DbProtect™

DbProtect 2009.1R5 Administrator's Guide

October 16, 2009

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

Contents

Chapter 1 - Introduction

This chapter explains what's in the *DbProtect Administrator's Guide*, the intended audience, and the components of DbProtect.

What you will find in this chapter:

- *Product, Guide, and Documentation Suite Overview*
- *Intended Audience*
- *DbProtect Version Compatibility Matrix, and Determining the Current Version of Installed DbProtect Applications*
- *Customer Support*.

Product, Guide, and Documentation Suite Overview

This section includes an overview, an explanation of conventions used, and a listing of other DbProtect guides available for customers.

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, structured risk mitigation, and real-time intrusion monitoring, 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 and threat 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 chapters:

- *Chapter 2 - Overview of DbProtect Administration*
- *Chapter 3 - Performing ASAP Updates and DbProtect Upgrades*
- *Chapter 4 - Starting and Stopping DbProtect*
- *Chapter 5 - Monitoring the Health of DbProtect*
- *Chapter 6 - Data Management*
- *Appendices.*

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 the day-to-day administration of the Db Protect, including the Console, Scan Engines, Sensors, and the back-end database. 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 dackups.
- **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 Version Compatibility Matrix, and Determining the Current Version of Installed DbProtect Applications

This section includes a **DbProtect version compatibility matrix**, and instructions which explain how to determine the current version of any installed DbProtect application (including the Console, Database Component, Scan Engine, and Sensor).

DbProtect version compatibility matrix

The DbProtect version compatibility matrix is below:

Suite Version	Supported Versions of:				
	Console Management Server	Database Component	Scan Engine	Sensor	Analytics
2009.1R5	4.2	2.2	6.1, 6.0, 5.8, 5.7, 5.6	3.10, 3.9, 3.8	1.3
2009.1R4	4.1	1.7	6.0, 5.8, 5.7, 5.6, 5.5	3.9, 3.8, 3.7	1.2
2009.1R3	4.0	1.5	5.8, 5.7, 5.6, 5.5	3. 8, 3.7, 3.6, 3.5, 3.4	1.0, 1.1
2009.1R2	3.11	1.4	5.7, 5.6, 5.5, 5.4.7, 5.4.6	3.7, 3.6, 3.5, 3.4, 3.3, 3.2	1.0
2009.1	3.10	1.3	5.6, 5.5, 5.4.7, 5.4.6	3.6, 3.5, 3.4, 3.3, 3.2	

Suite Version	Supported Versions of:				
	Console Management Server	Database Component	Scan Engine	Sensor	Analytics
2008.3	3.9	1.3, 1.2, 1.1, 1.0	5.6, 5.5, 5.4.7, 5.4.6	3.6, 3.5, 3.4, 3.3, 3.2	N/A
2008.2	3.8	1.3, 1.2, 1.1, 1.0	5.6, 5.5, 5.4.7, 5.4.6	3.6, 3.5, 3.4, 3.3, 3.2	
2008.1R2	3.7	1.3, 1.2, 1.1, 1.0	5.6, 5.5, 5.4.7, 5.4.6	3.6, 3.5, 3.4, 3.3, 3.2	
2008.1	3.6	1.3, 1.2, 1.1, 1.0	5.6, 5.5, 5.4.7, 5.4.6	3.6, 3.5, 3.4, 3.3, 3.2	

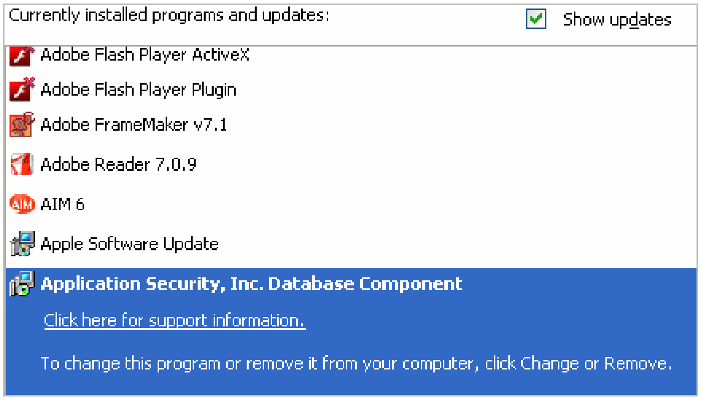
Determining the current version of any installed DbProtect software component

To determine the current version of any installed DbProtect software component:

1. Choose **Start > Control Panel** to display the **Control Panel** dialog box.
2. Double click the **Add or Remove Programs** icon to display the **Add or Remove Programs** dialog box.

3. Click any of the following DbProtect applications (assuming they are currently installed on your computer):

- **DbProtect Console Management Server**
- **AppSecInc Database Component**
- **DbProtect Scan Engine**
- **DbProtect Sensor**
- **DbProtect Console Message Collector**
- **DbProtect Analytics**.


Currently installed programs and updates:

☑ Show updates

Adobe Flash Player ActiveX

Adobe Flash Player Plugin

Adobe FrameMaker v7.1

Adobe Reader 7.0.9

AIM 6

Apple Software Update

Application Security, Inc. Database Component

Click here for support information.

To change this program or remove it from your computer, click Change or Remove.

FIGURE: **Add or Remove Programs** dialog box (**Application Security, Inc. Database Component** highlighted)

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`

Chapter 2 - Overview of DbProtect Administration

This chapter provides an oveview of DbