Once you have configured your host-based Sensor for Oracle (on Windows) to monitor Oracle databases in an Oracle Fail Safe environment (as explained in *Sensor configuration steps (Oracle Fail Safe)*), you must next complete the following **cluster configuration** steps:

1. In your cluster, make the other node the active node either by initiating a failover or by moving the cluster resources over to that node.
2. From the new active node, access your shared drive via Windows Explorer.
3. On the shared drive, go to the directory where your host-based Sensor for Oracle (on Windows) is installed and navigate to the `<installation directory>\sensor\conf\overrides` directory.
4. Open the file `networkAdapter_sensor_override.xsl` in any text editor such as Notepad.
5. In a separate text editor window, open the file `sensor.xml`, which is located in the `<installation directory>\sensor\conf\` directory.
6. In the `sensor.xml` file, locate the line that begins: `<networkAdapter name=`. **Copy everything on that line** between the double quotes (but **not** the double quotes themselves).
7. Go to the text editor window where the `networkAdapter_sensor_override.xsl` file is open and locate the following section:

```
<!-- This is node 1 -->
        <xsl:element name="networkAdapter">
          <!-- Insert network adapter in between xsl attribute tags -->
<xsl:attribute name="name">INSERT_NETWORK_ADAPTER_HERE</xsl:attribute>
```

8. Paste the information you copied in Step 6 **from** the `sensor.xml` file **to** the location in Step 7. Specifically, you must paste the information you copied in Step 6 between the tags `<xsl:attribute name="name">` and `</xsl:attribute>` so it replaces the string reading: `INSERT_NETWORK_ADAPTER_HERE`. The string `INSERT_NETWORK_ADAPTER_HERE` should no longer be visible once you paste the actual network adapter information for node 1 from the `sensor.xml` file into this location.
9. Open a command prompt window in the Sensor's `<installation directory>\sensor\bin\` directory on the shared drive.
10. From the command prompt window, run the utility: `list_net_adapter.exe`
11. The `list_net_adapter.exe` utility outputs the list of network adapters it detects on cluster node. Note which network adapter corresponds to the real IP address for that node (i.e., **not** the cluster heartbeat network adapter).

12. Copy the network adapter information.

13. Paste the network adapter information into the area of the networkAdapter_sensor_override.xsl file reserved for the other node of your Oracle Fail Safe cluster. It should be just below the location from Step 8. It looks something like this:

```
<!-- This is node 2 -->
        <xsl:element name="networkAdapter">
           <!-- Insert network adapter in between xsl attribute tags -->
            <xsl:attribute name="name">INSERT_NETWORK_ADAPTER_HERE</
xsl:attribute>
```

Again, paste the network adapter information between the tags `<xsl:attribute name="name">` and `</xsl:attribute>`, replacing the string that reads: INSERT_NETWORK_ADAPTER_HERE. The string INSERT_NETWORK_ADAPTER_HERE should no longer be visible once the actual network adapter information for node 2 from the list_net_adapter.exe utility is pasted in this location.

14. Save the changes made to networkAdapter_sensor_override.xsl, then close the file.

15. Rename the networkAdapter_sensor_override.xsl file so the words networkAdapter_ are removed. The new file name should be named: sensor_override.xsl

16. Copy the sensor_override.xsl file from the <installation directory>\sensor\conf\overrides directory to the <installation directory>\sensor\conf\ directory (one level up).

17. Restart the DbProtect Sensor service. You can do this in either of two ways:

- Stop then start the DbProtect Sensor service from the Windows Service Control Manager on the cluster's active node.
- Bring the **DbProtect AppRadar Sensor Cluster** resource offline, then bring it online again in the Cluster Administrator on either cluster node.

Once the host-based Sensor for Oracle (on Windows) restarts, a new file displays in your Sensor installation's <installation directory>\sensor\conf\ directory. The new file is named: sensor_transformed.xml. This new file contains two occurrences of the <networkAdapter> XML element, which the Sensor uses to monitor your Oracle Fail Safe cluster.

Appendix C: Installing and Configuring a Host-Based Sensor for Oracle to Monitor Oracle Databases on an Oracle RAC

Oracle Real Application Clusters (RAC) allows multiple computers to run Oracle relational database management system (RDBMS) software simultaneously while accessing a single database, thus providing a clustered database. In a non-RAC Oracle database, by contrast, a single instance accesses a single database.

In order to configure a host-based Sensor to monitor databases on an Oracle RAC, you must do the following:

1. Install a host-based Sensor for Oracle on each node in your Oracle RAC. For more information, see *Appendix B: Configuring a Host-Based Sensor for Oracle to Monitor Oracle Databases on an Oracle RAC* in the *DbProtect Installation Guide*.
2. Next, in the DbProtect Console, you must **register** each host-based Sensor for Oracle you installed. If you installed your host-based Sensor for Oracle on:
   - Windows, see *Configuring a host-based Sensor to monitor Oracle SIDs and services and deploying the configuration information (when Sensor is installed on Windows)*
   - any supported *nix operating system (i.e., Solaris, AIX, HP-UX, or Red Hat Enterprise Linux), see *Configuring a host-based Sensor to monitor Oracle SIDs and services and deploying the configuration information (when Sensor is installed on a *nix-based operating system)*.
3. In the DbProtect Console, configure an instance for each host-based Sensor for Oracle you registered in Step 2. Make sure your **Instance Alias** is:
   - unique for each registered host-based Sensor for Oracle
   - is easily identifiable for the database you are monitoring
   - easily identifies the node where the Sensor is installed (e.g., **Oracle RAC Node 1**, **Oracle RAC Node 2**, etc.).

If you installed your host-based Sensor for Oracle on:

- Windows, see *Configuring a host-based Sensor to monitor Oracle SIDs and services and deploying the configuration information (when Sensor is installed on Windows)*
- any supported *nix operating system (i.e., Solaris, AIX, HP-UX, or Red Hat Enterprise Linux), see *Configuring a host-based Sensor to monitor Oracle SIDs and services and deploying the configuration information (when Sensor is installed on a *nix-based operating system).*

4. When configuring each instance, also ensure you deploy the exact same Policy for each host-based Sensor for Oracle (otherwise, you may get inconsistent results for the Alerts you are expecting to see).

Again, if you installed your host-based Sensor for Oracle on:

- Windows, see *Configuring a host-based Sensor to monitor Oracle SIDs and services and deploying the configuration information (when Sensor is installed on Windows)*
- any supported *nix operating system (i.e., Solaris, AIX, HP-UX, or Red Hat Enterprise Linux), see *Configuring a host-based Sensor to monitor Oracle SIDs and services and deploying the configuration information (when Sensor is installed on a *nix-based operating system).*

Appendix D: Oracle Critical Patch Update Detection

This appendix explains the different methods DbProtect AppDetective uses to detect if the Oracle Critical Patch Update (CPU) has been applied to your Oracle database.

This appendix consists of the following topics:

- *Java method*
- *OS method*
- *Legacy patch detection*
- *Patches_History.txt Method for Oracle CPU Collection on OpenVMS*
- *REGISTRY&HISTORY Table Method*.

Java method

The **Java method** is new functionality added to DbProtect AppDetective 3.0.2 and greater. This new method uses existing Java configured on the target database server to collect the OPatch data. DbProtect AppDetective requires Java Virtual Machine (JVM) on the target database server, as well as the following two privileges, in order to use the method correctly:

- `JAVASYSPRIV`
- `CREATE PROCEDURE`

You can run the commands below to grant these privileges:

- `grant JAVASYSPRIV to <username>`
- `grant CREATE PROCEDURE to <username>`

Caution! **Java XML** is required to use the Java method. Some custom scripts used to install JVM may not include Java XML (`initxml.sql` and `xmlja.sql` scripts).

By default, DbProtect AppDetective uses the OS (operating system) method to detect if the Oracle CPU has been applied to your Oracle database; for more information, see *OS method*. The Java method uses Oracle Java stored procedures to connect to the operating system, and then reviews the OPatch files to detect which CPUs have been installed.

Note: Using the Java method creates the following database objects: a Java source and function. DbProtect AppDetective deletes these objects as soon as DbProtect AppDetective completes the Audit. If an error occurs during the Audit, it is probably because the operating system user lacks the aforementioned permissions.

In addition, you can only use the Java method on versions of Oracle 9iR2 and above, where CPUs have been applied to the database using OPatch.

For more information on enabling use of the Java method, see *Configuring the properties of a Scan Engine*.

OS method

By default, DbProtect AppDetective uses the **OS** (Operating System) **method** to detect if the Oracle CPU has been applied to your Oracle database. This method requires you to supply OS credentials, in addition to a valid database account.

The OS method uses:

- telnet or SSH to connect to the operating system, then reviews the OPatch files to detect which CPUs have been installed
- Windows Administrative shares, such as `C$` and `D$`, to connect to the operating system for the Windows platforms.

Note: The OS Method only applies to version of Oracle 9iR2 and above, where CPUs have been applied to the database using OPatch.

If you encounter an error when running an Audit, verify the following:

- You have supplied the proper user name and password.
- The operating system user has the proper `ORACLE_HOME` set.
- The operating system user has permission to access `ORACLE_HOME`.

For more information on enabling use of the OS method, see *Configuring the properties of a Scan Engine*.

Legacy patch detection

For versions of Oracle 8i and 9iR1, DbProtect AppDetective performs its own method of examining whether the CPU is applied on the target database. This method, **legacy patch detection**, also requires for you to supply OS credentials, in addition to having a valid database account.

Legacy patch detection uses telnet or SSH to connect to the operating system and then reviews various attributes such as files dates and sizes to tell what patches have been installed.

If you encounter an error when running an Audit, verify the following:

- You have supplied the proper user name and password.
- The operating system user has the proper `ORACLE_HOME` set.

The operating system user has permission to access `ORACLE_HOME`.

Patches_History.txt Method for Oracle CPU Collection on OpenVMS

Oracle CPU checks on OpenVMS work the same way as they do on other platforms. DbProtect AppDetective includes a feature that looks up a local copy of the CPU history file. This is called `comps.xml` on most platforms, but on **OpenVMS** the file is called `patches_history.txt`.

The `patches_history.txt` file is located under the `PATCHES` subdirectory of `ORACLE_HOME` on the target OpenVMS server. The `patches_history.txt` contains information about installed and de-installed patches.

DbProtect AppDetective uses an existing copy instead of collecting files remotely. After the CPU check finishes, DbProtect AppDetective renames the local file (with a `.bak` extension) so it won't be used next time.

CPU DATA COLLECTION

When DbProtect AppDetective executes the CPU check against an OpenVMS server, you can select one of two **CPU data collection methods**:

- **Java method.** The Oracle database account requires the same privileges as required for the Java method on other platforms. For more information, see *Java method.*
- **OS method.** As opposed to other platform, on OpenVMS the OS account **must** have *at least* one of the following:

  -`ORACLE_HOME` logical defined

  -actual `oratab` file in home directory

  -listener banner containing `PRMFILE` string.

  DbProtect AppDetective uses this information to extract the `ORACLE_HOME` path.

USING A LOCAL FILE FOR AN ORACLE CPU CHECK ON AN OPENVMS SERVER

If you cannot Telnet/SSH to a remote OpenVMS server, you can use a **local file** for to perform your Oracle CPU check.

To do so, you must place a copy of the `patches_history.txt` file under the DbProtect AppDetective installation directory -- specifically, under the `\mirror\<IP>\<PORT>\<SID>\PATCHES` directory. For example, if the address of your OpenVMS server is `192.168.1.1`, and there is Oracle database on port 1521 with the SID `sales`, then the path is: `\mirror\192.168.1.1\1521\sales\PATCHES` (under the AppDetectivePro installation directory).

If the `\mirror\192.168.1.1\1521\sales\PATCHES\patches_history.txt` exists, then DbProtect AppDetective parses this file, and uses *it* (instead of performing a Telnet/SSH to the remote OpenVMS server). When DbProtect AppDetective completes the Audit, it changes the file name by appending `.bak`, to avoid confusion in the future.

REGISTRY&HISTORY Table Method

For CPUs dated January 2009 and later, DbProtect AppDetective supports the `REGISTRY$HISTORY` CPU detection method. This method checks information in the `SYS.REGISTRY$HISTORY` table to determine whether a CPU was applied.

This method only requires `'SELECT on SYS.REGISTRY$HISTORY'` rights. This method does **not** require OS or JAVA credentials, but is considered less accurate in certain cases.

Appendix E: Importing Session Data with the DbProtect Import Utility

This appendix consists of the following topics:

- *What is the DbProtect Import Utility?*
- *What is Session data?*
- *Session data import prerequisites, minimum system requirements, and considerations*
- *What data does the DbProtect Import Utility import (and not import)?*
- *Using the DbProtect Import Utility*
- *Troubleshooting a corrupted source database with the pre_import_cleanups.sql script*.

What is the DbProtect Import Utility?

The **DbProtect Import Utility** is a standalone utility that allows you to import critical security (Session) data *from* a database source *to* a destination DbProtect database.

For the source database, you can select:

- an exported AppDetectivePro Session (`.adb`) file; for more information, see *Importing Session Data from an AppDetectivePro Session file*
- the AppDetectivePro back-end Microsoft SQL Server database or the DbProtect back-end Microsoft SQL Server database; for more information, see *Importing Session data from an AppDetectivePro or DbProtect Microsoft SQL Server database*.

What is Session data?

A **Session** is a logical grouping of target databases and the Penetration Tests/Audits run against them. It also contains all the vulnerabilities and other information obtained by running Penetration Tests and Audits.

When an AppDetectivePro user creates a Session, AppDetectivePro automatically performs a Discovery of target databases on the user's networks. The AppDetectivePro user may then run Penetration Tests and Audits against these Discovered target databases. Consequently, when you migrate AppDetectivePro Session data to DbProtect, you are migrating all Discovery, Penetration Test, Audit, vulnerability, and associated Policy information within the Session.

You can also **export** Polices from AppDetectivePro, then **import** the exported Policies into DbProtect AppDetective, using AppDetectivePro (installed automatically when you install DbProtect). For more information, see *Importing a Policy* and *Exporting a Policy*, respectively.

For more information on AppDetective Pro and Sessions, see the *AppDetective User's Guide*.

Session data import prerequisites, minimum system requirements, and considerations

A few important **Session data import prerequisites, minimum system requirements, and considerations** follow:

- If you want to import Session data from an exported AppDetectivePro file, **your version of AppDetectivePro must be version 5.4.3 or greater**. If your version of AppDetectivePro is older than 5.4.3, you must:

  -upgrade your version of AppDetectivePro to the most current version (at least a version greater than 5.4.3)

  -import your old, pre-version 5.4.3 AppDetectivePro Session file (`.adb`) into your upgraded (i.e., greater than 5.4.3) version of AppDetectivePro

  -export your upgraded AppDetectivePro Session file (`.adb`) file

  -go to *Importing Session Data from an AppDetectivePro Session file*.
- If your **database source** is an AppDetectivePro or DbProtect back-end database, the versions must be **AppDetective Pro 5.4.3 or greater**, or **DbProtect 2007.1 or greater**, respectively.
- The version of your **destination DbProtect database** must be DbProtect 2009.1 or greater.
- Before using the **DbProtect Import Utility**, make sure you have valid database credential information available for both your **source** database and **target** database.
- Your source database and destination database **cannot be the same database**.
- The **DbProtect Import Utility** requires Service Pack 2 (SP2) for Microsoft SQL Server 2000, or SP1 for Microsoft SQL Server 2005/2008, on both your source and destination databases.

What data does the DbProtect Import Utility import (and not import)?

What you will find in this help topic:

- *What data does the DbProtect Import Utility import?*
- *What data does the DbProtect Import Utility not import?*

WHAT DATA DOES THE DBPROTECT IMPORT UTILITY IMPORT?

The **DbProtect Import Utility imports** the following content from the selected Session/ Organization on the source file/database into the target Organizations:

- **Customer-created checks and their content.** The **DbProtect Import Utility** imports customer-created checks into the target DbProtect database. Re-importing does **not** generate duplicate checks.
- **Customer-created Policies and their content.** The **DbProtect Import Utility** imports all customer-created Policies. Re-importing does **not** generate duplicate Policies.
- **Target databases with IP addresses that match the target Organizations' IP ranges.** The **DbProtect Import Utility** migrates all target databases in the selected Session/Organization of the source file/database to the relevant Organization, if the IP address of the source Session/Organization falls within the IP ranges of the target Organization.

  Example: If the source Session file contains 100 target databases (in which 80 of them have a `192.168.1.*` IP address), and you select a target Organization with an IP range of `192.168.1.1 – 192.168.1.255`, then the **DbProtect Import Utility** imports 80 target databases, and filters out the remaining 20.

- **All tests (Penetration Tests and Audits) associated with the qualified target database.** Since any given target database can run multiple tests, the **DbProtect Import Utility** also imports tests associated with qualified target databases. In order to be "qualified", the target database's IP address must fall into the target Organization's IP range as described above. In addition, the **DbProtect Import Utility** implements an internal mechanism that filters out "unqualified" tests; for more information, see *What data does the DbProtect Import Utility not import?*

  If a target database already exists, the **DbProtect Import Utility** merges the tests into the same target database, **unless** the tests themselves already exist. If you want to distinguish the tests, check the combination of `scanid`, `ipaddress`, `port`, `name`, and `endtime`.

  Example: The **DbProtect Import Utility** detects that the target database described by `1, 192.168.1.234 1433 'MSSQLSERVER'` already exists. **Five tests** have been run before. The new incoming import request contains **10 new tests** for the same target database. As a result, the **DbProtect Import Utility** merges the tests. Subsequently, the target DbProtect database will now contain **15 tests** for this target database.
- **All test results associated with the qualified tests.** The **DbProtect Import Utility** imports test results, which may include vulnerabilities, users found, and a check status associated with each test. In order to be "qualified", the target database's IP address must fall into the target Organization's IP range, as described above.
- **Job histories will be created for the tests.** After an import is complete, the **DbProtect Import Utility** creates Job histories for each Organization in the target DbProtect database. The **DbProtect Import Utility** creates Jobs based on how many different Policies are used in the tests. For example, for the target Organization `root`, assume 100 Penetration Tests have been imported. Among these 100 tests, five different Policies were used. As a result, the **DbProtect Import Utility** creates five unique Job histories. You can verify these job histories by checking the **Job History** panel on the DbProtect Console; for more information, see *Filtering Job history*.

WHAT DATA DOES THE DBPROTECT IMPORT UTILITY NOT IMPORT?

The **DbProtect Import Utility** does **not** import the following content from the source database into the target Organizations:

- **Organizations, users, templates, jobs, job histories, reports from the source DbProtect database.** If the source database is a DbProtect database, it only imports all the customized checks, customized Policies, and qualified target databases. Tests, test results, users, templates, Jobs, and reports are **not** imported.
- **"Unqualified" tests (Penetration Tests and Audits).** In order to maintain the data integrity, the following tests/audits are filtered out:

  -Tests which are not finished. You can identify these by checking the Status on the Jobs panel of the DbProtect Console; for more information, see *Viewing Job details*.

  -Tests which the IP range is outside the range of the target Organizations.

  -Tests which use obsolete Policies. If a test uses Policy which no longer exists in the source DbProtect database, the **DbProtect Import Utility** skips this test (and all of its results).

Using the DbProtect Import Utility

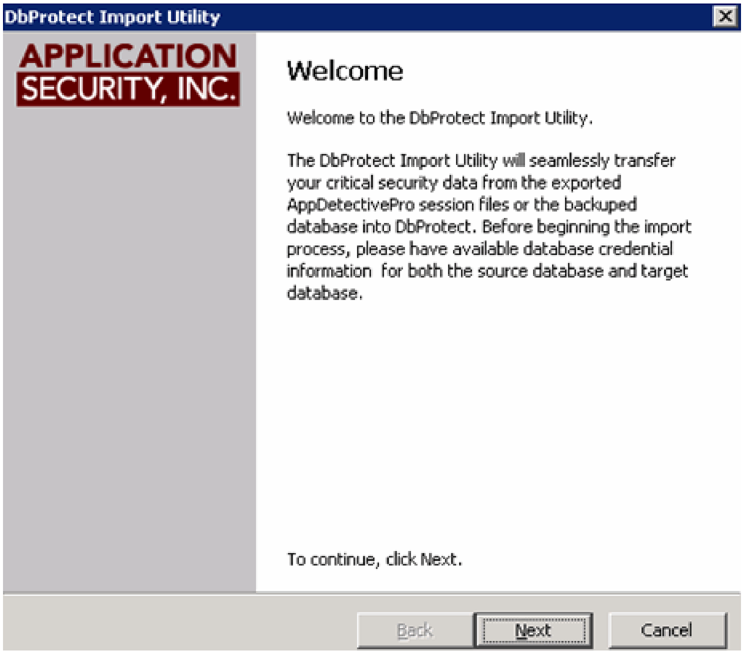
What you will find in this help topic:

- *Launching the DbProtect Import Utility*
- *Importing Session Data from an AppDetectivePro Session file*
- *Importing Session data from an AppDetectivePro or DbProtect Microsoft SQL Server database.*

LAUNCHING THE DBPROTECT IMPORT UTILITY

To launch the DbProtect Import Utility:

1. Choose **Start > Programs > AppSecInc > DbProtect > DbProtect Import Utility** to display the **Welcome** page of the **DbProtect Import Utility**.



Welcome

Welcome to the DbProtect Import Utility.

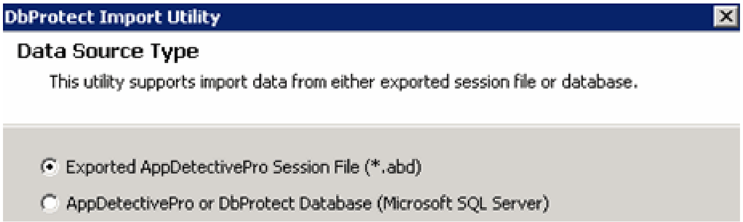
The DbProtect Import Utility will seamlessly transfer your critical security data from the exported AppDetectivePro session files or the backuped database into DbProtect. Before beginning the import process, please have available database credential information for both the source database and target database.

To continue, click Next.

FIGURE: **Welcome** page of the **DbProtect Import Utility**

2. Click the **Next** button.

The **Data Source Type** page of the **DbProtect Import Utility** displays.



DbProtect Import Utility

Data Source Type

This utility supports import data from either exported session file or database.

● Exported AppDetectivePro Session File (*.abd)

○ AppDetectivePro or DbProtect Database (Microsoft SQL Server)

FIGURE: **Data Source Type** page of the **DbProtect Import Utility**

The **Data Source Type** page of the **DbProtect Import Utility** allows you to select your database source. If you select:

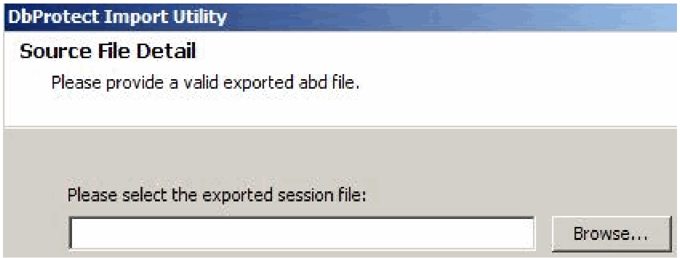
- **Exported AppDetectivePro Session File (*adb)** to import Session data from an exported AppDetectivePro Session, then go to *Importing Session Data from an AppDetectivePro Session file*
- **AppDetectivePro or DbProtect Database (Microsoft SQL Server)** to import Session data from an AppDetectivePro or DbProtect Microsoft SQL Server database, then go to *Importing Session data from an AppDetectivePro or DbProtect Microsoft SQL Server database*.

IMPORTING SESSION DATA FROM AN APPDETECTIVEPRO SESSION FILE

To import Session data from an exported AppDetectivePro Session (`.adb`) file:

1. As explained in ***Launching the DbProtect Import Utility***, the **Data Source Type** page of the **DbProtect Import Utility** allows you to select a database source for importing critical Session data.

If you selected **Exported AppDetectivePro Session File (*adb)** in Step 2 of *Launching the DbProtect Import Utility* to import Session data from an exported AppDetectivePro Session (`.adb`) file, then the **Source File Detail** page displays.



DbProtect Import Utility

Source File Detail

Please provide a valid exported abd file.

Please select the exported session file:

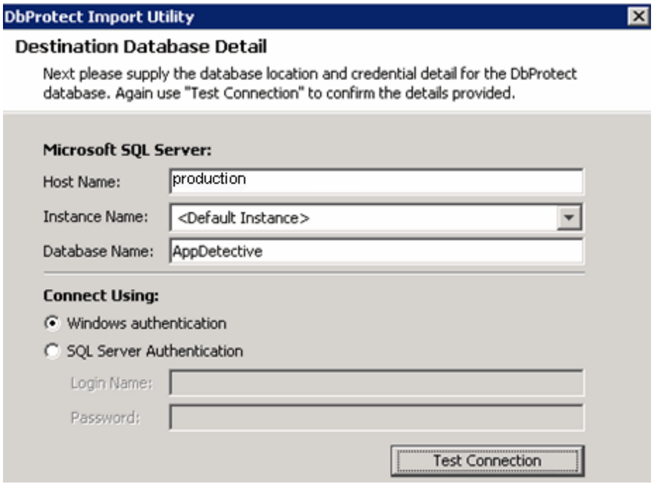
FIGURE: **Source File Detail** page of the **DbProtect Import Utility**

- You can manually enter the path and name of the AppDetectivePro Session (.adb) file, or click the **Browse** button to search for the .adb file on your computer or network.

Caution! If a pop-up informs you that your destination database is corrupted, you **must** run the pre_import_cleanups.sql script; for more information, see ***Troubleshooting a corrupted source database with the pre_import_cleanups.sql script*** at the end of this appendix.

- Click the **Next** button to display the **Destination Database Detail** page of the **DbProtect Import Utility**.

2. The **Destination Database Detail** page of the **DbProtect Import Utility** is shown below.



DbProtect Import Utility

Destination Database Detail

Next please supply the database location and credential detail for the DbProtect database. Again use "Test Connection" to confirm the details provided.

Microsoft SQL Server:

Host Name: production

Instance Name: <Default Instance>

Database Name: AppDetective

Connect Using:

● Windows authentication

○ SQL Server Authentication

Login Name:

Password:

FIGURE: **Destination Database Detail** page of the **DbProtect Import Utility**

Do the following:

- In the **Microsoft SQL Server:** portion of the **Destination Database Detail** page:

  -enter the **Host Name:** of your destination DbProtect database server, or a valid IP address

  -manually enter (or use the **Instance Name:** drop-down to select) a specific DbProtect database server (**<Default Instance>** is selected by default), or enter the instance name manually.

- In the **Connect Using:** portion of the **Destination Database Detail** page, select whether you want to connect to your destination database instance using:

  -**Windows Authentication** using the current logged-on Windows user's privileges.

Note: This user **must** be a Microsoft SQL Server user on the destination machine.

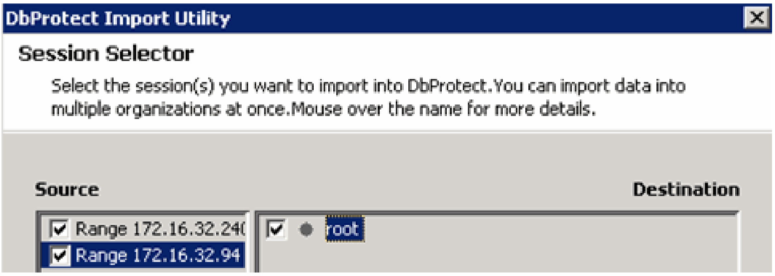
  -**SQL Authentication** (make sure SQL Authentication is enabled).

Note: If you're not sure which authentication type to select, see your database administrator.

If you choose **SQL Authentication**, then you must also enter the database user **Login Name:** and **Password:**

- Click the **Test Connection** button to test your connection to your destination database. The **DbProtect Import Utility** attempts to connect to your destination database. If the connection succeeds, the **Next** button is illuminated.

3. Click the **Next** button to display the **Session Selector** page of the **DbProtect Import Utility**.



Select the session(s) you want to import into DbProtect.You can import data into multiple organizations at once.Mouse over the name for more details.

☑ Range 172.16.32.24(

☑ Range 172.16.32.94

☑ ● root

FIGURE: **Session Selector** page of the **DbProtect Import Utility**

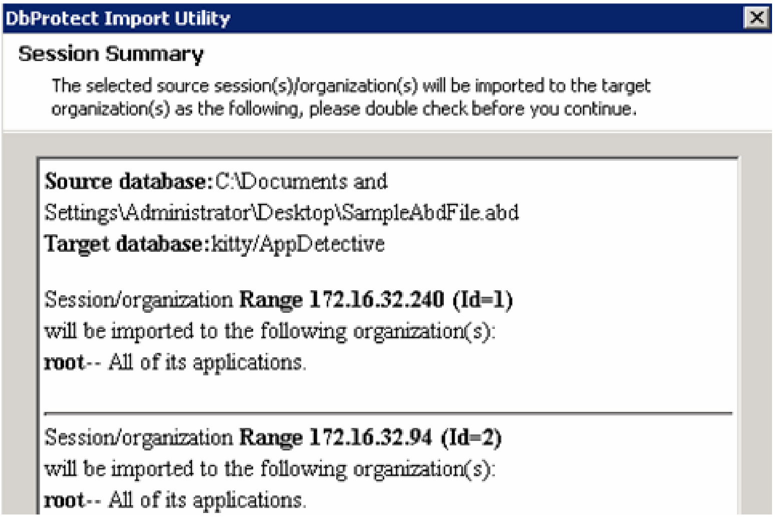
Select the Sessions you want to import from your selected AppDetectivePro Session (`.adb`) file (in the **Source** panel) into your DbProtect database (in the **Destination** panel).

Note: The **DbProtect Import Utility** imports all data (with source IP addresses that match the destination IP ranges) from your selected source Sessions into every Organization you selected in the **Destination** panel.

Example: Assume you are importing a Session with target databases in the IP range `192.168.1.1` - `192.168.1.255`, and the IP range `172.16.1.1 – 172.16.1.255`. Your `root` target Organization, however, only includes the IP range `192.168.1.1` - `192.168.1.255`. As a result, the **DbProtect Import Utility** imports all target databases in the IP range `192.168.1.1 - 192.168.1.255`, but ignores the `172.16.1.*` data. If you want to import `172.16.1.*` target database data, you must modify the IP range of your destination Organization; for more information, see *Editing an Organization*.

Hint: If you mouse over any Organization or Session name (in either the Source or Destination panels of the **Session Selector** page), then the **DbProtect Import Utility** displays the Session names and IP ranges for all Discovered target databases. This feature allows you to logically compare your source Sessions and destination Organizations.

4. Click the **Next** button to display the **Session Summary** page of the **DbProtect Import Utility**.



Session Summary

The selected source session(s)/organization(s) will be imported to the target organization(s) as the following, please double check before you continue.

Source database:C:\Documents and Settings\Administrator\Desktop\SampleAbdFile.abd
Target database:kitty/AppDetective

Session/organization **Range 172.16.32.240 (Id=1)**
will be imported to the following organization(s):
root-- All of its applications.

Session/organization **Range 172.16.32.94 (Id=2)**
will be imported to the following organization(s):
root-- All of its applications.

FIGURE: **Session Summary** page of the **DbProtect Import Utility**

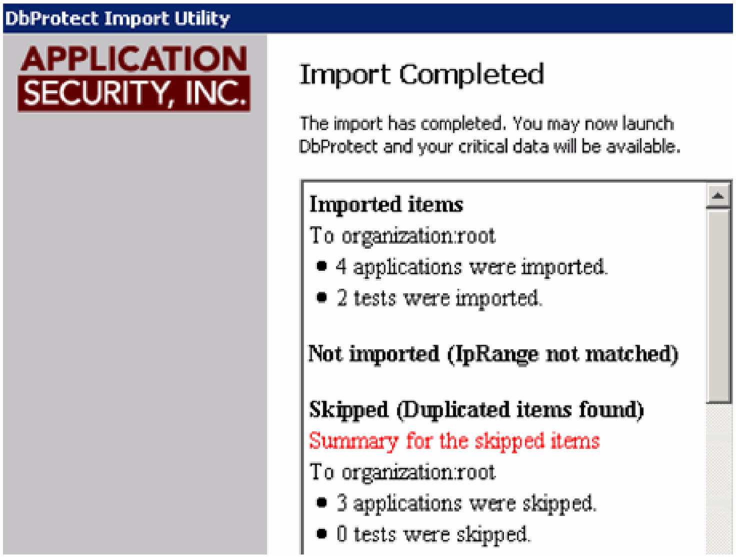
The **Session Summary** page of the **DbProtect Import Utility** displays a summary of which Sessions the utility is ready to import into your destination DbProtect database.

5. Click the **Next** button to import your Session data.

Note: For more information on what data the **DbProtect Import Utility** does (and does **not**) import, see *What data does the DbProtect Import Utility import (and not import)?*

When the import process completes, the **Import Completed** page of the **DbProtect Import Utility** displays.

Hint: You can copy/paste the import summary data and save it to a file for future reference.



Import Completed

The import has completed. You may now launch DbProtect and your critical data will be available.

Imported items
To organization:root
- 4 applications were imported.
- 2 tests were imported.

Not imported (IpRange not matched)

Skipped (Duplicated items found)
Summary for the skipped items
To organization:root
- 3 applications were skipped.
- 0 tests were skipped.

FIGURE: **Import Completed** page of the **DbProtect Import Utility**

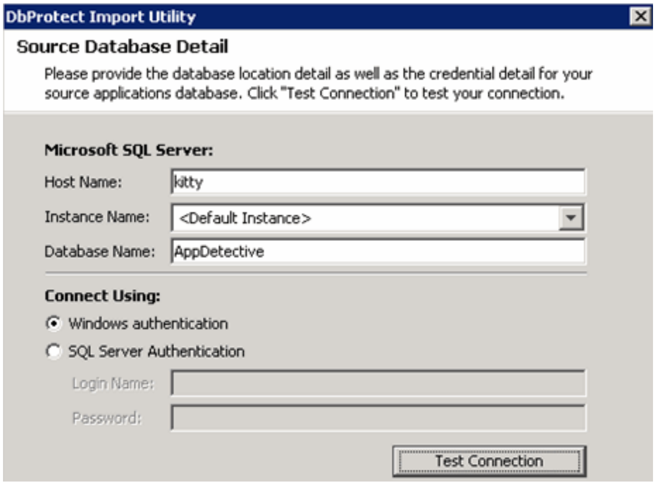
You may now launch DbProtect AppDetective. Your imported Session data is available; for more information, see *Vulnerability Management*.

IMPORTING SESSION DATA FROM AN APPDETECTIVEPRO OR DBPROTECT MICROSOFT SQL SERVER DATABASE

To import Session data from an AppDetectivePro or DbProtect Microsoft SQL Server database:

1. As explained in ***Launching the DbProtect Import Utility***, the **Data Source Type** page of the **DbProtect Import Utility** allows you to select a database source for importing critical Session data.

If you selected **AppDetectivePro or DbProtect Database (Microsoft SQL Server)** in Step 2 of *Launching the DbProtect Import Utility* to import Session data from the AppDetectivePro or DbProtect back-end database, then the **Source File Detail** page displays.



Source Database Detail

Please provide the database location detail as well as the credential detail for your source applications database. Click "Test Connection" to test your connection.

Microsoft SQL Server:

Host Name: kitty

Instance Name: <Default Instance>

Database Name: AppDetective

Connect Using:

● Windows authentication

○ SQL Server Authentication

Login Name:

Password:

FIGURE: **Source Database Detail** page of the **DbProtect Import Utility**

The **Source Database Detail** page of the **DbProtect Import Utility** allows you to specify the location of your source AppDetectivePro or DbProtect back-end database.

2. Do the following:

- In the **Microsoft SQL Server:** portion of the **Source Database Detail** page:

  -Enter the **Host Name:** of your AppDetectivePro or DbProtect back-end database

  -Manually enter (or use the **Instance Name:** drop-down to select) a specific AppDetectivePro or DbProtect back-end database (**<Default Instance>** is selected by default), or enter the instance name manually

  -Enter the **Database Name:**. The default source database name is `AppDetective`. However, if you backed-up your source database under a different name, manually enter the database name in this field.

- In the **Connect Using:** portion of the **Source Database Detail** page, select whether you want to connect to your destination database instance using:

  -**Windows Authentication** using the current logged-on Windows user's privileges.

Note: This user **must** be a Microsoft SQL Server user on the destination machine.

  -**SQL Authentication** (make sure SQL Authentication is enabled).

Note: If you're not sure which authentication type to select, see your database administrator.

If you choose **SQL Authentication**, then you must also enter the database user **Login Name:** and **Password:**

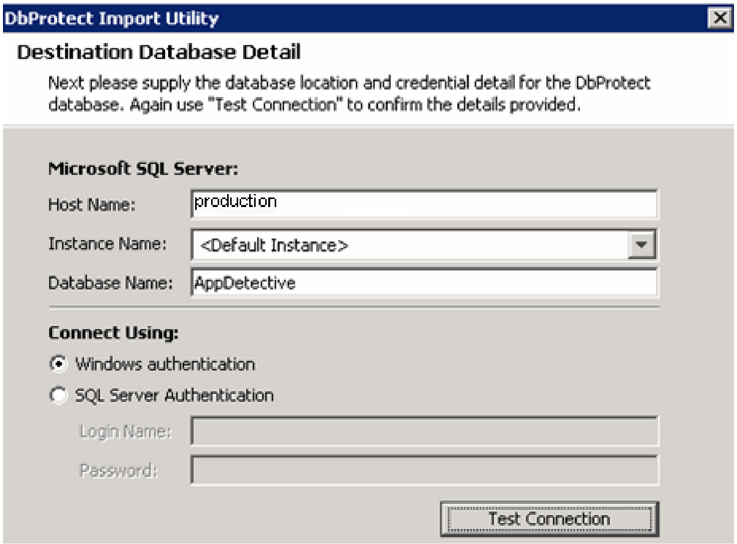
Note: If you do not know the SQL Authentication user name and password, see your database administrator.

- Click the **Test Connection** button to test your connection to the source database. The **DbProtect Import Utility** attempts to connect to your source database.

Caution! If a pop-up informs you that your destination database is corrupted, you **must** run the `pre_import_cleanups.sql` script; for more information, see ***Troubleshooting a corrupted source database with the pre_import_cleanups.sql script***.

If the connection succeeds, the **Next** button is illuminated.

3. Click the **Next** button to display the **Destination Database Detail** page of the **DbProtect Import Utility**.



DbProtect Import Utility

Destination Database Detail

Next please supply the database location and credential detail for the DbProtect database. Again use "Test Connection" to confirm the details provided.

Microsoft SQL Server:

Host Name: production

Instance Name: <Default Instance>

Database Name: AppDetective

Connect Using:

● Windows authentication

○ SQL Server Authentication

Login Name:

Password:

FIGURE: **Destination Database Detail** page of the **DbProtect Import Utility**

Do the following:

- In the **Microsoft SQL Server:** portion of the **Destination Database Detail** page:

  -enter the **Host Name:** of your destination DbProtect database server, or a valid IP address

  -manually enter (or use the **Instance Name:** drop-down to select) a specific DbProtect database server (**<Default Instance>** is selected by default), or enter the instance name manually.

- In the **Connect Using:** portion of the **Destination Database Detail** page, select whether you want to connect to your destination database using:

  -**Windows Authentication** using the current logged-on user's privileges.

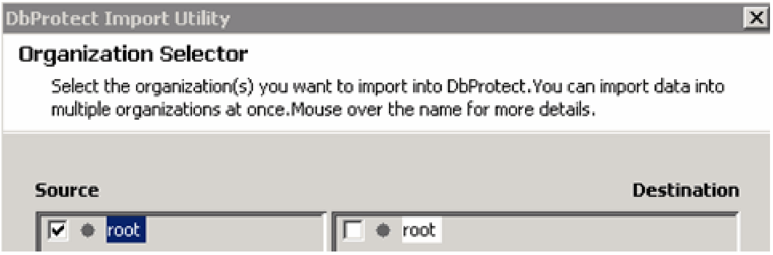
Note: This user **must** be a Microsoft SQL Server user on the destination machine.

-**SQL Authentication** (make sure SQL Authentication is enabled).

Note: If you're not sure which authentication type to select, see your database administrator.

- If you choose **SQL Authentication**, then you must also enter the database user **Login Name:** and **Password:**
- Click the **Test Connection** button to verify the connection on the destination database. If the connection succeeds, the **Next** button is illuminated.

4. Click the **Next** button to display the **Organization Selector** page of the **DbProtect Import Utility**.



DbProtect Import Utility

Organization Selector

Select the organization(s) you want to import into DbProtect.You can import data into multiple organizations at once.Mouse over the name for more details.

FIGURE: **Organization Selector** page of the **DbProtect Import Utility**

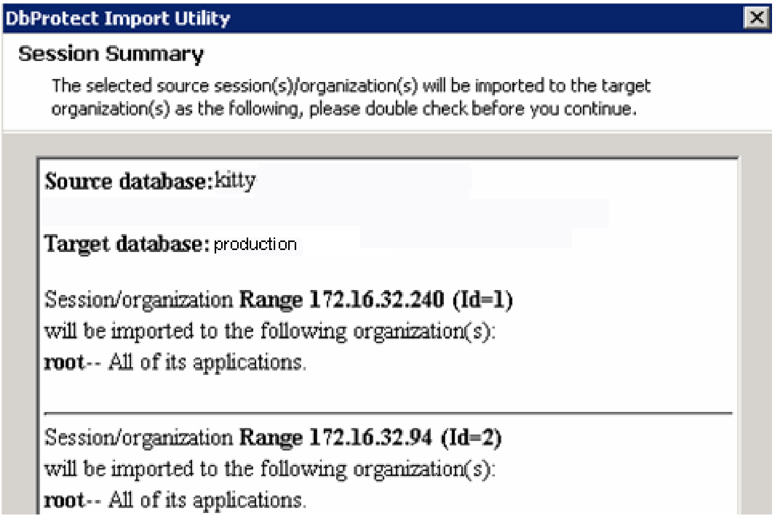
Select the Sessions you want to import from your selected AppDetectivePro or DbProtect back-end database (in the **Source** panel) into your DbProtect database (in the **Destination** panel).

Note: The **DbProtect Import Utility** imports all data (with source IP addresses that match the destination IP ranges) from your selected source Sessions into every Organization you selected in the **Destination** panel.

Example: Assume you are importing a Session with target databases in the IP range `192.168.1.1` - `192.168.1.255`, and the IP range `172.16.1.1 – 172.16.1.255`. Your `root` target Organization, however, only includes the IP range `192.168.1.1` - `192.168.1.255`. As a result, the **DbProtect Import Utility** imports all target databases in the IP range `192.168.1.1` - `192.168.1.255`, but ignores the `172.16.1.*` data. If you want to import the `172.16.1.*` data, you must modify the IP range of your destination Organization; for more information, see *Working with Scan Engines*.

Hint: If you mouse over any Organization name (in either the **Source** or **Destination** panels of the **Organization Selector** page), then the **DbProtect Import Utility** displays the Session names and IP ranges for all Discovered target databases. This feature allows you to logically compare your source Organizations and destination Organizations.

5. Click the **Next** button to display the **Session Summary** page of the DbProtect Import Utility.



Session Summary

The selected source session(s)/organization(s) will be imported to the target organization(s) as the following, please double check before you continue.

Source database: kitty

Target database: production

Session/organization **Range 172.16.32.240 (Id=1)**
will be imported to the following organization(s):
root-- All of its applications.

Session/organization **Range 172.16.32.94 (Id=2)**
will be imported to the following organization(s):
root-- All of its applications.

FIGURE: **Session Summary** page of the **DbProtect Import Utility**

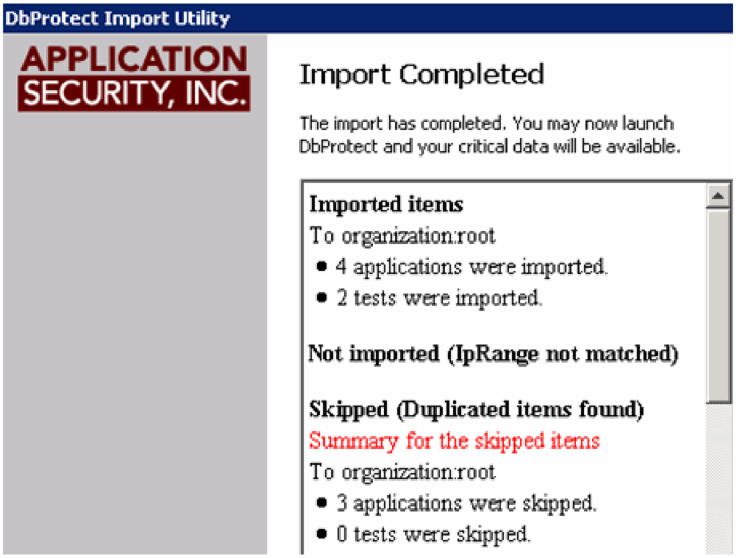
The **Session Summary** page of the **DbProtect Import Utility** displays a summary of which Sessions the utility is ready to import into your destination DbProtect database.

6. Click the **Next** button to import your Session data.

Note: For more information on what data the DbProtect Import Utility does and does **not** import, see *What data does the DbProtect Import Utility import (and not import)?*

When the import process completes, the **Import Completed** page of the **DbProtect Import Utility** displays.

Hint: You can copy/paste the import summary data and save it to a file for future reference.



Import Completed

The import has completed. You may now launch DbProtect and your critical data will be available.

Imported items

To organization:root

- 4 applications were imported.
- 2 tests were imported.

Not imported (IpRange not matched)

Skipped (Duplicated items found)

Summary for the skipped items

To organization:root

- 3 applications were skipped.
- 0 tests were skipped.

FIGURE: **Import Completed** page of the **DbProtect Import Utility**

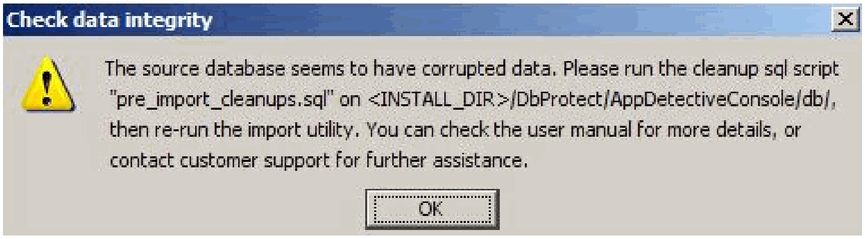
You may now launch DbProtect AppDetective. Your imported Session data is available; for more information, see *Vulnerability Management*.

Troubleshooting a corrupted source database with the pre_import_cleanups.sql script

In Step 2 of *Importing Session Data from an AppDetectivePro Session file* and *Importing Session data from an AppDetectivePro or DbProtect Microsoft SQL Server database*, the **DbProtect Import Utility** attempts to connect to your source database. The utility also checks whether there are any duplicated records in the following tables:

- `ScansServicesFound`
- `ChecksToRun`
- `VulnerabilityDetails`
- `HostNames`

If the **DbProtect Import Utility** discovers duplicate records in any of these tables, the **Check data integrity** pop up displays, informing you your source database contains corrupted data.



Check data integrity

The source database seems to have corrupted data. Please run the cleanup sql script "pre_import_cleanups.sql" on <INSTALL_DIR>/DbProtect/AppDetectiveConsole/db/, then re-run the import utility. You can check the user manual for more details, or contact customer support for further assistance.

FIGURE: **Check data integrity** pop up

In order to troubleshoot, do the following:

- Back up your corrupted source database.
- Close the **DbProtect Import Utility**.
- Run the `pre_import_cleanups.sql` script -- located in the following folder: `<installation directory>:\Program Files\AppSecInc\DbProtect\AppDetectiveConsole\db` -- against your corrupted source database server.
- Re-run the **DbProtect Import Utility**.

Note: If you experience trouble, contact Application Security, Inc. Customer Support at `support@appsecinc.com`.

Appendix F: Using the Configuration Manager Tool

Note: Starting with DbProtect 2008.1 R2, Application Security, Inc. removed the **Certificates** tab from the **Configuration Manager Tool**. This option used to allow you to install your company's own certificate to eliminate browser messages that indicated issues with the "website's security certificate". Security concerns, however, necessitated the removal of this option. Nevertheless, you can install a custom certificate using command line tools provided with DbProtect. For more information, see the *DbProtect Administrator's Guide*.

This appendix consists of the following topics:

- *What is the Configuration Manager Tool?*
- *Using the Configuration Manager Tool*.

What is the Configuration Manager Tool?

The **Configuration Manager Tool** allows you to modify the following DbProtect AppDetective configuration parameters on the host machine:

- **Server.** Clicking the **Server** tab on the **Configuration Manager Tool** allows you to configure the DbProtect AppDetective **listening port** and the **shutdown port**. The **listening port** is the port DbProtect AppDetective binds to and waits for incoming requests. The **shutdown port** is the port DbProtect AppDetective binds to and waits for incoming local shutdown requests. A shutdown request forces DbProtect AppDetective process to terminate.
- **Database.** Clicking the **Database** tab on the **Configuration Manager Tool** allows you to configure your **Database Server** and **Database Authentication** settings. Specifically, you can specify:

  -the database host machine where your AppDetectivePro database resides

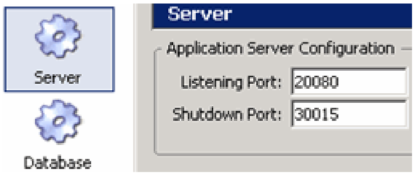
  -your back-end database credentials, which you can configure using Windows Authentication or SQL Authentication.

Note: In previous versions of DbProtect, you could use the **Configuration Manager Tool** to modify the Console's logging level. Now, you must manually change logging level values in the `log4j.properties` files; for more information, see *Appendix H: Manually Changing the Logging Level for the Console by Modifying the log4j.properties File*.

Using the Configuration Manager Tool

To use the **Configuration Manager Tool**:

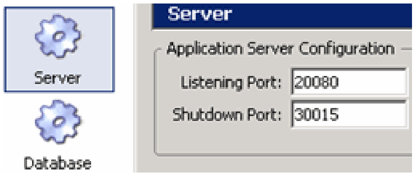
1. Choose **Start > Programs > AppSecInc > DbProtect > Configuration Manager** to display the **Configuration Manager**. The **General** tab is selected by default.



Listening Port: 20080
Shutdown Port: 30015

FIGURE: **Configuration Manager** (**Server** tab selected)

2. If you want to:
   - modify the DbProtect AppDetective **listening port** and/or **shutdown port**, then see Step 3
   - modify your DbProtect AppDetective **database server** information, see Step 4
   - modify your DbProtect AppDetective **database authentication** method, see Step 5.
3. To modify DbProtect AppDetective **listening port** and/or **shutdown port**:
   - Select the **Server** tab on the **Configuration Manager** (selected by default).
   - Modify the **Listening Port:** value. The **listening port** is the port DbProtect AppDetective binds to and waits for incoming requests.
   - Modify the **Shutdown Port:** value. The **shutdown port** is the port DbProtect AppDetective binds to and waits for incoming local shutdown requests. A shutdown request forces DbProtect AppDetective process to terminate.
   - Click the **OK** button.

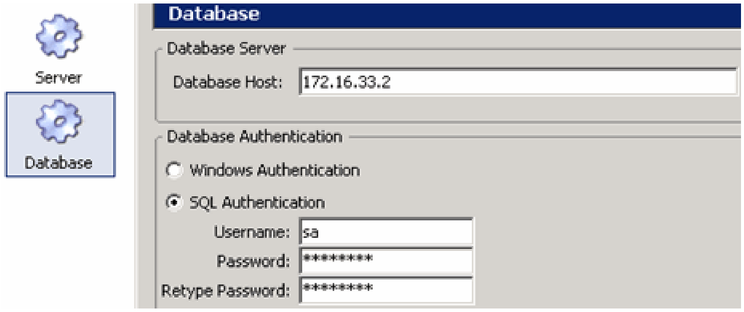


Listening Port: 20080
Shutdown Port: 30015

FIGURE: **Configuration Manager** (**Server** tab selected)

4. To modify your DbProtect AppDetective **database server** information:

- Select the **Database** tab on the **Configuration Manager**.
- Modify the AppDetectivePro **DB Host:** value.
- Click the **OK** button.



Database

Database Server

Database Host: 172.16.33.2

Database Authentication

○ Windows Authentication

● SQL Authentication

Username: sa

Password: ********

Retype Password: ********

FIGURE: **Configuration Manager** (**Database** tab selected)

5. To modify your DbProtect AppDetective **database authentication** method (using Windows Authentication or SQL Authentication):

- Select the **Database** tab on the **Configuration Manager**.
- In the **Database Authentication** portion of dialog box, select whether you want to configure your **back-end database credentials** using:

  -**Windows Authentication** using the Windows privileges of the user that runs the DbProtect services.

Note: This user **must** be a Microsoft SQL Server user on the back-end database machine.

-**SQL Authentication** (make sure SQL Authentication is enabled).

Note: If you're not sure which authentication type to select, see your database administrator.

If you choose **SQL Authentication**, then you must also enter the database user **Login Name:** and **Password:**

Appendix G: Moving or Changing Your DbProtect Back-End Database

To move or change your DbProtect back-end database, you must:

- use the built-in **AppDSN** utility to repair the OBDC (Open Database Connectivity) Database Source Name (DSN) entry on the DbProtect Console host, and on each installed Scan Engine host; for more information, see *Using the AppDSN utility to repair the ODBC DSN entry on your DbProtect Console host and on each installed Scan Engine host*
- update the JDBC connection strings on the DbProtect Console host; for more information, see *Updating the JDBC connection strings on the DbProtect Console host*.

AppDSN also allows you to change the type of authentication DbProtect AppDetective uses to authenticate to the DbProtect back-end database (i.e., *from* Windows authentication *to* SQL Server authentication -- or vice-versa).

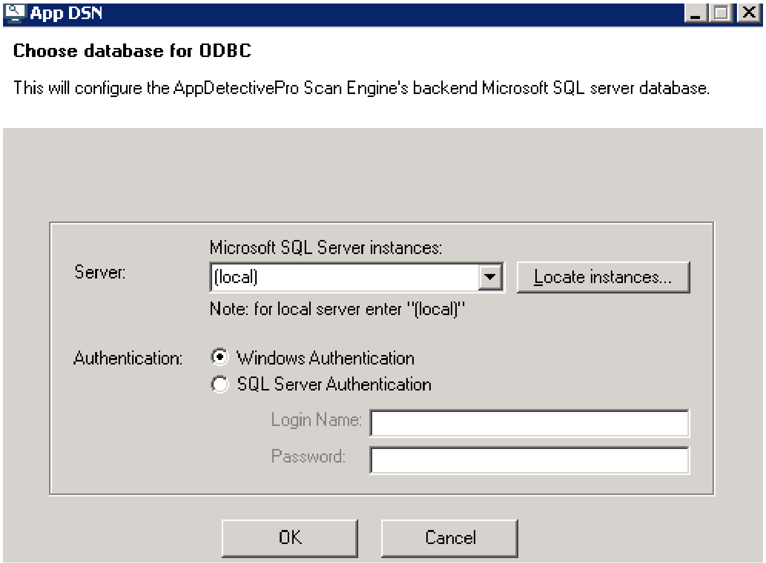
Using the AppDSN utility to repair the ODBC DSN entry on your DbProtect Console host and on each installed Scan Engine host

Again, you must use the AppDSN to repair the ODBC DSN entry on:

- the DbProtect Console host
- each installed Scan Engine host.

To use the AppDSN utility to repair the ODBC DSN entry on the DbProtect Console host and on each installed Scan Engine host:

1. Choose **Start > Programs > AppSecInc > AppDetective Scan Engine > AppDSN** to display the **AppDSN** utility.



Choose database for ODBC

This will configure the AppDetectivePro Scan Engine's backend Microsoft SQL server database.

Server: Microsoft SQL Server instances: (local)

Note: for local server enter "(local)"

Authentication: ● Windows Authentication ○ SQL Server Authentication

Login Name:

Password:

FIGURE: AppDSN utility

2. Use the **Server** drop-down to select the Microsoft SQL Server instance where the Scan Engine stores its results, or enter the Microsoft SQL Server instance name.

This **must** be the same database DbProtect AppDetective uses.

Hint: Click the **Locate instances...** button to search for/display all Microsoft SQL Server instances on your network.

3. Select to authenticate to the database server using: **Windows Authentication** (*strongly recommended*) or **SQL Server Authentication**.

If you select:

- **Windows Authentication**, then the `DbProtect Scan Engine` service uses the login/password credentials supplied in the Sensor installation section of the *DbProtect Installation Guide*. If you want to change or verify these values, you must run `services.msc`

- **SQL Server Authentication**, then you must enter a Microsoft SQL Server authentication **Login Name:** and **Password:**

4. Click the **OK** button.

The **Repair ODBC** utility changes the database server the Scan Engine uses to store its results, and/or changes the type of authentication DbProtect AppDetective uses to authenticate to the database server.

Updating the JDBC connection strings on the DbProtect Console host

To update the JDBC connection strings on the DbProtect Console host:

1. If you want to:

- change the username/password to connect to the DbProtect database, use the *Configuration Manager* tool; for more information, see *Appendix F: Using the Configuration Manager Tool*
- change the DbProtect database host or port, see Steps 2-4.

2. Stop the `DbProtect` and `Message Collector` services.

3. To change the DbProtect database host, first locate the following files:

- `<installation folder>\DbProtect\GUI\tomcat\conf\context.xml`
- `<installation folder>\Message Collector\tomcat\conf\context.xml`

Note: DbProtect encrypts credentials in these files. Application Security, Inc. recommends you use the **Configuration Manager** tool to modify the connection string and/or credentials; for more information see *Appendix F: Using the Configuration Manager Tool.*

At the bottom of each of these files you will notice the XML property values for the JDBC connection string. You can alter any of the values according to the following syntax: `jdbc:jtds:sqlserver://[host][:port][/database][;property=value[;...]]`. Change `[host]` to he desired hostname, and `[:port]` to the desired port.

4. Re-start the `DbProtect` and `Message Collector` services.

At the bottom of each of these files you will notice the XML property values for the JDBC connection string. You can alter any of the values according to the following syntax: `jdbc:jtds:sqlserver://[server][:port][/database][;property=value[;...]]`

Examples:

- Using **Windows Authentication**, URL = `"jdbc:jtds:sqlserver://larch/appdetective;ssl=request" username="" password=""`
- Using **SQL Server Authentication**, URL =`"jdbc:jtds:sqlserver://larch/appdetective;ssl=request" username="dbp-appuser" password="user$1560p"`

You can use either the instance name or the explicit port number for named instances. Using the port number explicitly eliminates the need to have SQL Server Browser Service running.

- URL = `"jdbc:jtds:sqlserver://[server][:port]/appdetective;ssl=request"`

  OR

- URL = `"jdbc:jtds:sqlserver://[server]/appdetective;ssl=request[;instance=<instance name>]`

Appendix H: Manually Changing the Logging Level for the Console by Modifying the log4j.properties File

This appendix consists of the following topics:

- *What are the Console logging levels?*
- *log4j.properties file location*
- *Manually modifying logging level values in a log4j.properties file.*

Note: This appendix explains how to manually modify logging level values in a `log4j.properties` file for DbProtect 2009.1R3 and greater. Previous versions of DbProtect have different instructions. Please refer to the appropriate, version-specific copy of the DbProtect User's Guide for `log4j.properties` file logging level modification instructions if your version of DbProtect is earlier than 2009.1R3.

What are the Console logging levels?

The Console **logging level** controls the volume of log information the Console outputs to its log files.

In versions of the Console prior to version 3.10, you could use the **Configuration Manager Tool** to modify the **Console's logging level**. However, 3.10 and greater versions of the Console require you to manually change the Console's logging level values in a `log4j.properties` file.

Note: Application Security, Inc. highly recommends you do **not** modify the Console `log4j.properties` file, unless instructed to do so by Customer Support.

VALID CONSOLE LOGGING LEVEL VALUES

Valid Console logging level values follow the hierarchy below, from most to least verbose:

- **DEBUG** (an increased logging level used to troubleshoot Console, Scan Engine, Sensor, and database problems)
- **INFO**
- **WARN**
- **ERROR**
- **FATAL** (a decreased logging level used to optimize Console performance).

log4j.properties file location

DbProtect 2009.1R3 and greater has only one log file and only one `log4j.properties` file (for both DbProtect Audit and Threat Management and DbProtect Vulnerability Management). It is located here: `<installation folder>\DbProtect\GUI\tomcat\common\classes`

The `log4j.properties` file for the **Message Collector** component is located here: `<AppSecInc Location>\Message Collector\tomcat\common\classes`

Manually modifying logging level values in a log4j.properties file

To manually modify the logging level values in a `log4j.properties` file:

1. For SOAP logging between the Console and Sensors/Scan Engines.

If you run an Audit, or deploy a Policy to a Sensor, the log includes SOAP messages containing Audit and/or Policy information.

Edit the `log4j.properties` file and change the level from **WARN** to **INFO** in the following lines:

- `log4j.logger.org.apache.cxf.interceptor.LoggingInInterceptor=WARN`
- `log4j.logger.org.apache.cxf.interceptor.LoggingOutInterceptor=WARN`

2. For SOAP logging between Console and Console client.

You can track SOAP messages passing between the client and the server. **After** you make the edits described below, the DbProtect log will contain SOAP messages with the current logged-in username.

- Edit the `log4j.properties` file and change the level from **WARN** to **INFO** on the following lines

  ```
  log4j.logger.org.apache.cxf.interceptor.LoggingInInterceptor=WARN
  log4j.logger.org.apache.cxf.interceptor.LoggingOutInterceptor=WARN
  ```
- Unpack the `appdetective.war` file.
- Open `appdetective/WEB-INF/cxf-servlet.xml` and locate the following lines:

  ```
  <jaxws:server id="ADCService"
  serviceClass="com.appsec.console.soap.adc.ADC" address="/
  ADCService">
  <jaxws:serviceBean>
  <bean class="com.appsec.console.soap.adc.ADCServiceImpl" />
  </jaxws:serviceBean>
  </jaxws:server>
  ```

  Change it to the following:

  ```
  <jaxws:server id="ADCService"
  serviceClass="com.appsec.console.soap.adc.ADC" address="/
  ADCService">

  <jaxws:serviceBean>

  <bean class="com.appsec.console.soap.adc.ADCServiceImpl" />

  </jaxws:serviceBean>
  ```

```
<jaxws:inInterceptors>
<ref bean="loggingInInterceptor"/>
</jaxws:inInterceptors>
<jaxws:outInterceptors>
<ref bean="loggingOutInterceptor"/>
</jaxws:outInterceptors>
</jaxws:server>
```

- Save the file and repack the `appdetective.war` file.
- Re-start the Console.

3. Log client-side activity.

The AppDetective applet uses a different `log4j.properties` file, which is packaged into `consoleapp.jar`

- Unpack the `appdetective.war` file.
- Create a backup of the following files:

```
-consoleapp.jar
-consoleapp.jar.pack.gz
```

- Delete the `consoleapp.jar.pack.gz` package file from the current folder.
- Rename the `consoleapp.jar` package file to: `consoleapp.zip`
- Use a zip tool to open the archive and edit `consoleapp.zip`.

Caution! Do **not** extract and replace, because this might corrupt the `.jar` file.

- Locate and open the `log4j.properties` file for editing.

The default Console appender is:
`log4j.appender.C=org.apache.log4j.ConsoleAppender`

Note: The appender writes to the Java console on the client side's machine.

- Define the logging level for the desired package (i.e., classes within `com.appsec.console.gui.xxx`).

  Example: You can change **WARN** to **INFO** in the snippet below to log SOAP messages on the client side.

Note: You must set #CXF SOAP logging to **INFO** or higher in order to see the SOAP messages.

```
log4j.logger.org.apache.cxf.interceptor.LoggingInInterceptor=
WARN

log4j.logger.org.apache.cxf.interceptor.LoggingOutInterceptor=
WARN
```

- Save the `log4j.properties` file and close the `.zip` file.
- Re-name `consoleapp.zip` to `consoleapp.jar`.

To restore the logging level to its original setting, do the following:

- Unpack the `appdetective.war` file.
- Restore the `consoleapp.jar` and `consoleapp.jar.pack.gz` files from your backup.
- Repack the `.war` file.
- Re-start the `DbProtect Console` service.

Appendix I: Required Audit Privileges

In this appendix:

- *IBM DB2 Audit Privileges*
- *IBM DB2 z/OS Audit Privileges*
- *Lotus Domino Groupware Audit Privileges*
- *Microsoft SQL Server Audit Privileges and User Creation Scripts*
- *MySQL Audit Privileges*
- *Oracle Audit Privileges and User Creation Script*
- *Sybase Audit Privileges*
- *Operating System Considerations (for Audits).*

IBM DB2 Audit Privileges

Note: For more information on IBM DB2 OS check requirements, see *Operating System Considerations (for Audits).*

To conduct a full **IBM DB2** Audit, you need the following **privileges**. Make sure the account you are using has rights to use the following tables, views, and functions:

- `CONNECT`
- `GET DATABASE MANAGER CONFIGURATION & LIST DATABASE DIRECTORY`
- `Service Info` (on Windows only)
- `SYSIBM.SYSCOLAUTH`
- `SYSIBM.SYSINDEXAUTH`
- `SYSIBM.SYSPASSTHRUAUTH`
- `SYSIBM.SCHEMAAUTH`
- `SYSIBM.SYSDBAUTH`
- `SYSIBM.SYSTABAUTH`
- `SYSIBM.SYSFUNCTIONS`
- `SYSIBM.SYSPROCEDURES`
- `SYSIBM.SYSVERSIONS`
- `SYSPROC.SNAPSHOT_DATABASE`

Note: `SYSPROC.SNAPSHOT_DATABASE` requires the Audit user to have `SYSMON` authority. Users with `SYSADM`, `SYSCTRL`, or `SYSMAINT` authority automatically inherit `SYSMON` authority.

Below is a list of **checks** within DbProtect Vulnerability Assessment for an IBM DB2 Audit, and the tables and views they need permission to access in order to function properly:

- `CLIENT authentication: GET DATABASE MANAGER CONFIGURATION & LIST DATABASE DIRECTORY`
- `SERVER authentication: GET DATABASE MANAGER CONFIGURATION & LIST DATABASE DIRECTORY`
- `DCS authentication: GET DATABASE MANAGER CONFIGURATION & LIST DATABASE DIRECTORY`
- `Trust All Client: GET DATABASE MANAGER CONFIGURATION & LIST DATABASE DIRECTORY`
- `Authentication type: GET DATABASE MANAGER CONFIGURATION & LIST DATABASE DIRECTORY`
- `Service runs as LocalSystem: Service Info (Windows ONLY)`
- `Permissions granted to PUBLIC: SYSIBM.SYSCOLAUTH, SYSIBM.SYSINDEXAUTH, SYSIBM.SYSPASSTHRUAUTH, SYSIBM.SCHEMAAUTH, SYSIBM.SYSDBAUTH, SYSIBM.SYSTABAUTH`
- `Permissions granted to user: SYSIBM.SYSCOLAUTH, SYSIBM.SYSINDEXAUTH, SYSIBM.SYSPASSTHRUAUTH, SYSIBM.SCHEMAAUTH, SYSIBM.SYSDBAUTH, SYSIBM.SYSTABAUTH`
- `Permissions grantable: SYSIBM.SYSCOLAUTH, SYSIBM.SYSINDEXAUTH, SYSIBM.SYSPASSTHRUAUTH, SYSIBM.SCHEMAAUTH, SYSIBM.SYSDBAUTH, SYSIBM.SYSTABAUTH`
- `Permissions on system catalog: SYSIBM.SYSDBAUTH, SYSIBM.SYSTABAUTH`
- `Permissions to list users: SYSIBM.SYSDBAUTH, SYSIBM.SYSTABAUTH`
- `db2ckpwd buffer overflow (Version verify): SYSIBM.SYSVERSIONS`
- `Query Compiler DoS (Verify version): SYSIBM.SYSVERSIONS`
- `Date/Varchar DoS (Verify version): SYSIBM.SYSVERSIONS`
- `Latest FixPak not installed: SYSIBM.SYSVERSIONS`
- `Control Center buffer overflow (Verify version): SYSIBM.SYSVERSIONS`
- `Excessive DBADM connections`

For the `Excessive DBADM connections` check, the IBM DB2 OS user **must** have:

- `SELECT` or `CONTROL` privilege on the `APPLICATIONS` and `SNAPAPPL_INFO` administrative views
- `SYSMON`, `SYSCTRL`, `SYSMAINT`, or `SYSADM` authority which is required to access snapshot monitor data.

Some DB2 Audit checks need to differentiate between fixpaks such as 4/4a, 6/6a, etc. These checks require specific **permissions**. Specifically, the checks affected are:

- `Arbitrary code execution in a federated system (Verify version)`
- `Arbitrary code execution when processing connection messages (Verify version)`
- `Arbitrary file creation in XML Extender functions (Verify version)`

- Buffer overflow in CALL statement (Verify version)
- Buffer overflow in db2fmp (Verify version)
- Buffer overflow in generate_distfile procedure (Verify version)
- Buffer overflow in REC2XML function (Verify version)
- Buffer overflow in SATADMIN.SATENCRYPT function (Verify version)
- Buffer overflow in the JDBC listener (Verify version)
- Buffer overflows in XML Extender functions (Verify version)
- DoS in string formatting functions (Verify version)
- Latest FixPak not installed
- Multiple Buffer overflows in libdb2.so.1 library (Verify version)
- Multiple critical vulnerabilities in IBM DB2 (Verify version)
- Multiple DoS vulnerabilities in SQLJRA protocol

The IBM DB2 OS user **must** have access to the db2greg command on all Unix platforms for the following IBM DB2 LUW checks:

- Permission on files
- Setuid bit enabled
- Setgid bit enabled

In order for DbProtect Vulnerability Assessment to work properly with any of these checks, you must set special **permissions**, depending on what version of DB2 is running on your server. The following table explains which permissions are required for which versions of DB2:

If your server is running DB2 version:	Requirements:
9.10 or later	SELECT or CONTROL privilege on the ENV_INST_INFO administrative view. OR SYSADM and/or ATTACH privileges. AND EXECUTE privilege on the ENV_GET_INST_INFO table function (required for IBM DB2 LUW v 8.2.2 and later).
8.2.2 or later	EXECUTE privilege on the ENV_GET_INST_INFO table function.
8.1.0 or later	SYSADM or ATTACH privileges.
7	Registry access or OS access.

IBM DB2 z/OS Audit Privileges

This topic consists of the following sub-topics:

- *Full IBM DB2 z/OS Audit Requirements*
- *Per Check IBM DB2 z/OS Audit Requirements.*

FULL IBM DB2 Z/OS AUDIT REQUIREMENTS

You require the following **permissions** (which `SYSADM` has by default) in order to conduct a full **IBM DB2 z/OS** Audit with all checks enabled:

- `SELECT` privileges on the following catalog tables:

```
-SYSIBM.SYSCOLAUTH
-SYSIBM.SYSDBAUTH
-SYSIBM.SYSPACKAUTH
-SYSIBM.SYSPLANAUTH
-SYSIBM.SYSROUTINEAUTH
-SYSIBM.SYSSCHEMAAUTH
-SYSIBM.SYSTABAUTH
-SYSIBM.SYSUSERAUTH
-SYSIBM.GETVARIABLE
```

- Permission to call the following function: `SYSIBM.GETVARIABLE`
- Permission to call the following stored procedure: `SYSPROC.DSNWZP`

PER CHECK IBM DB2 Z/OS AUDIT REQUIREMENTS

To conduct an IBM DB2 z/OS Audit with selected **checks** enabled, the following permissions are required in a per-check basis:

- All checks require permission to call the following function: `SYSIBM.GETVARIABLE`
- The following IBM DB2 z/OS Audit checks require permission to call the stored procedure `SYSPROC.DSNWZP`:

```
-Dual logging not enabled
-Dual archiving not enabled
-SMF accounting is not set to start automatically
-Audit Trace is not set to start automatically
-SMF statistics not set to start automatically
-Authorization checking disabled
-Collection interval for statistics
-System install administrators and operators
```

Note: If the `SYSPROC.DSNWZP` and `SYSPROC.ADMIN_DS_LIST` stored procedures are not enabled, you **must** enable them and set up the proper environments so they can function correctly.

- The IBM DB2 z/OS Audit check `Connection and sign-on exits` requires permission to call the stored procedure `SYSPROC.ADMIN_DS_LIST`.
- The following table lists IBM DB2 z/OS Audit checks which **must** have `SELECT` privileges on the corresponding IBM DB2 z/OS tables:

Check	Corresponding IBM DB2 z/OS tables requiring `SELECT` privileges
`Access list of authorization IDs`	`SYSIBM.SYSTABAUTH`
`Administrative authorities on DB2 Subsystem`	`SYSIBM.SYSUSERAUTH`
`Privileges granted to PUBLIC on packages`	`SYSIBM.SYSPACKAUTH`
`Administrative authorities for DB2 catalog database`	`SYSIBM.SYSDBAUTH`
`Administrative authorities over databases`	`SYSIBM.SYSDBAUTH`
`Privileges granted to PUBLIC on plans`	`SYSIBM.SYSPLANAUTH`
`PUBLIC granted Administrative authorities on DB2 Subsystem`	`SYSIBM.SYSUSERAUTH`
`Privileges granted to PUBLIC on columns`	`SYSIBM.SYSCOLAUTH`
`Privileges granted to PUBLIC on routines`	`SYSIBM.SYSROUTINEAUTH`
• `Easily-guessed usernames and passwords` • `No permission is required` • `Privileges granted to PUBLIC on databases`	`SYSIBM.SYSDBAUTH`
`Privileges granted to PUBLIC on DB2 subsystem`	`SYSIBM.SYSUSERAUTH`

Check	Corresponding IBM DB2 z/OS tables requiring SELECT privileges
Password same as username for account	SYSIBM.SYSDBAUTH SYSIBM.SYSTABAUTH SYSIBM.SYSPLANAUTH SYSIBM.SYSCOLAUTH SYSIBM.SYSSCHEMAAUTH SYSIBM.SYSPACKAUTH SYSIBM.SYSROUTINEAUTH SYSIBM.SYSUSERAUTH
Privileges on the DB2 catalog	PSYSTABAUTH
Privileges granted to PUBLIC on schemas	SYSIBM.SYSSCHEMAAUTH
Privileges granted to PUBLIC on DB2 catalog tables	SYSTABAUTH
Privileges granted to PUBLIC on tables	SYSTABAUTH
Administrative authority for database granted to PUBLIC	SYSIBM.SYSDBAUTH

Lotus Domino Groupware Audit Privileges

Note: For more information on Lotus Domino OS check requirements, see *Operating System Considerations (for Audits).*

To conduct a full **Lotus Domino Groupware** Audit, you need the following **privileges**. Make sure the account you are using has rights to use the following tables and views:

- `Read all databases`
- `Read decsadm.nsf and all of its documents`
- `Read names.nsf and all of its documents`
- `Execute commands on the server`
- `Read all user documents`

At a document level, DbProtect Vulnerability Assessment checks certain fields, including: `$Author`, `$Readers`, `RM_MapFrom`, `$Readers`, and fields of type `LNRTTYPE_AUTHORS_FIELD`.

DbProtect Vulnerability Assessment also verifies certain Lotus Domino Groupware properties (for example, if you have attachments and if they are encrypted). If any of the required fields listed above are encrypted and the id does not have access to it, then some of the checks below will **not** work properly.

Caution! **Despositor** access that **only** has access to read public documents is sufficient to run a Lotus Domino Groupware Audit, with the exception of the `names.nsf` database which requires **Reader** access.

Besides `SHOW` commands, the following Lotus Domino Groupware **commands** are also executed:

- `TELL HTTP SHOW FILE ACCESS`
- `SET SECURE`

Below is a list of **checks** within the DbProtect Vulnerability Assessment for a Lotus Domino Audit, and the tables and views they need permission to access in order to function properly:

- `Anonymous can create documents: Read all databases`
- `Anonymous granted Designer or higher access: Read all databases`
- `Anonymous user in Authors field: Read all databases`
- `Default has Editor or higher access: Read all databases`
- `Encrypted field full-text indexed: Read all databases`
- `Unspecified user type in ACL: Read all databases`
- `DECS password unencrypted: Read decsadm.nsf and all of its documents`
- `Anonymous ACL missing: Read all databases, Read names.nsf and all of its documents`
- `Access server unrestricted: Read names.nsf and all of its documents`
- `All people can use monitors: Read names.nsf and all of its documents`
- `All users can run personal agents: Read names.nsf and all of its documents`
- `Anonymous access via HTTPS: Read names.nsf and all of its documents`
- `Anonymous access via Notes RPC: Read names.nsf and all of its documents`
- `Bindsock arbitrary file creation: Read names.nsf and all of its documents`
- `CGI directory leak: Read names.nsf and all of its documents`
- `Check passwords on Notes IDs: Read names.nsf and all of its documents`
- `Create databases unrestricted: Read names.nsf and all of its documents`
- `Enumerate groups: Read names.nsf and all of its documents`
- `Failed access control on file attachments: Read names.nsf and all of its documents`
- `iNotes client ActiveX control buffer overflow: Read names.nsf and all of its documents`

- iNotes s_ViewName buffer overflow: Read names.nsf and all of its documents
- Latest maintenance release not applied: Read names.nsf and all of its documents
- Long POST request DoS: Read names.nsf and all of its documents
- Maximum number of request headers: Read names.nsf and all of its documents
- Maximum size of request contents: Read names.nsf and all of its documents
- Maximum size of request headers: Read names.nsf and all of its documents
- Maximum URL length: Read names.nsf and all of its documents
- Maximum URL path segments: Read names.nsf and all of its documents
- Non-admins can use monitors: Read names.nsf and all of its documents
- Notes RPC buffer overflow: Read names.nsf and all of its documents
- Notes_ExecDirectory buffer overflow: Read names.nsf and all of its documents
- Password change interval for user: Read names.nsf and all of its documents
- PATH buffer overflow: Read names.nsf and all of its documents
- Public keys compared to directory: Read names.nsf and all of its documents
- Restricted agents runlist: Read names.nsf and all of its documents
- Restricted Java/COM runlist: Read names.nsf and all of its documents
- Saved email not encrypted: Read names.nsf and all of its documents
- Servlets disabled: Read names.nsf and all of its documents
- Unrestricted agents runlist: Read names.nsf and all of its documents
- Unrestricted Java/COM runlist: Read names.nsf and all of its documents
- User can create new databases: Read names.nsf and all of its documents
- Administration over HTTP: Read names.nsf and all of its documents, Execute a command on the server
- Anonymous access via HTTP: Read names.nsf and all of its documents, Execute a command on the server
- Anonymous access via IIOP: Read names.nsf and all of its documents, Execute a command on the server
- Anonymous access via IIOPS: Read names.nsf and all of its documents, Execute a command on the server

- Anonymous access via LDAP: Read names.nsf and all of its documents, Execute a command on the server
- Anonymous access via LDAPS: Read names.nsf and all of its documents, Execute a command on the server
- ESMTP buffer overflow: Read names.nsf and all of its documents, Execute a command on the server
- Expired certificates allowed: Read names.nsf and all of its documents, Execute a command on the server
- HTTP authenticate buffer overflow: Read names.nsf and all of its documents, Execute a command on the server
- HTTP database browsing: Read names.nsf and all of its documents, Execute a command on the server
- HTTP logging not enabled: Read names.nsf and all of its documents, Execute a command on the server
- HTTP methods excluded from logging: Read names.nsf and all of its documents, Execute a command on the server
- HTTP MIME types excluded from logging: Read names.nsf and all of its documents, Execute a command on the server
- HTTP return codes excluded from logging: Read names.nsf and all of its documents, Execute a command on the server
- HTTP user agents excluded from logging: Read names.nsf and all of its documents, Execute a command on the server
- HTTPS allows anonymous access: Read names.nsf and all of its documents, Execute a command on the server
- Inadequate amgr process logging: Read names.nsf and all of its documents, Execute a command on the server
- Incomplete POST DoS: Read names.nsf and all of its documents, Execute a command on the server
- Interface address leak in banner: Read names.nsf and all of its documents, Execute a command on the server
- LDAP buffer overflow: Read names.nsf and all of its documents, Execute a command on the server
- LDAP format string: Read names.nsf and all of its documents, Execute a command on the server
- MS-DOS device web path leak: Read names.nsf and all of its documents, Execute a command on the server
- Personal agents runlist: Read names.nsf and all of its documents, Execute a command on the server
- Redirected host/location buffer overflow: Read names.nsf and all of its documents, Execute a command on the server
- Routing loop DoS (Verify version): Read names.nsf and all of its documents, Execute a command on the server
- SMTP buffer overflow: Read names.nsf and all of its documents, Execute a command on the server
- Unencrypted HTTP: Read names.nsf and all of its documents, Execute a command on the server

- `Unencrypted IIOP: Read names.nsf and all of its documents, Execute a command on the server`
- `Unencrypted IMAP: Read names.nsf and all of its documents, Execute a command on the server`
- `Unencrypted LDAP: Read names.nsf and all of its documents, Execute a command on the server`
- `Unencrypted NNTP: Read names.nsf and all of its documents, Execute a command on the server`
- `Unencrypted POP3: Read names.nsf and all of its documents, Execute a command on the server`
- `Web retriever HTTP status buffer overflow: Read names.nsf and all of its documents, Execute a command on the server`
- `Web Retriever logging: Read names.nsf and all of its documents, Execute a command on the server`
- `Easily-guessed Internet password: Read all user documents`
- `Easily-guessed Notes password: Read all user documents`
- `Agent manager debugging not enabled: Execute a command on the server`
- `Ambiguous webnames allowed: Execute a command on the server`
- `Console password not set: Execute a command on the server`
- `Inadequate console logging: Execute a command on the server`
- `NDS password present: Execute a command on the server`
- `NDS userid present: Execute a command on the server`
- `Phone line logging not enabled: Execute a command on the server`

Microsoft SQL Server Audit Privileges and User Creation Scripts

Note: For more information on Microsoft SQL Server OS check requirements, see *Operating System Considerations (for Audits)*.

This topic consists of the following sub-topics:

- *Microsoft SQL Server 2000 and MSDE Audit Privileges*
- *Running the Microsoft SQL Server 2000 User Creation Script*
- *Running the Microsoft SQL Server 2000 with Sysadmin User Creation Script*
- *Microsoft SQL Server 2005 and Microsoft SQL Server 2008 Audit Privileges*
- *Credentials for Microsoft SQL Server Audits*
- *Running the Microsoft SQL Server 2005 and 2008 User Creation Script*
- *Registry Access for Microsoft SQL Server 2000, 2005, and 2008.*

MICROSOFT SQL SERVER 2000 AND MSDE AUDIT PRIVILEGES

To conduct a full **Microsoft SQL Server 2000** or **MSDE** Audit, you need the following **privileges**. Make sure the account you are using has rights to use the following tables and views:

Check	Privileges Required
`master.dbo.xp_loginconfig`	`EXECUTE`
`master.dbo.xp_regread`	
`exec <db name>.dbo.sp_helprotect`	
`msdb.dbo.sp_get_sqlagent_properties`	
`master.dbo.xp_cmdshell`	
`@@VERSION`	`SELECT`
`master.dbo.syslogins (MSSQLSysLogins)`	
`master.dbo.sysxlogins`	
`master.dbo.sysdatabases`	
`master.dbo.sysconfigures`	
`master.dbo.syscurconfigs`	
`master.dbo.syscharsets`	
`<db name>.dbo.sysusers`	
`<db name>.dbo.sysobjects`	
`<db name>.dbo.syscomments`	

In addition, certain Microsoft SQL Server 2000 DISA-STIG Database Security Configuration checks require you to be a member of the `sysadmin` fixed server role or the `db_owner` fixed database role on the publication database. The following table provides specific information about which checks require which roles (and why):

Microsoft SQL Server 2000 DISA-STIG checks:	Use:	To run these checks, you must be a member of:
`DBMS replication account privileges`	Replication system stored procedures.	The `sysadmin` fixed server role or the `db_owner` fixed database role on the publication database.
`Replication snapshot folder protection`		
`Database auditing`	`fn_trace_getinfo` and `fn_trace_geteventinfo` functions.	The `sysadmin` fixed server role.
`Auditing of Security Events`		
`Startup Stored Procedures`		

Below is a list of **checks** within the DbProtect Vulnerability Assessment for a Microsoft SQL Server 2000 Audit, and the tables and views they need permission to access in order to function properly:

- `Agent jobs privilege escalation: exec <db name>.dbo.sp_helprotect, master.dbo.sysdatabases`
- `Auditing of failed logins: master.dbo.xp_loginconfig`
- `Auditing of successful logins: master.dbo.xp_loginconfig`
- `Blank password: master.dbo.sysxlogins`
- `Blank password for sa: master.dbo.sysxlogins`
- `Blank password for well-known login: master.dbo.sysxlogins`
- `BULK INSERT buffer overflow: @@VERSION`
- `C2 Audit Mode: @@VERSION, master.dbo.sysconfigures, master.dbo.syscurconfigs`
- `Case-insensitive sort order: master.dbo.syscharsets, master.dbo.sysconfigures,master.dbo.syscurconfigs`
- `Changing mode may leave sa password blank: @@VERSION`
- `Cleartext password written by installation: @@VERSION, master.dbo.xp_cmdshell`
- `Computed Column UDF DoS:  @@version`
- `Database ownership chaining not disabled: sysconfigures,syscurconfigs`
- `DBCC addextendedproc buffer overflow: @@VERSION`
- `DBCC BUFFER buffer overflow: @@VERSION`

- DBCC CHECKCONSTRAINTS buffer overflow: @@VERSION
- DBCC CLEANTABLE buffer overflow: @@VERSION
- DBCC INDEXDEFRAG buffer overflow: @@VERSION
- DBCC PROCBUF buffer overflow: @@VERSION
- DBCC SHOWCONTIG buffer overflow: @@VERSION
- DBCC SHOWTABLEAFFINITY buffer overflow: @@VERSION
- DBCC UPDATEUSAGE buffer overflow: @@VERSION
- DBMS remote system credential use and access: master.dbo.sysxlogins, [master].dbo.sysservers
- Default login enabled: @@VERSION, master.dbo.syslogins, master.dbo.xp_loginconfig
- Direct updates on data dictionary: master.dbo.sysconfigures, master.dbo.syscurconfigs
- DTS package procedures granted to public: sp_helprotect
- DTS package password publicly viewable: msdb.dbo.sysuser, exec msdb.dbo.sp_helprotect
- DTS password exposed in properties dialog: @@VERSION
- DTS passwords publicly viewable: <db name>.dbo.sysuser, exec <db name>.dbo.sp_helprotect, master.dbo.sysdatabases
- Easily-guessed password: @@VERSION
- Easily-guessed password for sa: @@VERSION
- Easily-guessed password for well-known login: @@VERSION
- Encoded password written by installation: @@VERSION, master.dbo.xp_cmdshell
- Enterprise Manager improperly revokes proxy account: @@VERSION
- Error logs can be overwritten: Registry access

Note: To learn more about enabling registry access for Microsoft SQL Server 2000, see *Registry Access for Microsoft SQL Server 2000, 2005, and 2008.*

- Escalated privileges in heterogeneous joins: @@VERSION
- Extended stored proc privilege upgrade: exec <db name>.dbo.sp_helprotect, master.dbo.sysdatabases
- Fixed server role granted: master.dbo.syslogins
- Format string in C runtime DoS: @@VERSION
- Format string vuln in xp_sprintf: @@VERSION
- FORMATMESSAGE buffer overflow: @@VERSION
- Global temporary stored proc exists: sysobjects,sysusers
- Guest user exists in database: <db name>.dbo.sysuser, master.dbo.sysdatabases
- Hello buffer overflow: @@VERSION
- Infected with Spida worm: <db name>.dbo.sysobjects, master.dbo.sysdatabases, master.dbo.xp_cmdshell
- Jet running in sandbox Mode: Registry access

Note: To learn more about enabling registry access for Microsoft SQL Server 2000, see *Registry Access for Microsoft SQL Server 2000, 2005, and 2008.*

- Job output file handling: @@VERSION

- `Latest service pack applied: @@VERSION`
- `Lumigent Log Explorer buffer overflow: <db name>.dbo.sysobjects, master.dbo.sysdatabases`
- `Malformed RPC request DoS: @@VERSION`
- `Malformed TDS packet header DoS: @@VERSION`
- `MDX Query buffer overflow: @@VERSION`
- `Objects not owned by dbo: <db name>.dbo.sysobjects, master.dbo.sysdatabases, <db name>.dbo.sysuser`
- `OLEDB ad hoc queries allowed: Registry access`

Note: To learn more about enabling registry access for Microsoft SQL Server 2000, see *Registry Access for Microsoft SQL Server 2000, 2005, and 2008.*

- `Orphaned user: @@VERSION, <db name>.dbo.sysuser, master.dbo.sysdatabases, master.dbo.syslogins`
- `Password same as login name: @@VERSION`
- `Permission grantable: exec <db name>.dbo.sp_helprotect, master.dbo.sysdatabases`
- `Permissions granted to public: <db name>.dbo.sp_helprotect`
- `Permission on mswebtasks: exec <db name>.dbo.sp_helprotect, master.dbo.sysdatabases`
- `Permission on registry extended proc: exec <db name>.dbo.sp_helprotect, master.dbo.sysdatabases`
- `Permission on sp_MSsetalertinfo: exec <db name>.dbo.sp_helprotect, master.dbo.sysdatabases`
- `Permission on sp_MSSetServerProperties: exec <db name>.dbo.sp_helprotect, master.dbo.sysdatabases`
- `Permission on sp_readwebtask: exec <db name>.dbo.sp_helprotect, master.dbo.sysdatabases`
- `Permission on sp_runwebtask: exec <db name>.dbo.sp_helprotect, master.dbo.sysdatabases`
- `Permission on xp_readerrorlog: exec <db name>.dbo.sp_helprotect, master.dbo.sysdatabases`
- `Permission to select from syslogins: exec <db name>.dbo.sp_helprotect, master.dbo.sysdatabases`
- `Permission to select from system table: <db name>.dbo.sysobjects, exec <db name>.dbo.sp_helprotect, master.dbo.sysdatabases`
- `Permissions granted on sp_add_dtspackage: msdb.dbo.sysuser, exec msdb.dbo.sp_helprotect`
- `Permissions granted on xp_cmdshell: @@VERSION, exec <db name>.dbo.sp_helprotect, master.dbo.sysdatabases`
- `Permissions granted to user: <db name>.dbo.sysuser, exec <db name>.dbo.sp_helprotect, master.dbo.sysdatabases`
- `Public can create Agent jobs: exec <db name>.dbo.sp_helprotect, master.dbo.sysdatabases`
- `pwdencrypt buffer overflow: @@VERSION`
- `RAISERROR buffer overflow: @@VERSION`

- `Registry extended proc not removed: <db name>.dbo.sysobjects, master.dbo.sysdatabases`
- `Remote access allowed: master.dbo.sysconfigures, master.dbo.syscurconfigs`
- `Remote data source function unchecked buffer: @@VERSION`
- `Replication password publicly viewable: xp_regread,sysobjects,@@version,sp_helprotect`
- `Resolution service DoS: @@VERSION`
- `Resolution service heap overflow: @@VERSION`
- `Resolution service stack overflow: @@VERSION`
- `Reusable cached administrator connection: @@VERSION`
- `sp_attachsubscription command injection: @@VERSION, <db name>.dbo.sysobjects, master.dbo.sysdatabases`
- `sp_MScopyscriptfile command injection: <db name>.dbo.sysobjects, master.dbo.sysdatabases, @@VERSION`
- `SQL Agent password publicly viewable:  @@version, msdb.dbo.sp_get_sqlagent_properties, sp_helprotect`
- `SQL Agent procedures granted to public:  sp_helprotect`
- `SQLServerAgent password in registry: @@VERSION, <db name>.dbo.sysobjects, master.dbo.sysdatabases`
- `srv_paraminfo buffer overflow in sp_OACreate: @@VERSION`
- `srv_paraminfo buffer overflow in sp_OADestroy: @@VERSION`
- `srv_paraminfo buffer overflow in sp_OAGetProperty: @@VERSION`
- `srv_paraminfo buffer overflow in sp_OAMethod: @@VERSION`
- `srv_paraminfo buffer overflow in sp_OASetProperty: @@VERSION`
- `srv_paraminfo buffer overflow in xp_displayparamstmt: @@VERSION`
- `srv_paraminfo buffer overflow in xp_execresultset: @@VERSION`
- `srv_paraminfo buffer overflow in xp_peekqueue: @@VERSION`
- `srv_paraminfo buffer overflow in xp_printstatements: @@VERSION`
- `srv_paraminfo buffer overflow in xp_proxiedmetadata: @@VERSION`
- `srv_paraminfo buffer overflow in xp_SetSQLSecurity: @@VERSION`
- `srv_paraminfo buffer overflow in xp_showcolv: @@VERSION`
- `srv_paraminfo buffer overflow in xp_sqlagent_monitor: @@VERSION`
- `srv_paraminfo buffer overflow in xp_sqlinventory: @@VERSION`
- `srv_paraminfo buffer overflow in xp_updatecolvbm: @@VERSION`
- `Standard SQL Server authentication allowed: @@VERSION, <db name>.dbo.sysobjects, master.dbo.sysdatabases, master.dbo.xp_loginconfig`
- `Statement permission granted: master.dbo.sysdatabases, exec <db name>.dbo.sp_helprotect`
- `SysAdmin only for CmdExec job steps: @@VERSION, <db name>.dbo.sysobjects, master.dbo.sysdatabases`
- `sysadmin role granted: master.dbo.syslogins`
- `Table to store DTS passwords publicly viewable: <db name>.dbo.sysuser, master.dbo.sysdatabases, exec <db name>.dbo.sp_helprotect`

- Temporary stored procedures bypass permissions: @@VERSION
- UDB broadcast buffer overflow: master.dbo.xp_cmdshell
- Unauthorized object permission grants: <db name>.dbo.sysuser, exec <db name>.dbo.sp_helprotect, master.dbo.sysdatabases
- Windows account name shown as hostname: @@VERSION, master.dbo.xp_loginconfig
- XMLHTTP control allows local file access: <db name>.dbo.sysobjects, master.dbo.sysdatabases, @@VERSION
- xp_cmdshell not removed: <db name>.dbo.sysobjects, master.dbo.sysdatabases replace for xp_cmdshell not removed/not disabled: select object_id()
- xp_controlqueueservice buffer overflow: <db name>.dbo.sysobjects, master.dbo.sysdatabases
- xp_createprivatequeue buffer overflow: @@VERSION, <db name>.dbo.sysobjects, master.dbo.sysdatabases
- xp_createqueue buffer overflow: @@VERSION, master.dbo.sysdatabases, <db name>.dbo.sysobjects
- xp_decodequeuecmd buffer overflow: @@VERSION, <db name>.dbo.sysobjects, master.dbo.sysdatabases
- xp_deleteprivatequeue buffer overflow: @@VERSION, <db name>.dbo.sysobjects, master.dbo.sysdatabases
- xp_deletequeue buffer overflow: @@VERSION, <db name>.dbo.sysobjects, master.dbo.sysdatabases
- xp_dirtree buffer overflow: @@VERSION, <db name>.dbo.sysobjects, master.dbo.sysdatabases
- xp_displayqueuemesgs buffer overflow: @@VERSION, master.dbo.sysdatabases, <db name>.dbo.sysobjects
- xp_dsninfo buffer overflow: <db name>.dbo.sysobjects, @@VERSION, master.dbo.sysdatabases
- xp_mergelineages buffer overflow: @@VERSION, master.dbo.sysdatabases, <db name>.dbo.sysobjects
- xp_oledbinfo buffer overflow: @@VERSION, <db name>.dbo.sysobjects, master.dbo.sysdatabases
- xp_proxiedmetadata buffer overflow: master.dbo.sysdatabases, <db name>.dbo.sysobjects, @@VERSION
- xp_readpkfromqueue buffer overflow: @@VERSION, <db name>.dbo.sysobjects, master.dbo.sysdatabases
- xp_readpkfromvarbin buffer overflow: @@VERSION, <db name>.dbo.sysobjects, master.dbo.sysdatabases
- xp_repl_encrypt buffer overflow: @@VERSION, <db name>.dbo.sysobjects, master.dbo.sysdatabases
- xp_resetqueue buffer overflow: @@VERSION, <db name>.dbo.sysobjects, master.dbo.sysdatabases
- xp_sprintf buffer overflow: @@VERSION
- xp_sqlagent_param buffer overflow: @@VERSION, <db name>.dbo.sysobjects, master.dbo.sysdatabases

- `xp_sqlinventory buffer overflow: @@VERSION, master.dbo.sysdatabases, <db name>.dbo.sysobjects`
- `xp_unpackcab buffer overflow: @@VERSION, <db name>.dbo.sysobjects, master.dbo.sysdatabases`
- `xstatus backdoor: @@VERSION, master.dbo.sysxlogins`

RUNNING THE MICROSOFT SQL SERVER 2000 USER CREATION SCRIPT

Application Security Inc. has written a convenient Microsoft SQL Server 2000 user creation script (`CreateUserSQLServer2k.sql`) which creates an account with the minimum privileges necessary to perform Audits on a Microsoft SQL 2000 instance.

The contents of the `CreateUserSQLServer2k.sql` script follow:

```
--create login

use [master]

EXEC sp_addlogin 'aduser', 'Admin123', 'master'

GO


--add user to each database

EXEC sp_MSforeachdb '

USE [?]

DECLARE @isUpdateable sql_variant


SELECT @isUpdateable = databasePropertyEx(name,''Updateability'') FROM
master.dbo.sysdatabases where databasePropertyEx(name,''Sta-
tus'')=''ONLINE'' and name = ''?''


IF @isUpdateable = ''READ_WRITE''

BEGIN

    EXEC sp_adduser ''aduser''

END'

GO


--assign privileges needed for audit

USE [master]

GO

GRANT EXECUTE ON dbo.xp_loginconfig TO [aduser]

GRANT SELECT ON dbo.syslogins TO [aduser]

GRANT SELECT ON dbo.sysxlogins TO [aduser]
GRANT SELECT ON dbo.sysaltfiles TO [aduser]
GRANT SELECT ON dbo.sysdatabases TO [aduser]
GRANT SELECT ON dbo.sysconfigures TO [aduser]
GRANT SELECT ON dbo.syscurconfigs TO [aduser]
GRANT SELECT ON dbo.sysservers TO [aduser]
GRANT SELECT ON dbo.sysmembers TO [aduser]
GRANT SELECT ON dbo.sysprotects TO [aduser]
GRANT SELECT ON dbo.spt_values TO [aduser]
GRANT EXECUTE ON sp_helpreplicationdboption TO [aduser]
GRANT EXECUTE ON sp_helpsrvrolemember TO [aduser]
GRANT EXECUTE ON sp_helprolemember TO [aduser]
GRANT SELECT ON dbo.sysoledbusers TO [aduser]

EXEC sp_MSforeachdb '
DECLARE @isUpdateable sql_variant

SELECT @isUpdateable = databasePropertyEx(name,''Updateability'') FROM
master.dbo.sysdatabases where databasePropertyEx(name,''Sta-
tus'')=''ONLINE'' and name = ''?''

IF @isUpdateable = ''READ_WRITE''
BEGIN
          GRANT EXECUTE ON [?].dbo.sp_helprotect TO [aduser]
          GRANT EXECUTE ON [?].dbo.sp_helpuser TO [aduser]
END
'

EXEC sp_MSforeachdb '
USE [?]

DECLARE @isUpdateable sql_variant

SELECT @isUpdateable = databasePropertyEx(name,''Updateability'') FROM
master.dbo.sysdatabases where databasePropertyEx(name,''Sta-
tus'')=''ONLINE'' and name = ''?''

IF @isUpdateable = ''READ_WRITE''
```

```
BEGIN
          GRANT SELECT ON dbo.sysusers TO [aduser]
          GRANT SELECT ON dbo.sysobjects TO [aduser]
          GRANT SELECT ON dbo.syscomments TO [aduser]
END
'

use [msdb]
GRANT SELECT ON dbo.sysjobs TO [aduser]
GRANT SELECT ON dbo.sysjobhistory TO [aduser]

print 'all done.'
```

RUNNING THE MICROSOFT SQL SERVER 2000 WITH SYSADMIN USER CREATION SCRIPT

Application Security Inc. has written a convenient **Microsoft SQL Server 2000 user creation script** (`CreateUserSQLServer2kwithSA.sql`) which creates an account with the minimum privileges necessary to perform Audits on a Microsoft SQL 2000 instance, and adds it to the SYSADMIN server role.

The contents of the `CreateUserSQLServer2kwithSA.sql` script follow:

```
USE master
GO
EXEC sp_addlogin 'aduser', 'Admin123'
GO

EXEC sp_MSforeachdb '
USE [?]
DECLARE @isUpdateable sql_variant

SELECT @isUpdateable = databasePropertyEx(name,''Updateability'') FROM
master.dbo.sysdatabases where
databasePropertyEx(name,''Status'')=''ONLINE'' and name = ''?''

IF @isUpdateable = ''READ_WRITE''
BEGIN EXEC sp_grantdbaccess ''aduser'', ''aduser''
END'
GO

EXEC sp_addsrvrolemember "aduser", SYSADMIN
```

MICROSOFT SQL SERVER 2005 AND MICROSOFT SQL SERVER 2008 AUDIT PRIVILEGES

Important: Application Security Inc. wrote a convenient **Microsoft SQL Server 2005** and **Microsoft SQL Server 2008 user creation script** (`CreateUserSQLServer2k52k8PublicRevoked.sql`) that creates an account with the minimum privileges necessary to perform an Audit on a Microsoft SQL Server instance. If you want to run this script, just make sure whatever account you use to conduct your Audit has at least the `SELECT` privileges listed in the script. For more information, see *Running the Microsoft SQL Server 2005 and 2008 User Creation Script*.

Any Audit check for Microsoft SQL Server 2005 and Microsoft SQL Server 2008 queries the following views:

- `sys.databases`
- `sys.configurations`
- `sys.server_principals`
- `sys.server_role_members`

In Microsoft SQL Server 2005 and Microsoft SQL Server 2008 the public group can select from these views but, due to metadata visibility concept, DbProtect Vulnerability Assessment may not return all records. For this reason, each of the checks listed below requires the following permissions in order to retrieve data: `VIEW DEFINITION`, `VIEW ANY DEFINITION`, and `CONTROL SERVER`.

In addition, you **must** have permission to select from `system table: select all rows from master.sys.database_permissions, <dbname>.sys.system_objects views` which implies `VIEW DEFINITION` on database scope permission.

For the check `Symmetric Keys: encrypting mechanism` to work properly, the auditing user should have access to all keys. The user must be a privileged user have been granted access to all the keys. You can use one of the following statements to grant access:

```
for every database
```

```
GRANT VIEW DEFINITION TO [aduser]
```

or

```
in master database
```

```
GRANT VIEW ANY DEFINITION TO [aduser]
```

In addition, certain Microsoft SQL Server 2005 and 2008 DISA-STIG Database Security Configuration checks require you to be a member of the `sysadmin` fixed server role or the `db_owner` fixed database role on the publication database. The following table provides specific information about which checks require which roles (and why):

Microsoft SQL Server 205 and 2008 DISA-STIG checks:	Use:	To run these checks, you must be a member of:
`DBMS replication account privileges`	Replication system stored procedures.	The `sysadmin` fixed server role or the `db_owner` fixed database role on the publication database
`Replication snapshot folder protection`		

Below is a list of DbProtect Vulnerability Assessment **checks** used to run a Microsoft SQL Server 2005 or and Microsoft SQL Server 2008 Audit, including the tables and views they need permission to access in order to function properly:

- `Agent XPs enabled: select from sys.configurations view.`
- `Application user access to external objects: select from <dbname>.sys.objects, <dbname>.sys.database_permissions.`
- `Asymmetric Keys: private key encryption type: select from master.dbo.sysdatabases, select from <dbname>.sys.asymmetric_keys, VIEW DEFINITION on database scope permission.`
- `Auditing of failed logins: master.dbo.xp_loginconfig.`
- `Auditing of failed/successful logins: execute xp_loginconfig.`
- `Audit trace status: select from fn_trace_getinfo, fn_trace_geteventinfo.`
- `Blank password checks: select password_hash column of sys.sql_logins for all sql logins which implies CONTROL SERVER permission.`
- `BUILTIN\Administrators not removed: select all rows from sys.server_principals view which implies VIEW ANY DEFINITION permission.`
- `C2 Audit Mode: select from sys.configurations view.`
- `CLR objects allowed: select from sys.configurations view.`
- `Common criteria compliance disabled: select from sys.configurations view.`
- `Database job/batch queue monitoring: select from master.sys.procedures, select name, job_id columns from msdb.dbo.sysjobs and select job_id column from msdb.dbo.sysjobhistory.`
- `Database Master Key: access control: select from master.dbo.sysdatabases, <dbname>.sys.database_principals, <dbname>.sys.database_permissions.`

- `Database Master Key: encryption password: select from master.dbo.sysdatabases,<dbname>.sys.key_encryptions,<dbname>.sys.symmetric_keys, VIEW DEFINITION on database scope permission.`
- `Database Master Key: is_master_key_encrypted_by_server: select from sys.databases.`
- `Database Master Key: password storage: select from sys.master_key_passwords.`
- `Database ownership chaining not disabled: select from sys.configurations view.`
- `DBA OS privilege assignment: execute sp_helpsrvrolemember.`
- `DBMS account password expiration: select from sys.sql_logins.`
- `DBMS administration OS accounts: execute sp_helpsrvrolemember.`
- `DBMS audit log backups: select from fn_trace_getinfo.`
- `DBMS audit record access: select from sys.server_permissions, master.dbo.syslogins and master.dbo.sysusers, execute sp_helpsrvrolemember.`
- `DBMS Password Policy Enforced: execute xp_loginconfig, select from sys.sql_logins.`
- `DBMS remote system credential use and access: select from dbo.sysservers, sys.linked_logins.`
- `DBMS services dedicated custom account: Registry access.`
- `DBMS software file backups: Registry access.`
- `DBMS dedicated software directory and partition: Registry access.`
- `DBMS network port, protocol, and services (PPS) configuration: Registry access*.`

Note: To learn more about enabling registry access for Microsoft SQL Server 2005 and 2008, see *Registry Access for Microsoft SQL Server 2000, 2005, and 2008*.

- `Dedicated data file directories: select from sys.master_files, sys.databases, Registry access*.`
- `Default password for well-known login: makes connection attempts.`
- `Default Trace Disabled: select from sys.configurations view.`
- `DTS package password publicly viewable: select all rows from msdb.sys.database_permissions, sys.types, sys.all_objects, sys.certificates, sys.fulltext_catalogs, sys.routes, sys.remote_service_bindings, sys.services, sys.service_contracts, sys.service_message_types, sys.xml_schema_collections, sys.assemblies views which implies VIEW DEFINITION on database scope permission.`
- `DTS package procedures granted to public: select from msdb.sys.database_permissions view.`
- `DTS procedures granted to PUBLIC: select from msdb.sys.database_principals, msdb.sys.database_permissions.`
- `Easily-guessed password checks: select password_hash column of sys.sql_logins for all sql logins which implies CONTROL SERVER permission.`
- `Encryption of DBMS sensitive data in transit: Registry access.`

- Error logs can be overwritten: Registry access.
- Event forwarding not disabled: Registry access.

Note: To learn more about enabling registry access for Microsoft SQL Server 2005 and 2008, see *Registry Access for Microsoft SQL Server 2000, 2005, and 2008*.

- Fixed server role granted: select all rows from sys.server_principals, sys.server_role_members views which implies VIEW ANY DEFINITION permission.
- Global temporary stored proc exists: select from tempdb.sys.all_objects.
- Guest user exists in database: select all rows from sys.databases and <dbname>.sys.database_principals, and <dbname>.sys.database_permissions views.
- Integration Services OS account least privileges: Windows Management Instrumentation (WMI).
- Latest service pack/hot fix not applied: uses @@version - requires no privileges.
- Linked Servers Definitions: select from sys.servers view. Permissions granted on sp_add_dtspackage: select all rows from msdb.sys.database_permissions, sys.types, sys.all_objects, sys.certificates, sys.fulltext_catalogs, sys.routes, sys.remote_service_bindings, sys.services, sys.service_contracts, sys.service_message_types, sys.xml_schema_collections, sys.assemblies views which implies VIEW DEFINITION on database scope permission.
- Lumigent Log Explorer buffer overflow: select all rows from master.sys.objects view which implies VIEW DEFINITION on master database permission.
- Not using NTFS partition: execute xp_instance_regread.
- OLEDB ad hoc queries allowed: select from sys.configurations view, Registry access.

Note: To learn more about enabling registry access for Microsoft SQL Server 2005 and 2008, see *Registry Access for Microsoft SQL Server 2000, 2005, and 2008*.

- Password same as login name: select password_hash column of sys.sql_logins view for all sql logins which implies CONTROL SERVER permission.
- Permission grantable: select all rows from sys.databases, <dbname>.sys.database_permissions views which implies VIEW DEFINITION on database scope permission.
- Permission on OLE automation procs: select all rows from master.sys.database_permissions view which implies VIEW DEFINITION on database scope permission.
- Permission on registry extended proc: select all rows from master.sys.database_permissions view which implies VIEW DEFINITION on database scope permission.

- Permission to select from system table: select all rows from master.sys.database_permissions view which implies VIEW DEFINITION on database scope permission.
- Permissions granted on xp_cmdshell: select all rows from master.sys.database_permissions view which implies VIEW DEFINITION on database scope permission.
- Permissions granted to PUBLIC: select all rows from sys.databases, <dbname>.sys.database_permissions views.
- Permissions granted to user: select all rows from sys.databases, <dbname>.sys.database_permissions, sys.types, sys.all_objects, sys.certificates, sys.fulltext_catalogs, sys.routes, sys.remote_service_bindings, sys.services, sys.service_contracts, sys.service_message_types, sys.xml_schema_collections, sys.assemblies views which implies VIEW DEFINITION on database scope permission.
- Permissions on files: execute xp_instance_regread.
- Protection of DBMS asymmetric encryption keys: select from master.dbo.sysdatabases, <dbname>.sys.asymmetric_keys, <dbname>.sys.database_principals, <dbname>.sys.database_permissions, VIEW DEFINITION on database scope permission.
- Proxy account subsystem privileges: select subsystem, subsystem_id columns from msdb.dbo.syssubsystems.
- Registry extended proc not removed: select from master.sys.system_objects view.
- Registry permissions: execute xp_instance_regread.
- Remote access allowed: select from sys.configurations view.
- Remote admin connections allowed: select from sys.configurations view.
- Sample database not removed: select all rows from sys.databases view.
- Service Broker Endpoints exist: select from sys.service_broker_endpoints.
- Service runs as LocalSystem: execute xp_instance_regread.
- SMO and DMO XPs enabled: select from sys.configurations view.
- SQL Server Agent account user rights: Windows Management Instrumentation (WMI).
- SQL Server Agent proxy accounts are not dedicated: execute sp_enum_login_for_proxy.
- SQL Server component service account user rights: Windows Management Instrumentation (WMI).
- SQL Server file permissions: Registry access*, OS access (Permission to read files in the installation directory of the database) also Windows Management Instrumentation (WMI).
- SQL Server service account: Windows Management Instrumentation (WMI).
- SQL Server service account user rights: Windows Management Instrumentation (WMI).

- Standard SQL Server authentication allowed: execute xp_instance_regread.
- Statement permission granted: select all rows from sys.databases, <dbname>.sys.database_permissions views which implies VIEW DEFINITION on database scope permission.
- Symmetric Keys: allowed encryption algorithms: select from master.dbo.sysdatabases, <dbname>.sys.symmetric_keys, VIEW DEFINITION on database scope permission.
- Symmetric Keys: encrypting mechanism: select from master.dbo.sysdatabases, <dbname>.sys.symmetric_keys, <dbname>.sys.key_encryptions, VIEW DEFINITION on database scope permission.
- sysadmin role granted: select all rows from sys.server_principals, sys.server_role_members views which implies VIEW ANY DEFINITION permission.
- Unauthorized object permission grants: select all rows from sys.databases, <dbname>.sys.database_permissions, sys.types, sys.all_objects, sys.certificates, sys.fulltext_catalogs, sys.routes, sys.remote_service_bindings, sys.services, sys.service_contracts, sys.service_message_types, sys.xml_schema_collections, sys.assemblies views which implies VIEW DEFINITION on database scope permission.
- XML web service access: select from sys.http_endpoints.
- Web assistant procedures enabled: select from sys.configurations view.
- xp_cmdshell not removed/not disabled: select from sys.configurations view.

CREDENTIALS FOR MICROSOFT SQL SERVER AUDITS

If you are unable to Audit a **Microsoft SQL Server** database using Windows Authentication, you may be using an account that lacks the proper **credentials**. There are a number of different ways to supply the proper credentials for Microsoft SQL Server. The appropriate method depends on your circumstances.

The following table explains how to change your credentials under different scenarios when you attempt to perform an Audit on the Microsoft SQL Server TARGET machine from another machine (HOST). Once you have valid credentials on the target HOST, you should be able to perform your Audit.

Part	If	Then
1	TARGET and HOST are in the same or trusted domain.	• If you are logged in to HOST as a user that has Administrative access to TARGET, you do not need to supply additional credentials. Or... • If you are logged in as user without Administrative access, you will need to supply TARGET’s sa credentials.

Part	If	Then
2	`TARGET` is in WORKGROUP_X and `HOST` is in DOMAIN_A Or... `TARGET` is in WORKGROUP_X and `HOST` is in WORKGROUP_Y Or... `TARGET` is in WORKGROUP_X and `HOST` is in WORKGROUP_X	• You can supply sa credentials in DbProtect Vulnerability Assessment. Or... • You can create a local user on `TARGET` and a local user on `HOST` with matching user names and passwords. **Note:** You **cannot** use Domain names here. Or... • Select the **Properties** branch option **Connect to Microsoft SQL Servers via Named Pipes** in the DbProtect Vulnerability Assessment **Properties** branch, then use the Net Use technique to establish credentials on `TARGET`. You **must** select this option to force DbProtect Vulnerability Assessment to use named pipes. You must check this option if you want to Audit a Microsoft SQL Server database (using Windows Authentication) against a machine on a different or untrusted domain. **Additional steps are required.** For more information, see *Auditing Microsoft SQL Server (Using Windows Authentication) Against a Machine on a Different or Untrusted Domain*. To use the Net Use technique: -Open a command prompt. -Enter the `net use` command to log in to the target server with valid credentials. -The command should adhere to the following format: `net use \\computerIP /user:[domainname\]username` -DbProtect Vulnerability Assessment prompts you for a valid password on the `TARGET`. -Verify access by re-entering `net use`. **Note:** DbProtect Vulnerability Assessment does **not** support Pen Testing any Microsoft SQL Server instances which use named pipes for connection.

Part	If	Then
3	TARGET is in DOMAIN_A and HOST is either in an untrusted DOMAIN_B or in WORKGROUP_X	- You can use any of the methods listed in Part 2, above. Or... - You can add HOST to DOMAIN_A.

RUNNING THE MICROSOFT SQL SERVER 2005 AND 2008 USER CREATION SCRIPT

Application Security Inc. has written a convenient **Microsoft SQL Server 2005** and **Microsoft SQL Server 2008 user creation script** (CreateUserSQLServer2k52k8PublicRevoked.sql) which creates an account with the minimum privileges necessary to perform Audits on either a Microsoft SQL Server 2005 or a Microsoft SQL Server 2008 instance.

Caution! If you want to run this script, make sure whatever account you use to conduct your Audit has at least the SELECT privileges listed in the script (see below).

The contents of the CreateUserSQLServer2k52k8PublicRevoked.sql script follow:

```
CREATE LOGIN [aduser] WITH PASSWORD=N'Admin123',
DEFAULT_DATABASE=[master]

GO


EXEC sp_MSforeachdb '

USE [?]

DECLARE @isUpdateable sql_variant


SELECT @isUpdateable = databasePropertyEx(name,"Updateability") FROM
master.dbo.sysdatabases where
databasePropertyEx(name,"Status")="ONLINE" and name = "?"


IF @isUpdateable = "READ_WRITE"

BEGIN

    CREATE USER [aduser] FOR LOGIN [aduser] WITH DEFAULT_SCHEMA=[dbo]

END'

GO


USE [master]
```

```
GO
GRANT EXECUTE ON dbo.xp_loginconfig TO [aduser]
GRANT SELECT ON dbo.syslogins TO [aduser]
GRANT SELECT ON dbo.sysdatabases TO [aduser]
GRANT SELECT ON dbo.sysconfigures TO [aduser]
GRANT SELECT ON dbo.syscurconfigs TO [aduser]
GRANT SELECT ON dbo.syscharsets TO [aduser]
GRANT SELECT ON sys.configurations TO [aduser]
GRANT SELECT ON sys.server_principals TO [aduser]
GRANT SELECT ON sys.server_role_members TO [aduser]
GRANT ALTER TRACE TO [aduser]
GRANT SELECT ON sys.fn_trace_getinfo TO [aduser]


EXEC sp_MSforeachdb '
DECLARE @isUpdateable sql_variant

SELECT @isUpdateable = databasePropertyEx(name,"Updateability") FROM
master.dbo.sysdatabases where
databasePropertyEx(name,"Status")="ONLINE" and name = "?"

IF @isUpdateable = "READ_WRITE"
BEGIN
    GRANT EXECUTE ON [?].dbo.sp_helprotect TO [aduser]
END'


GRANT SELECT ON sys.servers TO [aduser]
GRANT EXECUTE ON dbo.sp_helpsrvrolemember TO [aduser]
GRANT SELECT ON dbo.fn_trace_geteventinfo TO [aduser]
GRANT SELECT ON dbo.fn_trace_getinfo TO [aduser]
GRANT SELECT ON sys.databases TO [aduser]
GRANT SELECT ON sys.master_key_passwords TO [aduser]
GRANT SELECT ON sys.sql_logins TO [aduser]
GRANT SELECT ON sys.master_files TO [aduser]
GRANT SELECT ON sys.procedures TO [aduser]
GRANT SELECT ON sys.server_permissions TO [aduser]
GRANT SELECT ON sys.all_objects TO [aduser]
GRANT SELECT ON sys.certificates TO [aduser]
GRANT SELECT ON sys.fulltext_catalogs TO [aduser]
GRANT SELECT ON sys.routes TO [aduser]
GRANT SELECT ON sys.remote_service_bindings TO [aduser]
GRANT SELECT ON sys.services TO [aduser]
GRANT SELECT ON sys.service_contracts TO [aduser]
GRANT SELECT ON sys.service_message_types TO [aduser]
GRANT SELECT ON sys.xml_schema_collections TO [aduser]
GRANT SELECT ON sys.assemblies TO [aduser]
GRANT SELECT ON sys.http_endpoints TO [aduser]
GRANT SELECT ON dbo.sysservers TO [aduser]
GRANT SELECT ON dbo.sysservers TO [aduser]
GRANT SELECT ON sys.linked_logins  TO [aduser]
GRANT SELECT ON sys.service_broker_endpoints TO [aduser]
GRANT SELECT ON sys.credentials TO [aduser]
GRANT EXECUTE ON dbo.sp_helppublication TO [aduser]
GRANT EXECUTE ON dbo.sp_helpmergepublication TO [aduser]
GRANT EXECUTE ON dbo.sp_helpmergesubscription TO [aduser]
GRANT EXECUTE ON dbo.sp_helpsubscription TO [aduser]
GRANT EXECUTE ON dbo.sp_help_publication_access TO [aduser]
GRANT EXECUTE ON dbo.sp_helpuser TO [aduser]
GRANT SELECT ON sys.dm_os_cluster_nodes TO [aduser]
GRANT SELECT ON sys.database_files TO [aduser]
GRANT EXECUTE ON dbo.sp_helpreplicationdboption TO [aduser]
GRANT EXECUTE ON dbo.sp_helprolemember TO [aduser]
GRANT SELECT ON dbo.sysprocesses TO [aduser]
grant view any definition to [aduser]
GRANT VIEW SERVER STATE TO [aduser]
GO
```

```
USE [msdb]

GO

GRANT EXECUTE ON dbo.sp_get_sqlagent_properties TO [aduser]

GRANT SELECT ON dbo.sysproxysubsystem TO [aduser]

GRANT SELECT ON dbo.sysproxies TO [aduser]

GRANT EXECUTE ON dbo.sp_enum_login_for_proxy TO [aduser]

GRANT SELECT ON dbo.sysjobs ([name],[job_id]) TO [aduser]

GRANT SELECT ON dbo.sysjobhistory ([job_id]) TO [aduser]

GRANT SELECT ON dbo.syssubsystems ([subsystem],[subsystem_id]) TO
[aduser]

GRANT SELECT ON [dbo].[sysjobsteps] ([proxy_id],[subsystem], [job_id])
TO [aduser]

GRANT SELECT ON dbo.sysjobs TO [aduser]

GO



EXEC sp_MSforeachdb '

USE [?]

DECLARE @isUpdateable sql_variant

SELECT @isUpdateable = databasePropertyEx(name,"Updateability") FROM
master.dbo.sysdatabases where
databasePropertyEx(name,"Status")="ONLINE" and name = "?"


IF @isUpdateable = "READ_WRITE"

BEGIN

GRANT SELECT ON dbo.sysusers TO [aduser]

GRANT SELECT ON dbo.sysobjects TO [aduser]

GRANT SELECT ON dbo.syscomments TO [aduser]

GRANT VIEW DEFINITION TO [aduser]

GRANT SELECT ON sys.database_permissions TO [aduser]

GRANT SELECT ON sys.objects TO [aduser]

GRANT SELECT ON sys.asymmetric_keys TO [aduser]

GRANT SELECT ON sys.database_principals TO [aduser]

GRANT SELECT ON sys.key_encryptions TO [aduser]

GRANT SELECT ON sys.symmetric_keys TO [aduser]

GRANT SELECT ON sys.types TO [aduser]
GRANT SELECT ON sys.sysmembers TO [aduser]
GRANT SELECT ON sys.database_role_members TO [aduser]
GRANT SELECT ON sys.schemas TO [aduser]
GRANT SELECT ON sys.system_objects TO [aduser]
END'
GO
```

REGISTRY ACCESS FOR MICROSOFT SQL SERVER 2000, 2005, AND 2008

Some **Microsoft SQL Server 2000**, **2005**, and **2008** Audit privileges require you to have **remote registry access** in order to perform Audits on Microsoft SQL Server instances. These required Audit privileges are listed in:

- *Microsoft SQL Server 2000 and MSDE Audit Privileges* (for all applicable **Microsoft SQL Server 2000** Audit privileges)
- *Microsoft SQL Server 2005 and Microsoft SQL Server 2008 Audit Privileges* (for all applicable **Microsoft SQL Server 2005 and 2008** Audit privileges).

Depending on your version of Microsoft SQL Server 2000, 2005, and 2008 (and whether you are using Microsoft SQL Server Authentication or Windows Authentication), you can get the remote registry value in either of the following two ways:

4. Via the `xp_regread` extended stored procedure (explained in the following table).

If your version of Microsoft SQL Server is:	And you are using:	Detail
Microsoft SQL Server 2000 (service pack **prior** to SP4)	Microsoft SQL Server Authentication	Grant `execute` on `xp_regread` to the DbProtect Vulnerability Assessment user or the `Public` role.
	Windows Authentication	Grant `execute` on `xp_regread` to the Windows user or to the `Public` role, and permissions on the key being accessed.

If your version of Microsoft SQL Server is:	And you are using:	Detail
Microsoft SQL Server 2000 SP4 and Microsoft SQL Server 2005 or 2008	Microsoft SQL Server Authentication	Grant execute on xp_regread to the DbProtect Vulnerability Assessment user or the Public role.
	Windows Authentication	Grant execute on xp_regread to Windows user or the Public role, and permissions on the key being accessed.
	Microsoft SQL Server Authentication or Windows Authentication	Although authentication mode (i.e., Microsoft SQL Server Authentication or Windows Authentication) is used, DbProtect Vulnerability Assessment requires an entry on the target (HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft SQL Server\<INSTANCE>\MSSQLServer\ExtendedProcedures\Xp_regread Allowed Paths) of the requested registry subkey. (Reference: http://support.microsoft.com/kb/887165) Since the Microsoft SQL Server installation program pre-populates the Xp_regread Allowed Paths registry entry with the extended stored procedures that Microsoft SQL Server can access, you only need to add the following registry entries: • HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft SQL Server\Instance Names\SQL • HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSSQLServerOLAPService • HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ReportServer

5. Get the remote registry value via the Windows Remote Registry API, and provide a valid Windows account with remote registry access.

MySQL Audit Privileges

Note: For more information on MySQL Server OS check requirements, see *Operating System Considerations (for Audits).*

To conduct a full **MySQL** Audit, you need the following **privileges**. Make sure the account you are using has rights to use the following tables and views:

- `Anonymous user exists: SELECT on user table`
- `Blank account passwords: SELECT on user table`
- `Blank root password: SELECT on user table`
- `Default passwords for test accounts: SELECT on user table`
- `Easily-guessed account passwords: SELECT on user table`
- `Easily-guessed root password: SELECT on user table`
- `FILE privileges granted: SELECT on user table`
- `General log file not enabled: execute SHOW VARIABLES`
- `Password for user same as username: SELECT on user table`
- `Permissions grantable: SELECT on the user table, SELECT on the db table, SELECT on the host table, SELECT on the tables_priv table, and SELECT on the procs_priv table`
- `Permissions on GRANT tables: SELECT on the user table, SELECT on the db table, SELECT on the host table, SELECT on the tables_priv table, SELECT on the procs_priv table, and SELECT on the columns_priv' table`
- `Permissions on user table: SELECT on the user table, SELECT on the db table, SELECT on the host table, SELECT on the tables_priv table, and SELECT on the columns_priv table.`
- `PROCESS privileges granted: SELECT on user table`
- `Sample database not removed: execute SHOW DATABASES`
- `SSL encryption not enabled: execute SHOW VARIABLES`
- `Grant SELECT on procs_priv`

Note: The `Grant SELECT on procs_priv` privilege is only required on the `Permissions on GRANT tables` and `Permissions grantable` MySQL Audit checks on MySQL 5.0 and greater.

MYSQL CHECKS

MySQL Audit

- `Easily-guessed root password`
- `Easily-guessed passwords`
- `Blank password`
- `Blank root password`
- `Universal access`
- `SSL is enabled`
- `Grant tables privileges`

- Ensure sample databases have been removed
- Permissions on [User] table
- Permissions granted directly to user
- Logging not enabled
- MySQL mysqld Privilege Escalation Vulnerability
- MySQL libmysqlclient Library Read_One_Row Buffer Overflow Vulnerability
- MySQL COM_CHANGE_USER Password Memory Corruption Vulnerability
- MySQL Double Free Heap Corruption Vulnerability
- MySQL COM_CHANGE_USER Password Length Account Compromise Vulnerability
- MySQL libmysqlclient Library Read_Rows Buffer Overflow Vulnerability
- MySQL COM_TABLE_DUMP Memory Corruption Vulnerability
- MySQL COM_TABLE_DUMP Memory Corruption Vulnerability
- MySQL Bind Address Not Enabled Weak Default Configuration Vulnerability
- MySQL Null Root Password Weak Default Configuration Vulnerability
- WinMySQLadmin Plain Text Password Storage Vulnerability
- MySQL Root Operation Symbolic Link File Overwriting Vulnerability
- MySQL SHOW GRANTS Password Hash Disclosure Vulnerability
- MySQL Local Buffer Overflow Vulnerability
- MySQL Authentication Algorithm Vulnerability
- MySQL GRANT Global Password Changing Vulnerability
- MySQL Unauthenticated Remote Access Vulnerability
- Permissions on GRANT tables
- Permissions grantable

Note: The `Grant SELECT on procs_priv` privilege is only required on the `Permissions on GRANT tables` and `Permissions grantable` MySQL Audit checks on MySQL 5.0 and greater.

MySQL Pen Test

- Easily-guessed root password
- Easily-guessed password
- Blank password
- Blank root password
- MySQL mysqld Privilege Escalation Vulnerability
- MySQL libmysqlclient Library Read_One_Row Buffer Overflow Vulnerability
- MySQL COM_CHANGE_USER Password Memory Corruption Vulnerability

- MySQL Double Free Heap Corruption Vulnerability
- MySQL COM_CHANGE_USER Password Length Account Compromise Vulnerability
- MySQL libmysqlclient Library Read_Rows Buffer Overflow Vulnerability
- MySQL COM_TABLE_DUMP Memory Corruption Vulnerability
- MySQL COM_TABLE_DUMP Memory Corruption Vulnerability
- MySQL Bind Address Not Enabled Weak Default Configuration Vulnerability
- MySQL Null Root Password Weak Default Configuration Vulnerability
- WinMySQLadmin Plain Text Password Storage Vulnerability
- MySQL Root Operation Symbolic Link File Overwriting Vulnerability
- MySQL SHOW GRANTS Password Hash Disclosure Vulnerability
- MySQL Local Buffer Overflow Vulnerability
- MySQL Authentication Algorithm Vulnerability
- MySQL GRANT Global Password Changing VulnerabilityMySQL
- MySQL Unauthenticated Remote Access Vulnerability

Oracle Audit Privileges and User Creation Script

Note: For more information on Oracle OS check requirements, see *Operating System Considerations (for Audits)* and *Appendix O: Oracle Critical Patch Update Detection* in the *AppDetectivePro User's Guide.*

This topic consists of the following sub-topics:

- *Oracle Audit Privileges*
- *Running the Oracle User Creation Script.*

ORACLE AUDIT PRIVILEGES

To conduct a full **Oracle** Audit, you need the following **privileges**. Make sure the account you are using has rights to use the following tables, views, and functions:

- $PWFILE_USERS
- ALTER USER username TEMPORARY TABLESPACE TEMP
- DBA_OBJ_AUDIT_OPTS
- DBA_OBJECTS
- DBA_PROFILES
- DBA_ROLES
- DBA_ROLE_PRIVS
- DBA_STMT_AUDIT_OPTS
- DBA_SYS_PRIVS
- DBA_TABLES

- DBA_TAB_PRIVS
- DBA_USERS
- DBA_VIEWS
- DBMS_UTILITY.PORT_STRING
- PRODUCT_COMPONENT_VERSION
- SYS.LINK$
- SYS.USER$
- SYS.REGISTRY$HISTORY
- SYS.DBA_DB_LINKS
- SYS.DBA_LIBRARIES
- SYS.DBA_OBJECTS
- SYS.DBA_ROLE_PRIVS
- SYS.DBA_SOURCE
- SYS.DBA_USERS
- SYS.DBA_DB_LINKS
- SYS.V_$INSTANCE
- SYS.DBA_TS_QUOTAS
- V$LOG
- V$PWFILE_USERS
- V$VERSION
- V_$DATABASE
- V_$DATAFILE
- V_$LOGFILE
- V_$SESSION
- V_$PARAMETER (DbProtect Vulnerability Assessment selects from V$PARAMETER but you must grant SELECT on V_$PARAMETER)

Note: The user account must have the CREATE SESSION privilege. In addition, the user account used for Audits needs a temporary table space assigned, which you can create with the following command: ALTER USER username TEMPORARY TABLESPACE TEMP

The following **script** creates an **account** with the **minimum privileges** necessary to perform a Security Audit on an Oracle SID. Be sure that whatever account is used to conduct your Audit has at least the SELECT privileges listed below:

```
DROP USER aduser cascade;

CREATE USER aduser IDENTIFIED BY AD123;

GRANT SELECT ON SYS.DBA_DB_LINKS TO aduser;

GRANT SELECT ON SYS.DBA_DATA_FILES TO aduser;

GRANT SELECT ON SYS.DBA_OBJECTS TO aduser;

GRANT SELECT ON SYS.DBA_OBJ_AUDIT_OPTS TO aduser;
GRANT SELECT ON SYS.DBA_PROCEDURES TO aduser;
GRANT SELECT ON SYS.DBA_PROFILES TO aduser;
GRANT SELECT ON SYS.DBA_ROLES TO aduser;
GRANT SELECT ON SYS.DBA_ROLE_PRIVS TO aduser;
GRANT SELECT ON SYS.DBA_STMT_AUDIT_OPTS TO aduser;
GRANT SELECT ON SYS.DBA_SYS_PRIVS TO aduser;
GRANT SELECT ON SYS.DBA_TABLES TO aduser;
GRANT SELECT ON SYS.DBA_INDEXES TO aduser;
GRANT SELECT ON SYS.DBA_TAB_PRIVS TO aduser;
GRANT SELECT ON SYS.DBA_TS_QUOTAS TO aduser;
GRANT SELECT ON SYS.DBA_USERS TO aduser;
GRANT SELECT ON SYS.DBA_SOURCE TO aduser;
GRANT SELECT ON SYS.DBA_VIEWS TO aduser;
GRANT SELECT ON SYS.PRODUCT_COMPONENT_VERSION TO aduser;
GRANT SELECT ON SYS.LINK$ TO aduser;
GRANT SELECT ON SYS.USER$ TO aduser;
GRANT SELECT ON SYS.V_$PARAMETER TO aduser;
GRANT SELECT ON SYS.V_$LOG TO aduser;
GRANT SELECT ON SYS.V_$PWFILE_USERS TO aduser;
GRANT SELECT ON SYS.V_$INSTANCE TO aduser;
GRANT SELECT ON SYS.V_$DATABASE TO aduser;
GRANT SELECT ON SYS.DBA_PRIV_AUDIT_OPTS TO aduser;
GRANT SELECT ON SYS.DBA_REPCATLOG TO aduser;
GRANT SELECT ON SYS.DEFPROPAGATOR TO aduser;
GRANT SELECT ON SYS.V_$DATAFILE TO aduser;
GRANT SELECT ON SYS.V_$LOGFILE TO aduser;
GRANT SELECT ON SYS.V_$SESSION TO aduser;
GRANT SELECT ON SYS.REGISTRY$HISTORY TO aduser;
GRANT CREATE SESSION TO aduser;
grant javasyspriv to aduser;
grant create procedure to aduser;
```

The following is a list of **checks** within the DbProtect Vulnerability Assessment for Oracle Security Audit, and the tables and views which they need permission to in order to function properly:

- `_TRACE_FILES_PUBLIC undocumented configuration parameter is NOT set to FALSE`

Note: This check requires SYSDBA privileges, and, because of this, it is not part of any built-in Policies.

- `Account associated with DEFAULT profile: DBA_USERS`
- `Account granted the predefined role CONNECT: DBA_ROLE_PRIVS`
- `Account granted the predefined role DBA:  DBA_ROLE_PRIVS`
- `Account granted the predefined role RESOURCE:  DBA_ROLE_PRIVS`
- `Accounts with SYSTEM as default tablespace:  DBA_USERS`
- `ANSI join syntax bypasses object privileges: PRODUCT_COMPONENT_VERSION`
- `ANY system privilege applies to data dictionary:  V$PARAMETER`
- `Auditing Not Enabled:  V$PARAMETER`
- `Auditing of CREATE SESSION not enabled:  DBA_STMT_AUDIT_OPTS`
- `BFILENAME buffer overflow (Verify version):PRODUCT_COMPONENT_VERSION`
- `Brute-force database password:  DBA_USERS`
- `Brute-force role password:  SYS.USER$`
- `Cleartext password stored with database link:  SYS.LINK$`
- `Create library privilege:  DBA_SYS_PRIVS, PRODUCT_COMPONENT_VERSION`
- `Database link buffer overflow (Verify version):PRODUCT_COMPONENT_VERSION`
- `Database user allows remote authentication:  DBA_USERS, V$PARAMETER`
- `DBLINK_ENCRYPT_LOGIN not enabled:  SYS.LINK$, V$PARAMETER`
- `DBMS dedicated software directory and partition: V$DATAFILE, V$LOGFILE, V$PARAMETER`
- `Default database password: DBA_USERS`
- `Easily-guessed database password:  DBA_USERS`
- `Easily-guessed role password:  SYS.USER$`
- `Expired password:  DBA_USERS, PRODUCT_COMPONENT_VERSION`
- `Kick Listener DoS (Verify version):  PRODUCT_COMPONENT_VERSION`
- `Label Security row label improperly assigned: PRODUCT_COMPONENT_VERSION`
- `Label Security SQL predicates bypassed:  PRODUCT_COMPONENT_VERSION`

- Label Security unauthorized higher level read: PRODUCT_COMPONENT_VERSION
- Listener debug DoS (Verify version): PRODUCT_COMPONENT_VERSION
- Listener format string buffer overflow (Verify version): PRODUCT_COMPONENT_VERSION
- Locked account: DBA_USERS, PRODUCT_COMPONENT_VERSION
- MTDS DoS (Verify version): PRODUCT_COMPONENT_VERSION
- NERP DoS (Verify version): PRODUCT_COMPONENT_VERSION
- Non-standard account with DBA role: DBA_ROLE_PRIVS
- NSPTCN buffer overflow (Verify version): PRODUCT_COMPONENT_VERSION
- NSPTCN data offset DoS (Verify version): PRODUCT_COMPONENT_VERSION
- Object privilege grantable: DBA_TAB_PRIVS
- Object privilege granted to account: DBA_TAB_PRIVS, DBA_USERS
- Object privilege granted to PUBLIC: DBA_TAB_PRIVS
- Oracle Configuration Manager: DBA_USERS
- Oracle DIAGNOSTIC_DEST parameter: V$PARAMETER
- Oracle file overwrite: PRODUCT_COMPONENT_VERSION
- Oracle LOG_ARCHIVE_DEST parameter: V$DATABASE, V$PARAMETER
- OS authentication prefix: V$PARAMETER
- Overdue password change: sys.user$
- Password for database user same as username: DBA_USERS
- Privilege granted to SELECT from data dictionary: DBA_TABLES, DBA_TAB_PRIVS
- Privilege on audit trail table: DBA_TAB_PRIVS
- Privilege on database link table: DBA_TAB_PRIVS, DBA_USERS
- Privilege to execute UTL_FILE granted to PUBLIC: DBA_TAB_PRIVS
- Privilege to execute UTL_HTTP granted to PUBLIC: DBA_TAB_PRIVS
- Privilege to execute UTL_SMTP granted to PUBLIC: DBA_TAB_PRIVS
- Privilege to execute UTL_TCP granted to PUBLIC: DBA_TAB_PRIVS
- Profile settings - Failed Login Attempts: DBA_PROFILES, PRODUCT_COMPONENT_VERSION
- Profile settings - Password Grace Time: DBA_PROFILES, PRODUCT_COMPONENT_VERSION
- Profile settings - Password Life Time: DBA_PROFILES, PRODUCT_COMPONENT_VERSION
- Profile settings - Password Lock Time: DBA_PROFILES, PRODUCT_COMPONENT_VERSION

- Profile settings – Password Reuse Maximum: DBA_PROFILES, PRODUCT_COMPONENT_VERSION
- Profile settings – Password Reuse Time: DBA_PROFILES, PRODUCT_COMPONENT_VERSION
- Profile settings – Password Verify Function: DBA_PROFILES, PRODUCT_COMPONENT_VERSION
- Remote login password file not disabled: V$PARAMETER
- Remote OS Authentication enabled: V$PARAMETER
- Remote OS Roles enabled: V$PARAMETER
- Requestor version DoS (Verify version): PRODUCT_COMPONENT_VERSION
- Role without password: DBA_ROLES
- Roles granted WITH ADMIN OPTION: DBA_ROLE_PRIVS
- SERVICE_CURLOAD DoS (Verify version): PRODUCT_COMPONENT_VERSION
- SERVICE_NAME buffer overflow (Verify version): PRODUCT_COMPONENT_VERSION
- SNMP DoS (Verify version): PRODUCT_COMPONENT_VERSION
- SQL92_SECURITY parameter not enabled: V$PARAMETER
- SYSDBA auditing bug: PRODUCT_COMPONENT_VERSION
- SYSDBA privilege assignments
- System privilege granted to account: DBA_SYS_PRIVS, DBA_USERS
- System privilege granted to PUBLIC: DBA_SYS_PRIVS
- System privilege granted WITH ADMIN OPTION: DBA_SYS_PRIVS
- System privilege with ANY clause: DBA_SYS_PRIVS
- TCL debugger installs with setUID root: DBA_SYS_PRIVS
- TCL debugger installs with setUID root: PRODUCT_COMPONENT_VERSION
- TO_TIMESTAMP_TZ buffer overflow (Verify version):PRODUCT_COMPONENT_VERSION
- TZ_OFFSET buffer overflow (Verify version):PRODUCT_COMPONENT_VERSION
- Trace reporting buffer overflow: PRODUCT_COMPONENT_VERSION
- UTL_FILE_DIR unrestricted: V$PARAMETER
- XSQL Servlet stylesheet as URL parameter: PRODUCT_COMPONENT_VERSION
- Auditing of Schema Objects: DBA_OBJ_AUDIT_OPTS, DBA_VIEWS

RUNNING THE ORACLE USER CREATION SCRIPT

Application Security Inc. has written a convenient Oracle user creation script (`CreateUserSQLServer2k.sql`) which creates an account with the minimum privileges necessary to perform Audits on a Microsoft SQL 2000 instance.

The contents of the CreateUserSQLServer2k.sql script follow:

```
DROP USER aduser cascade;

CREATE USER aduser IDENTIFIED BY AD123;

GRANT SELECT ON SYS.DBA_DB_LINKS TO aduser;

GRANT SELECT ON SYS.DBA_DATA_FILES TO aduser;

GRANT SELECT ON SYS.DBA_OBJECTS TO aduser;

GRANT SELECT ON SYS.DBA_OBJ_AUDIT_OPTS TO aduser;

GRANT SELECT ON SYS.DBA_PROCEDURES TO aduser;

GRANT SELECT ON SYS.DBA_PROFILES TO aduser;

GRANT SELECT ON SYS.DBA_ROLES TO aduser;

GRANT SELECT ON SYS.DBA_ROLE_PRIVS TO aduser;

GRANT SELECT ON SYS.DBA_STMT_AUDIT_OPTS TO aduser;

GRANT SELECT ON SYS.DBA_SYS_PRIVS TO aduser;

GRANT SELECT ON SYS.DBA_TABLES TO aduser;

GRANT SELECT ON SYS.DBA_INDEXES TO aduser;

GRANT SELECT ON SYS.DBA_TAB_PRIVS TO aduser;

GRANT SELECT ON SYS.DBA_TS_QUOTAS TO aduser;

GRANT SELECT ON SYS.DBA_USERS TO aduser;

GRANT SELECT ON SYS.DBA_SOURCE TO aduser;

GRANT SELECT ON SYS.DBA_VIEWS TO aduser;

GRANT SELECT ON SYS.PRODUCT_COMPONENT_VERSION TO aduser;

GRANT SELECT ON SYS.LINK$ TO aduser;

GRANT SELECT ON SYS.USER$ TO aduser;

GRANT SELECT ON SYS.V_$PARAMETER TO aduser;

GRANT SELECT ON SYS.V_$LOG TO aduser;

GRANT SELECT ON SYS.V_$PWFILE_USERS TO aduser;

GRANT SELECT ON SYS.V_$INSTANCE TO aduser;

GRANT SELECT ON SYS.V_$DATABASE TO aduser;

GRANT SELECT ON SYS.DBA_PRIV_AUDIT_OPTS TO aduser;

GRANT SELECT ON SYS.DBA_REPCATLOG TO aduser;

GRANT SELECT ON SYS.DEFPROPAGATOR TO aduser;
GRANT SELECT ON SYS.V_$DATAFILE TO aduser;
GRANT SELECT ON SYS.V_$LOGFILE TO aduser;
GRANT SELECT ON SYS.V_$SESSION TO aduser;

GRANT SELECT ON SYS.REGISTRY$HISTORY TO aduser;

GRANT CREATE SESSION TO aduser;
grant javasyspriv to aduser;
grant create procedure to aduser;
```

Sybase Audit Privileges

To conduct a full **Sybase** Audit, you need the following **privileges**. Make sure the account you are using has rights to use the following tables and views:

- `SELECT @@VERSION`
- `master.dbo.syslogins`
- `master.dbo.syssrvroles`
- `master.dbo.sysdatabases`
- `master.dbo.sysconfigures`
- `master.dbo.syscurconfigs`
- `master.dbo.sysroles`
- `master.dbo.sysloginroles`
- `master.dbo.sysattributes`
- `master.dbo.sysservers`
- `exec sp_loginconfig`
- `exec sp_displayaudit (if it's >= 11.5)`
- `sp_auditoption (if it's < 11.5 and >= 11.0)`
- `master.dbo.syblicenseslog`
- `master.dbo.syscharsets`
- `<db name>.dbo.sysusers`
- `<db name>.dbo.sysobjects`
- `<db name>.dbo.syscomments`
- `exec <db name>.dbo.sp_help_resource_limit` (if it's >= 11.5)

The following is a list of **checks** within the DbProtect Vulnerability Assessment for Sybase Security Audit, and the tables and views which they need permission to in order to function properly:

- `Audit database owned by sa_role member: master.dbo.syslogins, master.dbo.sysloginroles, master.dbo.syssrvroles, <dbname>.dbo.sysusers`

- Guest user exists in sybsecurity: master.dbo.syslogins, master.dbo.syssrvroles, <dbname>.dbo.sysusers
- Login granted sa_role: master.dbo.syslogins, master.dbo.sysloginroles, master.dbo.syssrvroles, <dbname>.dbo.sysusers
- Login granted sso_role: master.dbo.syslogins, master.dbo.sysloginroles, master.dbo.syssrvroles, <dbname>.dbo.sysusers
- Objects not owned by dbo: master.dbo.syslogins, master.dbo.syssrvroles, <dbname>.dbo.sysusers, <dbname>.dbo.sysobjects
- Permission granted in sybsecurity: master.dbo.syslogins, master.dbo.syssrvroles, <dbname>.dbo.sysobjects
- Permission granted on system table: master.dbo.syslogins, master.dbo.syssrvroles, <dbname>.dbo.sysobjects
- Permission granted on xp_cmdshell: master.dbo.syslogins, master.dbo.syssrvroles, <dbname>.dbo.sysobjects
- Permission to select from syslogins: master.dbo.syslogins, master.dbo.syssrvroles
- Permissions granted to public: master.dbo.syslogins, master.dbo.syssrvroles, <dbname>.dbo.sysusers
- Permissions granted to user: master.dbo.syslogins, master.dbo.syssrvroles, <dbname>.dbo.sysusers
- Remote access allowed: master.dbo.syslogins, master.dbo.syssrvroles
- Roles revoked from the sa login: master.dbo.syslogins, master.dbo.sysloginroles, master.dbo.syssrvroles
- Server configured with remote server: master.dbo.syslogins, master.dbo.syssrvroles
- Statement permission granted: master.dbo.syslogins, master.dbo.syssrvroles, <dbname>.dbo.sysusers
- Unrestricted access to syscomments: master.dbo.syslogins, master.dbo.syssrvroles
- Updates allowed to system tables: master.dbo.syslogins, master.dbo.syssrvroles
- With grant option: master.dbo.syslogins, master.dbo.syssrvroles, <dbname>.dbo.sysusers
- xp_cmdshell context: master.dbo.syslogins, master.dbo.syssrvroles, <dbname>.dbo.sysobjects
- Absolute value of numeric DoS (Verify version): master.dbo.syslogins, master.dbo.syssrvroles
- Allow resource limit: master.dbo.syslogins, master.dbo.syssrvroles
- Audit logout not set: sybsystemprocs.dbo.sp_loginconfig, sso_role
- Audit queue size: master.dbo.syslogins, master.dbo.syssrvroles
- Audit subsystem not installed: master.dbo.syslogins, master.dbo.syssrvroles
- Auditing disabled: sybsystemprocs.dbo.sp_loginconfig, sso_role

- Auditing of failed logins not enabled: sybsystemprocs.dbo.sp_loginconfig, sso_role
- Auditing of successful logins not enabled: sybsystemprocs.dbo.sp_loginconfig, sso_role
- Current audit table: master.dbo.syslogins, master.dbo.syssrvroles
- DBCC CHECKVERIFY buffer overflow: master.dbo.syslogins, master.dbo.syssrvroles
- DROP DATABASE buffer overflow: master.dbo.syslogins, master.dbo.syssrvroles
- Event log computer name: master.dbo.syslogins, master.dbo.syssrvroles
- Event logging: master.dbo.syslogins, master.dbo.syssrvroles
- Exceeded licensing limitations: master.dbo.syblicenseslog
- Latest patch not applied: master.dbo.syslogins, master.dbo.syssrvroles
- List resource limits: master.dbo.syslogins, master.dbo.syssrvroles
- Log audit logon failure: master.dbo.syslogins, master.dbo.syssrvroles
- Log audit logon success: master.dbo.syslogins, master.dbo.syssrvroles
- No patches available for version: master.dbo.syslogins, master.dbo.syssrvroles
- Password array buffer overflow: master.dbo.syslogins, master.dbo.syssrvroles
- Require message confidentiality with encryption: master.dbo.syslogins, master.dbo.syssrvroles
- Require message integrity: master.dbo.syslogins, master.dbo.syssrvroles
- Select all DoS (Verify version): master.dbo.syslogins, master.dbo.syssrvroles
- Select/Into DoS (Verify version): master.dbo.syslogins, master.dbo.syssrvroles
- SSL enabled: master.dbo.syslogins, master.dbo.syssrvroles
- Start mail session: master.dbo.syslogins, master.dbo.syssrvroles
- Suspend audit when full disabled: master.dbo.syslogins, master.dbo.syssrvroles
- Vulns for v12.5.3 ESD#1 (Verify version): master.dbo.syslogins, master.dbo.syssrvroles
- xp_cmdshell not removed: master.dbo.syslogins, master.dbo.syssrvroles, <dbname>.dbo.sysobjects
- xp_freedll buffer overflow: master.dbo.syslogins, master.dbo.syssrvroles, <dbname>.dbo.sysobjects
- Blank password for sa: master.dbo.syslogins, master.dbo.syssrvroles
- Check password for digit: master.dbo.syslogins, master.dbo.syssrvroles
- Default login exists: sybsystemprocs.dbo.sp_loginconfig, sso_role

- Default login granted role: sybsystemprocs.dbo.sp_loginconfig, sso_role
- Default password for dba repository user: master.dbo.syslogins, master.dbo.syssrvroles
- Default password for entldbdbo: master.dbo.syslogins, master.dbo.syssrvroles
- Default password for entldbreader: master.dbo.syslogins, master.dbo.syssrvroles
- Default password for jagadmin: master.dbo.syslogins, master.dbo.syssrvroles
- Default password for PIAdmin: master.dbo.syslogins, master.dbo.syssrvroles
- Default password for pkiuser: master.dbo.syslogins, master.dbo.syssrvroles
- Default password for PortalAdmin: master.dbo.syslogins, master.dbo.syssrvroles
- Default password for pso: master.dbo.syslogins, master.dbo.syssrvroles
- Default SAP password: master.dbo.syslogins, master.dbo.syssrvroles
- Easily-guessed password: master.dbo.syslogins, master.dbo.syssrvroles
- Easily-guessed sa password: master.dbo.syslogins, master.dbo.syssrvroles
- Expired logins: master.dbo.syslogins, master.dbo.syssrvroles
- Guest user exists in database: master.dbo.syslogins, master.dbo.syssrvroles, <dbname>.dbo.sysusers
- Locked logins: master.dbo.syslogins, master.dbo.syssrvroles
- Login attributes less restrictive: master.dbo.syslogins, master.dbo.syssrvroles
- Login mode: sybsystemprocs.dbo.sp_loginconfig, sso_role
- Maximum failed logins: master.dbo.syslogins, master.dbo.syssrvroles
- Minimum password length: master.dbo.syslogins, master.dbo.syssrvroles
- Orphaned user: master.dbo.syslogins, master.dbo.syssrvroles, <dbname>.dbo.sysusers
- Password same as login name: master.dbo.syslogins, master.dbo.syssrvroles
- Per login password expiration: master.dbo.syslogins, master.dbo.syssrvroles
- Roles without passwords: master.dbo.syslogins, master.dbo.syssrvroles
- Secure default login exists: master.dbo.syslogins, master.dbo.syssrvroles
- System-wide password expiration: master.dbo.syslogins, master.dbo.syssrvroles

- `Unified login required: master.dbo.syslogins, master.dbo.syssrvroles`
- `Unlocked sa login: master.dbo.syslogins, master.dbo.syssrvroles`
- `Use security services: master.dbo.syslogins, master.dbo.syssrvroles`
- `Not using NTFS partition: master.dbo.syslogins, master.dbo.syssrvroles`
- `Permissions on files: master.dbo.syslogins, master.dbo.syssrvroles`
- `Registry permissions: master.dbo.syslogins, master.dbo.syssrvroles`
- `Service runs as LocalSystem: master.dbo.syslogins, master.dbo.syssrvroles`
- `Setgid bit enabled: master.dbo.syslogins, master.dbo.syssrvroles`
- `Setuid bit enabled: master.dbo.syslogins, master.dbo.syssrvroles`

Operating System Considerations (for Audits)

Some DbProtect Vulnerability Assessment Audit checks require more than just a valid database account to perform correctly. They have different requirements depending upon whether the **operating system** (OS) is Windows or UNIX. (The checks are listed in the Audit category OS Integrity.) They only run if the target database has the appropriate OS.

This topic consists of the following sub-topics:

- *Windows OS Audit Check Requirements*
- *UNIX OS Audit Check Requirements.*

WINDOWS OS AUDIT CHECK REQUIREMENTS

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

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

UNIX OS AUDIT CHECK REQUIREMENTS

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

If you run the following checks:	Then you must have permission to:
Permissions on Files	List files in the installation directories of the database.
Setgid Bit Enabled	
Setuid Bit Enabled	

Properly-Configured Environment Variables

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

If you want to Audit the following platform:	Then you must have permission to:
Oracle	Make sure the `$ORACLE_HOME` variable is correct.
Sybase	Make sure the `$SYBASE` variable is correct.
MySQL	Define a `datadir` or `basedir` variable to point to the database root.

Appendix J: Fix Scripts (Detail)

The following tables list each AppDetectivePro fix script (for Oracle and SQL Server); for more information on fix scripts, see *Working with Fix Scripts*.

This appendix consists of the following topics:

- *Microsoft SQL Server Fix Scripts*
- *Oracle Fix Scripts*
- *Sybase Fix Scripts*
- *IBM DB2 Fix Scripts*
- *MySQL Fix Scripts.*

MICROSOFT SQL SERVER FIX SCRIPTS

Check	Script
xp_controlqueueservice buffer overflow	USE master GO DROP PROCEDURE xp_controlqueueservice GO
Password same as login name	USE master GO sp_password '<!!--LOGIN--!!>', '<NEW PASSWORD>', '<!!--LOGIN--!!>' GO
Blank password	Note: The following SQL statements require sysadmin privileges in order to be performed USE master GO sp_password NULL, '<NEW PASSWORD>', '<!!--LOGIN--!!>' GO
Easily-guessed password for well-known login	USE master GO sp_password '<!!--PASSWORD--!!>', '<NEW PASSWORD>', '<!!--LOGIN--!!>' GO
Easily-guessed password for sa	USE master GO sp_password '<!!--PASSWORD--!!>', '<NEW PASSWORD>', 'sa' GO
Blank password for well-known login	Note: The following SQL statements require sysadmin privileges in order to be performed. USE master GO sp_password NULL, '<NEW PASSWORD>', '<!!--LOGIN--!!>' GO

Check	Script
Blank password for sa	Note: The following SQL statements require sysadmin privileges in order to be performed USE master GO sp_password NULL, '<NEW PASSWORD>', 'sa' GO
srv_paraminfo buffer overflow in xp_showcolv	USE master GO REVOKE EXECUTE ON master.dbo.xp_showcolv FROM public GO
Extended stored proc privilege upgrade	USE master GO REVOKE ALL ON [<!!--EXTENDED STORED PROCEDURE--!!>] FROM public GO
srv_paraminfo buffer overflow in xp_proxiedmetadata	USE master GO REVOKE EXECUTE ON master.dbo.xp_proxiedmetadata FROM public GO
xp_dsninfo buffer overflow	USE master GO DROP PROCEDURE xp_dsninfo GO
xp_oledbinfo buffer overflow	Note: Despite performing the following SQL statements, vulnerabilities may still show up in future Security Audits. To fully fix this vulnerability, please apply the latest patch.
xp_repl_encrypt buffer overflow	Note: Despite performing the following SQL statements, vulnerabilities may still show up in future Security Audits. To fully fix this vulnerability, please apply the latest patch.
xp_dirtree buffer overflow	Note: Despite performing the following SQL statements, vulnerabilities may still show up in future Security Audits. To fully fix this vulnerability, please apply the latest patch.

Check	Script

Enterprise Manager improperly revokes proxy account	DECLARE @regread_dropped int
	DECLARE @regwrite_dropped int
	SELECT @regread_dropped=0, @regwrite_dropped=0
	IF not exists (select * from master.dbo.sysobjects where name = 'xp_instance_regread')
	BEGIN
	EXECUTE master.dbo.sp_addextendedproc 'xp_instance_reg

Permission on registry extended proc	USE <!!--DATABASE--!!> GO REVOKE EXECUTE ON [<!!--EXTENDED STORED PROCEDURE--!!>] FROM <!!--GRANTED TO--!!> GO
srv_paraminfo buffer overflow in sp_OAGetProperty	Note: Despite performing the following SQL statements, vulnerabilities may still show up in future Security Audits. To fully fix this vulnerability, please apply the latest patch.
Remote access allowed	USE master GO sp_configure 'remote access', 0 GO RECONFIGURE GO
srv_paraminfo buffer overflow in xp_updatecolvbm	USE master GO REVOKE EXECUTE ON master.dbo.xp_updatecolvbm FROM public GO
Format string vuln in xp_sprintf	USE master GO REVOKE EXECUTE ON master.dbo.xp_sprintf FROM public GO

Check	Script
Changing mode may leave sa password blank	Note: The following SQL statements require sysadmin privileges in order to be performed USE master GO sp_password NULL, '<NEW PASSWORD>','sa' GO
srv_paraminfo buffer overflow in xp_sqlagent_monitor	Note: Despite performing the following SQL statements, vulnerabilities may still show up in future Security Audits. To fully fix this vulnerability, please apply the latest patch.
srv_paraminfo buffer overflow in sp_OACreate	Note: Despite performing the following SQL statements, vulnerabilities may still show up in future Security Audits. To fully fix this vulnerability, please apply the latest patch.
srv_paraminfo buffer overflow in xp_peekqueue	USE master GO REVOKE EXECUTE ON master.dbo.xp_peekqueue FROM public GO
Permissions granted to user	USE [<!--DATABASE--!>] GO REVOKE <!--PRIVILEGE--!> ON <!--OBJECT NAME--!> FROM [<!--GRANTED TO--!>] GO
Easily-guessed password	USE master GO sp_password '<!--PASSWORD--!>', '<NEW PASSWORD>', '<!--LOGIN--!>' GO
Permission on OLE automation procs	USE master GO REVOKE EXECUTE ON [<!--OBJECT NAME--!>] FROM [<!--USER NAME--!>] GO
srv_paraminfo buffer overflow in sp_OASetProperty	Note: Despite performing the following SQL statements, vulnerabilities may still show up in future Security Audits. To fully fix this vulnerability, please apply the latest patch.

Check	Script
srv_paraminfo buffer overflow in xp_execresultset	USE master GO REVOKE EXECUTE ON master.dbo.xp_execresultset FROM public GO
Direct updates on data dictionary	USE master GO sp_configure 'allow updates', 0 GO RECONFIGURE WITH OVERRIDE GO
srv_paraminfo buffer overflow in xp_SetSQLSecurity	USE master GO REVOKE EXECUTE ON master.dbo.xp_SetSQLSecurity FROM public GO
srv_paraminfo buffer overflow in xp_printstatements	USE master GO REVOKE EXECUTE ON master.dbo.xp_printstatements FROM public GO
srv_paraminfo buffer overflow in sp_OAMethod	Note: Despite performing the following SQL statements, vulnerabilities may still show up in future Security Audits. To fully fix this vulnerability, please apply the latest patch.

Unauthorized object permission grants	IF DB_ID(N'<!!--DATABASE--!!>') IS NOT NULL
	EXEC('USE [<!!--DATABASE--!!>]' + ' REVOKE <!!--PERMISSION--!!> ON [<!!--OWNER--!!>].[<!!--OBJECT NAME--!!>] FROM [<!!--GRANTEE--!!>]')

Default trace disabled	USE master exec sp_configure 'show advanced options', 1 reconfigure exec sp_configure 'default trace enabled', 1 reconfigure

Check	Script
Agent jobs privilege escalation	USE <!!--DATABASE--!!> GO REVOKE ALL ON [<!!--STORED PROCEDURE--!!>] FROM public GO
Remote admin connections allowed	exec sp_configure 'remote admin connections', 0 go reconfigure go
Agent XPs enabled	USE master EXEC sp_configure 'show advanced options', 1 RECONFIGURE EXEC sp_configure 'Agent XPs', '0' RECONFIGURE
sp_replwritetovarbin limited memory overwrite vulnerability	USE master GO REVOKE ALL ON master.dbo.sp_replwritetovarbin FROM [<!!--GRANTED TO--!!>] GO
xp_cmdshell not removed/not disabled	USE master GO sp_dropextendedproc @functname='xp_cmdshell' GO

Unauthorized object permission grants	IF DB_ID(N'<!!--DATABASE--!!>') IS NOT NULL
	EXEC('USE [<!!--DATABASE--!!>]' + ' REVOKE <!!--PERMISSION--!!> ON [<!!--COLUMN--!!>] FROM [<!!--GRANTEE--!!>]')

C2 Audit Mode	USE master EXEC sp_configure 'show advanced option', '1' RECONFIGURE WITH OVERRIDE EXEC sp_configure 'c2 audit mode', 1 RECONFIGURE WITH OVERRIDE

Check	Script
Unauthorized object permission grants	DECLARE @oldValue int SELECT @oldValue = value FROM master..syscurconfigs where config=102 We have to run SP_CONFIGURE to allow updates to the system catalogs EXEC SP_CONFIGURE 'ALLOW UPDATES', 1 RECONFIGURE WITH OVERRIDE
Unauthorized object permission grants	EXEC SP_CONFIGURE 'ALLOW UPDATES', @oldValue RECONFIGURE WITH OVERRIDE GO

Permissions granted to GUEST	IF DB_ID(N'<!!--DATABASE--!!>') IS NOT NULL
	EXEC('USE [<!!--DATABASE--!!>]' + ' REVOKE <!!--PERMISSION--!!> FROM GUEST')"
	Permissions granted to GUEST
	IF DB_ID(N'<!!--DATABASE--!!>') IS NOT NULL
	EXEC('USE [<!!--DATABASE--!!>]' + ' REVOKE <!!--PERMISSION--!!> ON [<!!--OWNER--!!>].[<!!--OBJECT NAME--!!>] FROM GUEST')

Unauthorized object permission grants	IF DB_ID(N'<!!--DATABASE--!!>') IS NOT NULL
	EXEC('USE [<!!--DATABASE--!!>]' + ' REVOKE <!!--PERMISSION--!!> ON [<!!--SCHEMA NAME--!!>].[<!!--OBJECT NAME--!!>] FROM [<!!--GRANTEE--!!>]')

Permissions granted to GUEST	IF DB_ID(N'<!!--DATABASE--!!>') IS NOT NULL EXEC('USE [<!!--DATABASE--!!>]' + ' REVOKE <!!--PERMISSION--!!> ON [<!!--SCHEMA NAME--!!>].[<!!--OBJECT NAME--!!>] FROM GUEST'

Unauthorized object permission grants	IF DB_ID(N'<!!--DATABASE--!!>') IS NOT NULL
	EXEC('USE [<!!--DATABASE--!!>]' + ' REVOKE <!!--PERMISSION--!!> FROM [<!!--GRANTEE--!!>]')

Permission on sp_runwebtask	USE master GO REVOKE ALL ON master.dbo.sp_runwebtask FROM public GO

Check	Script
Statement permission granted	USE <!!--DATABASE--!!> GO REVOKE <!!--PRIVILEGE--!!> FROM <!!--GRANTED TO--!!> GO
Permission grantable	USE [<!!--DATABASE--!!>] GO REVOKE <!!--PRIVILEGE--!!> ON [<!!--DATABASE--!!>].[<!!--SCHEMA NAME--!!>].[<!!--OBJECT NAME--!!>] FROM <!!--GRANTED TO--!!> CASCADE GO
Guest user exists in database	USE <!!--DATABASE--!!> GO sp_dropuser guest GO
Registry extended proc not removed	USE master GO sp_dropextendedproc @functname='<!!--EXTENDED STORED PROCEDURE--!!>' GO
xp_createqueue buffer overflow	USE master GO DROP PROCEDURE xp_createqueue GO
Permissions granted on xp_cmdshell	USE master GO IF exists (select * from master.dbo.sysobjects where name = 'xp_cmdshell') REVOKE EXECUTE ON [xp_cmdshell] FROM [<!!--USER NAME--!!>] GO
Permission grantable	USE [<!!--DATABASE--!!>] GO REVOKE <!!--PRIVILEGE--!!> ON [<!!--DATABASE--!!>].[<!!--OWNER--!!>].[<!!--OBJECT NAME--!!>] FROM <!!--GRANTED TO--!!> CASCADE GO

Check	Script
Permissions granted to user	USE [<!!--DATABASE--!!>] GO REVOKE <!!--PRIVILEGE--!!> FROM [<!!--GRANTED TO--!!>] GO
C2 Audit Mode	DECLARE @oldValue int SELECT @oldValue = value FROM master..syscurconfigs where config=518 --We have to run SP_CONFIGURE 'show advanced option', '1' to be able to change advanced options
Permissions granted to user	USE [<!!--DATABASE--!!>] GO REVOKE <!!--PRIVILEGE--!!> ON [<!!--SCHEMA NAME--!!>].[<!!--OBJECT NAME--!!>] FROM [<!!--GRANTED TO--!!>] CASCADE GO
Permission to select from system table	USE [<!!--DATABASE--!!>] GO REVOKE SELECT ON [<!!--DATABASE--!!>].[<!!--SCHEMA NAME--!!>].[<!!--TABLE NAME--!!>] FROM [<!!--GRANTED TO--!!>] CASCADE GO
Permission to select from system table	USE [<!!--DATABASE--!!>] GO REVOKE SELECT ON [<!!--DATABASE--!!>].[<!!--OWNER--!!>].[<!!--TABLE NAME--!!>] FROM [<!!--GRANTED TO--!!>] CASCADE GO
Error logs can be overwritten	Note: Despite performing the following SQL statements, vulnerabilities may still show up in future Security Audits. To fully fix this vulnerability, please apply the latest patch. Permission to select from syslogins USE master GO REVOKE SELECT ON master.dbo.syslogins FROM <!!--GRANTED TO--!!> GO

Check	Script
Objects not owned by dbo	USE <!!--DATABASE--!!> GO DROP TABLE [<!!--DATABASE--!!>].[<!!--OWNER--!!>].[<!!--OBJECT NAME--!!>] GO
srv_paraminfo buffer overflow in sp_OADestroy	Note: Despite performing the following SQL statements, vulnerabilities may still show up in future Security Audits. To fully fix this vulnerability, please apply the latest patch.
Default password for well-known login	USE master GO sp_password <!!--PASSWORD--!!>, <NEW PASSWORD>, <!!--LOGIN--!!> GO
Permissions granted to PUBLIC	EXEC SP_CONFIGURE 'ALLOW UPDATES', @oldValue RECONFIGURE WITH OVERRIDE GO
sysadmin role granted"USE master	GO EXEC sp_dropsrvrolemember N'<!!--LOGIN--!!>', 'sysadmin' GO
xp_deletequeue buffer overflow	USE master GO DROP PROCEDURE xp_deletequeue GO
xp_displayqueuemesgs buffer overflow	USE master GO DROP PROCEDURE xp_displayqueuemesgs GO
xp_readpkfromqueue buffer overflow	USE master GO DROP PROCEDURE xp_readpkfromqueue GO

Check	Script
xp_sprintf buffer overflow	USE master GO REVOKE EXECUTE ON master.dbo.xp_sprintf FROM public GO
xp_unpackcab buffer overflow	USE master GO DROP PROCEDURE xp_unpackcab GO
Permission on sp_MSsetalertinfo	USE master GO REVOKE ALL ON master.dbo.sp_MSsetalertinfo FROM public GO
xp_mergelineages buffer overflow	USE master GO DROP PROCEDURE xp_mergelineages GO
xp_decodequeuecmd buffer overflow	USE master GO DROP PROCEDURE xp_decodequeuecmd GO
xp_resetqueue buffer overflow	USE master GO DROP PROCEDURE xp_resetqueue GO
Permissions granted to GUEST	EXEC SP_CONFIGURE 'ALLOW UPDATES', @oldValue RECONFIGURE WITH OVERRIDE GO
xp_sqlagent_param buffer overflow	Note: Despite performing the following SQL statements, vulnerabilities may still show up in future Securit Audits. To fully fix this vulnerability, please apply the latest patch.

Check	Script
xp_readpkfromvarbin buffer overflow	USE master GO DROP PROCEDURE xp_readpkfromvarbin GO
Encoded password written by installation	USE master GO sp_password <!!--SQLDOMAINPWD--!!>,<NEW PASSWORD>,'sa' GO
Encoded password written by installation	USE master GO sp_password <!!--CONFIRMPWD--!!>,<NEW PASSWORD>,'sa' GO
Encoded password written by installation	USE master GO sp_password <!!--ENTERPWD--!!>,<NEW PASSWORD>,'sa' GO
xp_sqlinventory buffer overflow	USE master GO DROP PROCEDURE xp_sqlinventory GO
Encoded password written by installation	USE master GO sp_password <!!--AGTDOMAINPWD--!!>,<NEW PASSWORD>,'sa' GO
Fixed server role granted	USE master GO EXEC sp_dropsrvrolemember N'<!!--LOGIN--!!>', '<!!--PRIVILEGE--!!>' GO

Check	Script
Encoded password written by installation	USE master GO sp_password <!!--SVPWD--!!>,<NEW PASSWORD>,'sa' GO
Encoded password written by installation	USE master GO sp_password <!!--SVPASSWORD--!!>,<NEW PASSWORD>,'sa' GO
DTS password table publicly viewable	USE msdb GO sp_dropuser guest GO REVOKE SELECT ON RTblDBMProps FROM public GO
Table to store DTS passwords publicly viewable	USE msdb GO sp_dropuser guest GO REVOKE SELECT ON RTblDBMProps FROM public GO
sp_MScopyscriptfile command injection	Note: Despite performing the following SQL statements, vulnerabilities may still show up in future Security Audits. To fully fix this vulnerability, please apply the latest patch.
Public can create Agent jobs	USE <!!--DATABASE--!!> GO REVOKE ALL ON [<!!--STORED PROCEDURE--!!>] FROM public GO
Permission on sp_MSSetServerProperties	USE master GO REVOKE ALL ON master.dbo.sp_MSSetServerProperties FROM public GO

Check	Script
xp_deleteprivatequeue buffer overflow	USE master GO DROP PROCEDURE xp_deleteprivatequeue GO
srv_paraminfo buffer overflow in xp_displayparamstmt	USE master GO REVOKE EXECUTE ON master.dbo.xp_displayparamstmt FROM public GO

Permissions granted to PUBLIC	IF DB_ID(N'<!!--DATABASE--!!>') IS NOT NULL
	EXEC('USE [<!!--DATABASE--!!>]' + ' REVOKE <!!--PERMISSION--!!> ON [<!!--OWNER--!!>].[<!!--OBJECT NAME--!!>] FROM PUBLIC')
	xp_proxiedmetadata buffer overflow
	Note: Despite performing the following SQL statements, vulnerabilities may still show up in future Security Audits. To fully fix this vulnerability, please apply the latest patch.

xp_createprivatequeue buffer overflow	USE master GO DROP PROCEDURE xp_createprivatequeue GO
Permissions granted on sp_add_dtspackage	USE msdb GO REVOKE EXECUTE ON sp_add_dtspackage FROM public GO Permissions granted to GUEST"IF DB_ID(N'<!!--DATABASE--!!>') IS NOT NULL EXEC('USE [<!!--DATABASE--!!>]' + ' REVOKE <!!--PERMISSION--!!> ON [<!!--COLUMN--!!>] FROM GUEST')
Permission on mswebtasks	USE msdb GO REVOKE <!!--PERMISSION--!!> ON msdb.dbo.mswebtasks FROM public GO

Check	Script
Permission on sp_readwebtask	USE master GO REVOKE ALL ON master.dbo.sp_readwebtask FROM public GO
Permission on xp_readerrorlog	USE master GO REVOKE ALL ON master.dbo.xp_readerrorlog FROM <!!--GRANTED TO--!!> GO
xstatus backdoor	EXEC SP_CONFIGURE 'ALLOW UPDATES', @oldValue RECONFIGURE WITH OVERRIDE GO
xstatus backdoor	DECLARE @oldValue int SELECT @oldValue = value FROM master..syscurconfigs where config=102 We have to run SP_CONFIGURE to allow updates to the system catalogs EXEC SP_CONFIGURE 'ALLOW UPDATES', 1 RECONFIGURE WITH OVERRIDE
DTS package procedures granted to public	USE <!!--DATABASE--!!> GO REVOKE ALL ON [<!!--DATABASE--!!>].[<!!--OWNER--!!>].[<!!--PROCEDURE NAME--!!>] FROM public GO
Agent jobs privilege escalation	USE <!!--DATABASE--!!> GO REVOKE ALL ON [<!!--EXTENDED STORED PROCEDURE--!!>] FROM public GO
xstatus backdoor	USE master exec('delete from master.dbo.sysxlogins where [name] = ''<!!--LOGIN--!!>''') EXEC sp_grantlogin N'<!!--LOGIN--!!>'

Check	Script
DTS package procedures granted to public	USE <!!--DATABASE--!!> GO REVOKE ALL ON [<!!--DATABASE--!!>].[<!!--OWNER--!!>].[<!!--TABLE NAME--!!>] FROM public GO
SQL injection in sp_MSdropretry	Note: Despite performing the following SQL statements, vulnerabilities may still show up in future Security Audits. To fully fix this vulnerability, please apply the latest patch.
SQL Agent password publicly viewable	USE msdb GO sp_dropuser guest GO REVOKE ALL ON sp_get_sqlagent_properties FROM public GO
SQL Agent procedures granted to public	USE msdb GO sp_dropuser guest GO REVOKE ALL ON sp_get_sqlagent_properties FROM public GO
Permissions granted to GUEST	DECLARE @oldValue int SELECT @oldValue = value FROM master..syscurconfigs where config=102 We have to run SP_CONFIGURE to allow updates to the system catalogs EXEC SP_CONFIGURE 'ALLOW UPDATES', 1 RECONFIGURE WITH OVERRIDE

Permissions granted to PUBLIC	IF DB_ID(N'<!!--DATABASE--!!>') IS NOT NULL
	EXEC('USE [<!!--DATABASE--!!>]' + ' REVOKE <!!--PERMISSION--!!> ON [<!!--COLUMN--!!>] FROM PUBLIC')
	Permissions granted to PUBLIC"IF DB_ID(N'<!!--DATABASE--!!>') IS NOT NULL
	EXEC('USE [<!!--DATABASE--!!>]' + ' REVOKE <!!--PERMISSION--!!> ON [<!!--SCHEMA NAME--!!>].[<!!--OBJECT NAME--!!>] FROM PUBLIC')

Check	Script
Sample database not removed	USE master GO DROP DATABASE <!!--DATABASE--!!> GO
Permissions granted to PUBLIC	DECLARE @oldValue int SELECT @oldValue = value FROM master..syscurconfigs where config=102 We have to run SP_CONFIGURE to allow updates to the system catalogs EXEC SP_CONFIGURE 'ALLOW UPDATES', RECONFIGURE WITH OVERRIDE

Permissions granted to PUBLIC	IF DB_ID(N'<!!--DATABASE--!!>') IS NOT NULL
	   EXEC('USE [<!!--DATABASE--!!>]' + ' REVOKE <!!--PERMISSION--!!> FROM PUBLIC')

ORACLE FIX SCRIPTS

Check	Script
Brute-force role password	ALTER ROLE <!!--USERNAME--!!> IDENTIFIED BY <PASSWORD>;

Object privilege granted to PUBLIC	BEGIN
	IF UPPER('<!!--PRIVILEGE--!!>') IN ('DEQUEUE', 'ENQUEUE') THEN
	DBMS_AQADM.REVOKE_QUEUE_PRIVILEGE('<!!--PRIVILEGE--!!>', '<!!--OWNER--!!>.<!!--OBJECT NAME--!!>', 'PUBLIC');
	ELSE
	EXECUTE IMMEDIATE 'REVOKE <!!--PRIVILEGE--!!> ON "<!!--OWNER--

Account granted the predefined role CONNECT	CREATE ROLE <NEW ROLE>; GRANT CREATE SESSION TO <NEW ROLE>;
Account granted the predefined role CONNECT	REVOKE CONNECT FROM <!!--GRANTED TO--!!>; GRANT <NEW ROLE> TO <!!--GRANTED TO--!!>;
Non-standard account with DBA role	REVOKE DBA FROM <!!--GRANTED TO--!!>;
Account granted the predefined role RESOURCE	CREATE ROLE <NEW ROLE>; GRANT CREATE SESSION TO <NEW ROLE>;
Privilege to execute UTL_HTTP granted to PUBLIC	REVOKE EXECUTE ON SYS.UTL_HTTP FROM PUBLIC;
Easily-guessed role password	ALTER ROLE <!!--USER NAME--!!> IDENTIFIED BY <PASSWORD>;
Privilege to execute UTL_SMTP granted to PUBLIC	REVOKE EXECUTE ON SYS.UTL_SMTP FROM PUBLIC;
Profile settings - Failed Login Attempts	ALTER PROFILE <!!--PROFILE--!!> LIMIT FAILED_LOGIN_ATTEMPTS 10;

Check	Script

Object privilege grantable	BEGIN
	IF UPPER('<!!--PRIVILEGE--!!>') IN ('DEQUEUE', 'ENQUEUE') THEN DBMS_AQADM.REVOKE_QUEUE_PRIVILEGE('<!!--PRIVILEGE--!!>', '<!!--OWNER--!!>.<!!--OBJECT NAME--!!>', '<!!--GRANTED TO--!!>'); DBMS_AQADM.GRANT_QUEUE_PRIVILEGE('<!!--PRIVILEGE--!!>'

Privilege on database link table	REVOKE <!!--PRIVILEGE--!!> ON SYS.LINK$ FROM <!!--USER NAME--!!>;
Object privilege granted to account	CREATE ROLE <NEW ROLE>;
Default database password	ALTER USER <!!--USER NAME--!!> IDENTIFIED BY <NEW PASSWORD>;
Account granted the predefined role RESOURCE	REVOKE RESOURCE FROM <!!--GRANTED TO--!!>; GRANT <NEW ROLE> TO <!!--GRANTED TO--!!>;
System privilege granted WITH ADMIN OPTION	REVOKE <!!--PRIVILEGE--!!> FROM <!!--GRANTED TO--!!>; GRANT <!!--PRIVILEGE--!!> TO <!!--GRANTED TO--!!>;
Role without password	ALTER ROLE <!!--ROLE--!!> IDENTIFIED BY <PASSWORD>;
Profile settings - Password Verify Function	ALTER PROFILE <!!--PROFILE--!!> LIMIT PASSWORD_VERIFY_FUNCTION <NEW VERIFY FUNCTION>;
Profile settings - Password Reuse Time	ALTER PROFILE <!!--PROFILE--!!> LIMIT PASSWORD_REUSE_TIME 180 PASSWORD_REUSE_MAX UNLIMITED;
Profile settings - Password Reuse Maximum	ALTER PROFILE <!!--PROFILE--!!> LIMIT PASSWORD_REUSE_MAX 10 PASSWORD_REUSE_TIME UNLIMITED;
Profile settings - Password Lock Time	ALTER PROFILE <!!--PROFILE--!!> LIMIT PASSWORD_LOCK_TIME 1;
Profile settings - Password Life Time	ALTER PROFILE <!!--PROFILE--!!> LIMIT PASSWORD_LIFE_TIME 90;
Profile settings - Password Grace Time	ALTER PROFILE <!!--PROFILE--!!> LIMIT PASSWORD_GRACE_TIME 3;

Check	Script

Object privilege granted to account	BEGIN
	IF NOT UPPER('<!!--PRIVILEGE--!!>') IN ('INDEX', 'REFERENCES') THEN
	EXECUTE IMMEDIATE 'REVOKE <!!--PRIVILEGE--!!> ON " "<!!--OWNER--!!>" "." "<!!--OBJECT NAME--!!>" " FROM <!!--GRANTED TO--!!>';
	EXECUTE IMMEDIATE 'GRANT <!!--PRIVILEGE--!!> ON " "<!!-

Privilege to execute UTL_FILE granted to PUBLIC	REVOKE EXECUTE ON SYS.UTL_FILE FROM PUBLIC;
Auditing of CREATE SESSION not enabled	AUDIT SESSION;
SQL Injection in OWF_MGR.WF_LOV	REVOKE EXECUTE ON OWF_MGR.WF_LOV FROM PUBLIC;
Password for database user same as username	ALTER USER <!!--USER NAME--!!> IDENTIFED BY <NEW PASSWORD>;
Expired password	ALTER USER <!!--USERNAME--!!> IDENTIFED BY <NEW PASSWORD>;
Account granted ALTER SYSTEM privilege	REVOKE ALTER SYSTEM FROM <!!--GRANTED TO--!!>;
System privilege with ANY clause	REVOKE <!!--PRIVILEGE--!!> FROM <!!--GRANTED TO--!!>;
Create library privilege	REVOKE <!!--PRIVILEGE--!!> FROM <!!--GRANTED TO--!!>;
Privilege on audit trail table	REVOKE <!!--PRIVILEGE--!!> ON SYS.AUD$ FROM <!!--GRANTED TO--!!>;
Account associated with DEFAULT profile	ALTER USER <!!--USERNAME--!!> PROFILE <NEW PROFILE NAME>;
Account associated with DEFAULT profile	CREATE PROFILE <NEW PROFILE NAME> LIMIT SESSIONS_PER_USER 2 CPU_PER_SESSION unlimited CPU_PER_CALL 6000 LOGICAL_READS_PER_SESSION unlimited LOGICAL_READS_PER_CALL 100 IDLE_TIME 30 CONNECT_TIME 480;
Privilege granted to SELECT from data dictionary	REVOKE <!!--PRIVILEGE--!!> ON <!!--TABLE NAME--!!> FROM <!!--GRANTED TO--!!>;

Check	Script
Account granted the predefined role DBA	CREATE ROLE <NEW ROLE>;

System privilege granted to account	CREATE ROLE <NEW ROLE>;VARIABLE privilege_name VARCHAR2(20);
	VARIABLE privilege_user VARCHAR2(100);

Account can access source code as SYS	REVOKE <!!--PRIVILEGE--!!> FROM <!!--GRANTED TO--!!>;

System privilege granted to account"	BEGIN
	:privilege_user := 'Privilege: ' || '<!!--PRIVILEGE--!!>' || ' - User: ' || '<!!--GRANTED TO--!!>';
	END;
	/
	PRINT :privilege_user;
	BEGIN
	--UNLIMITED TABLESPACE, SYSDBA or SYSOPER privilege cannot be granted to a role.
	IF NOT UPPER('<!!--PRIVILEGE"

Overdue password change	ALTER USER <!!--USERNAME--!!> IDENTIFIED BY <PASSWORD>;
Account can grant any role	REVOKE GRANT ANY ROLE FROM <!!--GRANTED TO--!!>;
SQL Injection in PORTAL.WPG_SESSION	REVOKE EXECUTE ON PORTAL.WPG_SESSION FROM PUBLIC;
Accounts with SYSTEM as default tablespace	ALTER USER <!!--USER NAME--!!> DEFAULT TABLESPACE <NEW DEFAULT TABLESPACE>;
SQL Injection in ORASSO.WPG_SESSION	REVOKE EXECUTE ON ORASSO.WPG_SESSION FROM PUBLIC;
Account granted the predefined role DBA	REVOKE DBA FROM <!!--GRANTED TO--!!>; GRANT CREATE SESSION TO <NEW ROLE>; GRANT <NEW ROLE> TO <!!--GRANTED TO--!!>;
Account can replace public links	REVOKE CREATE PUBLIC DATABASE LINK FROM <!!--GRANTED TO--!!>; REVOKE DROP PUBLIC DATABASE LINK FROM <!!--GRANTED TO--!!>;

Check	Script
Privilege to execute DBMS_RANDOM granted to PUBLIC	REVOKE EXECUTE ON SYS.DBMS_RANDOM FROM PUBLIC;
Roles granted WITH ADMIN OPTION	REVOKE <!!--ROLE--!!> FROM <!!--GRANTED TO--!!>; GRANT <!!--ROLE--!!> TO <!!--GRANTED TO--!!>;
Account granted the JAVA_ADMIN role	REVOKE JAVA_ADMIN FROM <!!--GRANTED TO--!!>;
Default role password	ALTER ROLE <!!--ROLE--!!> IDENTIFIED BY <PASSWORD>;
System privilege granted to PUBLIC	REVOKE "<!!--PRIVILEGE--!!>" FROM PUBLIC;
SQL Injection in OWF_MGR.WF_EVENT_HTML	REVOKE EXECUTE ON OWF_MGR.WF_EVENT_HTML FROM PUBLIC;
Privilege to execute UTL_TCP granted to PUBLIC	REVOKE EXECUTE ON SYS.UTL_TCP FROM PUBLIC;
Account can become another user	REVOKE BECOME USER FROM <!!--GRANTED TO--!!>; REVOKE ALTER USER FROM <!!--GRANTED TO--!!>;
Account can create public synonyms	REVOKE CREATE PUBLIC SYNONYM FROM <!!--GRANTED TO--!!>;

SYBASE FIX SCRIPTS

Check	Script
Server configured with remote server	USE master sp_dropserver <!!--SERVER NAME--!!>, droplogins
Allow resource limit	USE master sp_configure 'allow resource limits', 1 RECONFIGURE
Permission granted in sybsecurity	USE <!!--DATABASE--!!> REVOKE <!!--PRIVILEGE--!!> ON <!!--DATABASE--!!>.<!!--OWNER--!!>.<!!--OBJECT--!!>.<!!--COLUMN--!!> FROM <!!--GRANTED TO--!!>
Permission granted on xp_cmdshell	USE <!!--DATABASE--!!> REVOKE EXECUTE ON xp_cmdshell FROM <!!--GRANTED TO--!!>
Permission granted in sybsecurity	USE <!!--DATABASE--!!> REVOKE <!!--PRIVILEGE--!!> ON <!!--DATABASE--!!>.<!!--OWNER--!!>.<!!--OBJECT--!!> FROM <!!--GRANTED TO--!!>
Auditing disabled	sp_auditoption 'enable auditing', 'on' sp_configure 'auditing', 1
Log audit logon failure	USE master sp_configure 'log audit logon failure', 1 RECONFIGURE
Blank password for sa	USE master sp_password <CURRENT PASSWORD>, <NEW PASSWORD>, 'sa'
Easily-guessed sa password	USE master sp_password <CURRENT PASSWORD>, <NEW PASSWORD>, 'sa'
Default password for entldbreader	USE master sp_password <CURRENT PASSWORD>, <NEW PASSWORD>, 'entldbreader'
Default password for jagadmin	USE master sp_password <CURRENT PASSWORD>, <NEW PASSWORD>, 'jagadmin'

Suspend audit when full disabled	USE master sp_configure 'suspend audit when device full', 1 RECONFIGURE
Statement permission granted	USE <!!--DATABASE--!!> REVOKE <!!--PRIVILEGE--!!> FROM <!!--GRANTED TO--!!>
Default password for entldbdbo	USE master sp_password <CURRENT PASSWORD>, <NEW PASSWORD>, 'entldbdbo'
Default password for dba repository user	USE master sp_password <CURRENT PASSWORD>, <NEW PASSWORD>, 'dba'
Easily-guessed password	USE master sp_password <CURRENT PASSWORD>, <NEW PASSWORD>, <!!--LOGIN--!!>
Permissions granted to public	USE <!!--DATABASE--!!> REVOKE <!!--PRIVILEGE--!!> ON <!!--DATABASE--!!>.<!!--OWNER--!!>.<!!--OBJECT--!!>.<!!--COLUMN--!!> FROM public
Require message integrity	USE master execute sp_configure 'msg integrity reqd', 1 execute sp_configure 'use security services', 1
Default password for pso	USE master sp_password <CURRENT PASSWORD>, <NEW PASSWORD>, 'pso'
Unrestricted access to syscomments	USE master sp_configure 'select on syscomments.text', 0 RECONFIGURE
Audit database owned by sa_role member	USE master sp_changedbowner <!!--LOGIN--!!> <, true >

Login attributes less restrictive	USE master sp_modifylogin <!!--LOGIN--!!>, 'max failed_logins', <NEW VALUE> sp_modifylogin <!!--LOGIN--!!>, 'passwd expiration', <NEW VALUE> sp_modifylogin <!!--LOGIN--!!>, 'min passwd length', <NEW VALUE> sp_modifylogin 'all overrides', 'max failed_login
Unlocked sa login	USE master sp_role ""grant"", sa_role, <NEW SA LOGIN> sp_role ""grant"", sso_role, <NEW SA LOGIN> sp_locklogin 'sa', ""lock""
With grant option	USE <!!--DATABASE--!!> REVOKE <!!--PRIVILEGE--!!> ON <!!--DATABASE--!!>.<!!--OWNER--!!>.<!!--OBJECT--!!> FROM <!!--DATABASE--!!>.<!!--USER--!!> CASCADE
Auditing of failed logins not enabled	sp_auditoption 'logins', 'fail' sp_audit 'login', 'all', 'all', 'fail'
Permissions granted to public	USE <!!--DATABASE--!!> REVOKE <!!--PRIVILEGE--!!> ON <!!--DATABASE--!!>.<!!--OWNER--!!>.<!!--OBJECT--!!> FROM public
Expired logins	USE master sp_password <CURRENT PASSWORD>, <NEW PASSWORD>, <!!--LOGIN--!!>
Login granted sa_role	USE master REVOKE sa_role FROM <!!--LOGIN--!!>
Login granted sso_role	USE master REVOKE sso_role FROM <!!--LOGIN--!!>
Guest user exists in sybsecurity	USE sybsecurity sp_dropuser guest
Auditing of successful logins not enabled	sp_auditoption 'logins', 'ok' sp_audit 'login', 'all', 'all', 'pass'
Permissions granted to user	USE <!!--DATABASE--!!> REVOKE <!!--PRIVILEGE--!!> ON <!!--DATABASE--!!>.<!!--OWNER--!!>.<!!--OBJECT--!!> FROM <!!--GRANTED TO--!!>

Event logging	USE master execute sp_configure 'event logging', 1 RECONFIGURE
Objects not owned by dbo	USE <!!--DATABASE--!!> DROP TABLE <!!--DATABASE--!!>.<!!--OWNER--!!>.<!!--OBJECT--!!>
Remote access allowed	USE master sp_configure 'allow remote access', 0 RECONFIGURE
Roles revoked from the sa login	USE master REVOKE ROLE sa_role FROM sa REVOKE ROLE sso_role FROM sa REVOKE ROLE oper_role FROM sa REVOKE ROLE sybase_ts_role FROM sa
List resource limits	USE <!!--DATABASE--!!> sp_add_resource_limit <!!--LOGIN--!!>, <!!--APPLICATION--!!>, <!!--RANGE--!!>, <LIMIT TYPE>, <!!--LIMIT--!!> <, <ENFORCED> <, <ACTION> <, <SCOPE> >>>
Start mail session	USE master execute sp_configure 'start mail session', 0 RECONFIGURE
Unified login required	USE master sp_configure 'unified login required', 1 sp_configure 'use security services', 1 RECONFIGURE
Allow sendmsg	USE master execute sp_configure 'allow sendmsg', 0 RECONFIGURE
Orphaned user	USE master sp_dropuser '<!!--USERNAME--!!>' sp_droplogin '<CORRESPONDING LOGIN>' sp_addlogin '<CORRESPONDING LOGIN>', <LOGIN PASSWORD> sp_adduser '<CORRESPONDING LOGIN>', '<!!--USERNAME--!!>'

Secure default login exists	USE master execute sp_configure 'secure default login', 0, '' RECONFIGURE
Roles without passwords	USE master ALTER ROLE <!!--ROLE--!!> ADD PASSWD <NEW PASSWORD>
Require message confidentiality with encryption	USE master execute sp_configure 'msg confidentiality reqd', 1 execute sp_configure 'use security services', 1 RECONFIGURE
Event log computer name	USE master sp_configure 'event log computer name', 0, '<YOUR SERVER NAME>'
Use security services	USE master sp_configure 'use security services', 1 RECONFIGURE
Default SAP password"USE master	sp_password <CURRENT PASSWORD>, <NEW PASSWORD>, <!!--LOGIN--!!>
Audit queue size	USE master sp_configure 'audit queue size', <NEW VALUE>
Log audit logon success	USE master sp_configure 'log audit logon success', 1 RECONFIGURE
Default password for PortalAdmin	USE master sp_password <CURRENT PASSWORD>, <NEW PASSWORD>, 'PortalAdmin'
Default password for pkiuser	USE master sp_password <CURRENT PASSWORD>, <NEW PASSWORD>, 'pkiuser'
Password same as login name	USE master sp_password <CURRENT PASSWORD>, <NEW PASSWORD>, <!!--LOGIN--!!>
Guest user exists in database	USE <!!--DATABASE--!!> sp_dropuser guest

System-wide password expiration	USE master sp_configure 'systemwide password expiration', 90 RECONFIGURE
Audit logout not set	USE master sp_auditoption 'logouts', <CHOOSE 'on'|'off'> sp_audit 'logout', 'all', 'all', <CHOOSE 'on'|'fail'|'pass'> "
Permission granted on system table	USE <!!--DATABASE--!!> REVOKE SELECT ON <!!--DATABASE--!!>.<!!--OWNER--!!>.<!!--OBJECT--!!> FROM <!!--GRANTED TO--!!>
xp_cmdshell not removed	USE master sp_dropextendedproc xp_cmdshell
Permission to select from syslogins	USE master REVOKE <!!--PRIVILEGE--!!> ON master.dbo.syslogins FROM <!!--GRANTED TO--!!>
xp_cmdshell context	USE master sp_configure 'xp_cmdshell context', 1 RECONFIGURE
Current audit table	USE master sp_configure ""current audit table"", <CURRENT AUDIT TABLE> <, ""with truncate"">
Minimum password length	USE master sp_configure 'minimum password length', <NEW VALUE>
Maximum failed logins	USE master sp_configure 'maximum failed logins', <NEW VALUE>
Check password for digit	USE master sp_configure 'check password for digit', 1 RECONFIGURE
Default password for PIAdmin	USE master sp_password <CURRENT PASSWORD>, <NEW PASSWORD>, 'PIAdmin'
Updates allowed to system tables	USE master sp_configure 'allow updates to system tables', 0 RECONFIGURE

IBM DB2 FIX SCRIPTS

Check	Script
Permissions to list users	REVOKE CONTROL ON <!!--TABLE NAME--!!> TO PUBLIC REVOKE ALTER ON <!!--TABLE NAME--!!> TO PUBLIC REVOKE DELETE ON <!!--TABLE NAME--!!> TO PUBLIC REVOKE INDEX ON <!!--TABLE NAME--!!> TO PUBLIC REVOKE INSERT ON <!!--TABLE NAME--!!> TO PUBLIC REVOKE SELECT ON
Permissions granted to PUBLIC	REVOKE <!!--PRIVILEGE--!!> FROM publicthx
Permissions granted to PUBLIC	REVOKE <!!--PRIVILEGE--!!> ON <!!--TABLE--!!> FROM public
Permissions granted to PUBLIC	REVOKE <!!--PRIVILEGE--!!> ON <!!--SCHEMA--!!> FROM public
CREATE_NOT_FENCED privilege granted	REVOKE CREATE_NOT_FENCED ON DATABASE FROM PUBLIC REVOKE CREATE_NOT_FENCED ON DATABASE FROM USER <!!--GRANTED TO--!!> REVOKE CREATE_NOT_FENCED ON DATABASE FROM GROUP <!!--GRANTED TO--!!>
Permissions granted to PUBLIC	REVOKE <!!--PRIVILEGE--!!> ON <!!--INDEX--!!> FROM public
Permissions granted to PUBLIC	REVOKE <!!--PRIVILEGE--!!> ON <!!--COLUMN--!!> FROM public
Auditing buffer size	UPDATE DATABASE MANAGER CONFIGURATION USING AUDIT_BUF_SZ <NEW VALUE>
Permissions granted to user	REVOKE <!!--PRIVILEGE--!!> ON INDEX <!!--INDEX--!!> FROM <!!--GRANTED TO--!!>
Permissions granted to user	REVOKE <!!--PRIVILEGE--!!> ON SCHEMA <!!--SCHEMA--!!> FROM <!!--GRANTED TO--!!>
Permissions granted to user	REVOKE <!!--PRIVILEGE--!!> ON <!!--TABLE--!!> FROM <!!--GRANTED TO--!!>
Permissions granted to user	REVOKE <!!--PRIVILEGE--!!> FROM <!!--GRANTED TO--!!>

Check	Script
Permissions to list users	REVOKE CONTROL ON <!!--TABLE NAME--!!> TO PUBLIC REVOKE ALTER ON <!!--TABLE NAME--!!> TO PUBLIC REVOKE DELETE ON <!!--TABLE NAME--!!> TO PUBLIC REVOKE INDEX ON <!!--TABLE NAME--!!> TO PUBLIC REVOKE INSERT ON <!!--TABLE NAME--!!> TO PUBLIC REVOKE SELECT ON
AUTHENTICATION parameter type	UPDATE DBM CFG USING AUTHENTICATION <NEW METHOD>
AUTHENTICATION parameter set to DCS	UPDATE DBM CFG USING AUTHENTICATION DCS_ENCRYPT
Permissions on system catalog	REVOKE CONTROL ON <!!--TABLE NAME--!!> TO PUBLIC REVOKE ALTER ON <!!--TABLE NAME--!!> TO PUBLIC REVOKE DELETE ON <!!--TABLE NAME--!!> TO PUBLIC REVOKE INDEX ON <!!--TABLE NAME--!!> TO PUBLIC REVOKE INSERT ON <!!--TABLE NAME--!!> TO PUBLIC REVOKE SELECT ON
AUTHENTICATION parameter set to SERVER	UPDATE DBM CFG USING AUTHENTICATION SERVER_ENCRYPT
AUTHENTICATION parameter set to CLIENT	UPDATE DBM CFG USING AUTHENTICATION SERVER_ENCRYPT
Permissions granted to user	REVOKE <!!--PRIVILEGE--!!> ON <!!--COLUMN--!!> FROM <!!--GRANTED TO--!!>

MYSQL FIX SCRIPTS

Check	Script

Easily-guessed root password	UPDATE user SET Password=PASSWORD('<NEW PASSWORD>') WHERE user='root';
	FLUSH PRIVILEGES;

FILE privileges granted	REVOKE FILE ON *.* FROM '<!!--USER--!!>'@'<!!--HOST--!!>';
	FLUSH PRIVILEGES;

PROCESS privileges granted	REVOKE PROCESS ON *.* FROM '<!!--USER--!!>'@'<!!--HOST--!!>';
	FLUSH PRIVILEGES;

Password for user same as username	UPDATE user SET Password=PASSWORD('<NEW PASSWORD>') WHERE user='<!!--USER--!!>'@'<!!--HOST--!!>';
	FLUSH PRIVILEGES;

Sample database not removed	DROP DATABASE <!!--SAMPLE DATABASE--!!>

Easily-guessed account passwords	UPDATE user SET Password=PASSWORD('<NEW PASSWORD>']) WHERE user='<!!--USER--!!>'@'<!!--HOST--!!>';
	FLUSH PRIVILEGES;

Blank root password	UPDATE user SET Password=PASSWORD('<NEW PASSWORD>') WHERE user='root';
	FLUSH PRIVILEGES;

Default passwords for test accounts	REVOKE ALL ON *.* FROM '<!!--USER--!!>'@'<!!--HOST--!!>';
	DELETE FROM user WHERE User='<!!--USER--!!>'@'<!!--HOST--!!>';
	FLUSH PRIVILEGES;

Blank account passwords	UPDATE user SET Password=PASSWORD('<NEW PASSWORD>') WHERE user='<!!--USER--!!>'@'<!!--HOST--!!>';
	FLUSH PRIVILEGES;

Anonymous user exists	DELETE FROM mysql.user WHERE User = '<!!--USER--!!>'@'<!!--HOST--!!>';

Appendix K: Backing Up, Restoring, Archiving, and Purging Alerts

Recording events that produce a heavy volume of data in DbProtect Audit and Threat Management may diminish system performance when used for reporting. Also, large data collection creates storage issues as Informational Alerts (a/k/a "audit Alerts") consume disk space at a steady rate.

One solution: back up Alerts that are no longer needed from the database into another physical archive for storage. The Alerts are available for restoration, but set aside so current data analysis performance is expedited. Once you have moved audit Alerts to the backup tables, you can purge the data from your database.

This document explains how to archive, restore, purge, and export Alerts. It consists of the following topics:

- *Understanding the AppSecInc-provided SQL script, backup tables, and stored procedures*
- *Setup*
- *Backing up your Security and Informational Alerts*
- *Restoring your Security and Informational Alerts*
- *Archiving and purging Your Security and Informational Alerts*
- *Stored procedures for purging Security Alerts and Informational Alerts.*

Understanding the AppSecInc-provided SQL script, backup tables, and stored procedures

AppSecInc provides a **SQL script** called `appradar_ext_alert_backup.sql` (available from Application Security, Inc. Customer Support; for more information, see *Customer Support*).

The `appradar_ext_alert_backup.sql` script creates the following **backup tables** and related indexes:

- `ins_alerts_security_backup`
- `ins_alerts_info_backup`
- `ins_origins_backup`
- `ins_sql_backup`

These backup tables are temporary storage areas for Security and Informational Alerts that should be archived.

The `appradar_ext_alert_backup.sql` script also creates the following **stored procedures**:

- `appdetective.dbo.arcx_spBackupAlerts @cutoff_end_date`
- `appdetective.dbo.arcx_spRestoreAlerts.`

Setup

Before you back up your Security and Informational Alerts, do the following:

1. Run the following SQL script: `appradar_ext_alert_backup.sql`.

Note: You only need to run this script **once**.

Backing up your Security and Informational Alerts

You can **back up** your Security and Informational Alerts -- based on their event-generated timestamp -- *from* the system Alert tables *into* the backup tables.

This topic consists of the following sub-topics:

- *Backup*
- *Backup Example.*

BACKUP

To **back up** your Security and Informational Alerts:

1. Stop the `Message Collector` service.

Note: You will **not** lose any Security and Informational Alert activity. Sensors temporarily store new Security and Informational Alerts in the replay logs until the Message Collector is ready to accept incoming Security and Informational Alerts again.

2. Execute the `arcx_spBackupAlerts` stored procedures to back up your Security and Informational Alerts. Be sure to specify an end date for your backup; for more information, see the *Backup Example*.
3. Restart the `Message Collector` service.

BACKUP EXAMPLE

If you want to move all Security and Informational Alerts generated any time on or before September 1, 2005, execute the `arcx_spBackupAlerts` stored procedure. The time it takes for this procedure to complete depends on the number of Security and Informational Alerts that match the date and time criteria.

```
use appdetective

go

exec appdetective.dbo.arcx_spBackupAlerts '9/1/2005 23:59:59'

go
```

Note: The date/time parameter is **required**.

Restoring your Security and Informational Alerts

This topic consists of the following sub-topics:

- *Restoration*.
- *Restoration example*.

Note: This procedure restores **all** your existing backed-up data.

RESTORATION

To **restore** your Security and Informational Alerts:

1. Stop the `Message Collector` service.

Note: You will **not** lose any Security and Informational Alert activity. Sensors temporarily store new Security and Informational Alerts in the replay logs until the Message Collector is ready to accept incoming Security and Informational Alerts again.

2. Execute the `arcx_spRestoreAlerts` stored procedure to restore your Security and Informational Alerts; for more information, see the *Restoration example*.
3. Restart the `Message Collector` service.

RESTORATION EXAMPLE

If you want to restore the Security and Informational Alerts to the DbProtect Audit and Threat Management processing tables, execute the `arcx_spRestoreAlerts` stored procedure.

```
use appdetective

go

exec appdetective.dbo.arcx_spRestoreAlerts

go
```

This restores all Security and Informational Alerts from the backup tables and returns them to the DbProtect Audit and Threat Management processing tables.

Archiving and purging Your Security and Informational Alerts

Once you have moved Audits to the backup tables, you can **archive** them using a utility such as Microsoft SQL Server's Data Transformation Services or bcp. Once you have archived your data, you can clear the backup tables by **purging** them, as follows:

- `truncate table ins_alerts_security_backup`
- `truncate table ins_alerts_info_backup`
- `truncate table ins_origins_backup`
- `truncate table ins_sql_backup`

Stored procedures for purging Security Alerts and Informational Alerts

This topic consists of the following sub-topics:

- *Purging*
- *Purging Examples (Required Stored Procedures)*.

PURGING

The following AppSecInc-provided stored procedures allow you to purge your database completely and irreversibly of all Alerts (Security and Informational).

The following stored procedures are **required**:

- `appdetective.dbo.arc_spPurgeSecurityAlerts @beforeAndIncludingTime`
- `appdetective.dbo.arc_spPurgeInfoAlerts @beforeAndIncludingTime`

Note: The date/time parameters are **required**.

The following stored procedures are **optional**:

- `arc_spPurgeOrphanOrigins`
- `arc_spPurgeOrphanSQLS`.

Note: The purging stored procedures are included in the DbProtect installation, **not** in the attached .zip file.

The following table explains each stored procedure used to purge Security and Informational Alerts:

Stored Procedure	Explanation
`appdetective.dbo. arc_spPurgeSecurityAlerts @beforeAndIncludingTime`	You must run this **required** stored procedure if you want to purge Security Alerts from the `ins_alerts_security` table. The date/time parameter is **required**.
`appdetective.dbo. arc_spPurgeInfoAlerts @beforeAndIncludingTime`	You must run this **required** stored procedure if you want to purge Informational Alerts from the `ins_alerts_info` table. The date/time parameter is **required**.
`arc_spPurgeOrphanOrigins`	If you run either of the stored procedures, above, you can run these two **optional** stored procedures to purge related Security and Informational Alert data from the `ins_origins` and `ins_sql` tables.
`arc_spPurgeOrphanSQL`	

To run the stored procedures used to purge Security and Informational Alerts (and, optionally, related table data):

1. Stop the `Message Collector` service.
2. Execute required stored procedures.

If you want to purge:

- Security Alerts from the `ins_alerts_security` table, then execute the following **required** stored procedure: `appdetective.dbo. arc_spPurgeSecurityAlerts @beforeAndIncludingTime`
- Informational Alerts from the `ins_alerts_info` table, then execute the following **required** stored procedure: `appdetective.dbo. arc_spPurgeInfoAlerts @beforeAndIncludingTime`.

Note: The date/time parameters are **required**.

For more information, see *Purging Examples (Required Stored Procedures)*.

Execute optional stored procedures.

If you want to purge related Security and Informational Alert data from the:

- `ins_origins` table, then execute the following **optional** stored procedure: `arc_spPurgeOrphanOrigins`
- `ins_sql` table, then execute the following **optional** stored procedure: `arc_spPurgeOrphanSQL`.

3. Re-start the `Message Collector` service.

PURGING EXAMPLES (REQUIRED STORED PROCEDURES)

If you want to purge Security Alerts generated any time on or before September 1, 2005 from the `ins_alerts_security` table, then execute the following **required** stored procedure:

```
appdetective.dbo. arc_spPurgeSecurityAlerts '9/1/2005 23:59:59'
```

If you want to purge Informational Alerts generated any time on or before September 1, 2005 from the `ins_alerts_info` table, then execute the following **required** stored procedure:

```
appdetective.dbo. arc_spPurgeInfoAlerts '9/1/2005 23:59:59'
```

The date/time parameters are **required**.

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

In order to run a Discovery, Pen Test, or Audit against a Microsoft SQL Server database, certain ports on the machine running Microsoft SQL Server **must** be open. This appendix consists of the following topics:

- *Open Ports (on Computers Running Microsoft SQL Server) Required to Run a Discovery*
- *Open Ports (on Computers Running Microsoft SQL Server) Required to Run a Pen Test*
- *Open Ports (on Computers Running Microsoft SQL Server) Required to Run an Audit*.

Open Ports (on Computers Running Microsoft SQL Server) Required to Run a Discovery

To Discover Microsoft SQL Server on the default port:

- TCP: `1433` Microsoft SQL Server default port.

  OR:

- UDP: `1434` Microsoft SQL Monitor.

Note: Microsoft SQL Server 2005/2008 requires the Microsoft SQL Server Browser service to run on the target server.

To Discover Microsoft SQL Server on a non-default port:

- TCP: Any port number for the default instance or named instances.

  OR:

- UDP: `1434` Microsoft SQL Monitor.

Note: Microsoft SQL Server 2005/2008 requires the Microsoft SQL Server Browser service to run on the target server.

Open Ports (on Computers Running Microsoft SQL Server) Required to Run a Pen Test

TCP: 1433 Microsoft SQL Server default port or any port number for the default instance or named instances.

Open Ports (on Computers Running Microsoft SQL Server) Required to Run an Audit

To connect to Microsoft SQL Server via named pipes:

- **TCP:** 135 Service Control Manager, 445 Microsoft Directory Service, DCOM dynamic ports (1024-65535).

Note: DCOM dynamically allocates TCP and UDP ports in the range 1024-65535.

To connect to SQL Server via TCP/IP:

- **TCP:** 135 Service Control Manager, 445 Microsoft Directory Service, 1433 SQL Server default port or any port number for the default instance or named instances, DCOM dynamic ports (1024-65535).

Note: DCOM dynamically allocates TCP and UDP ports in the range 1024-65535.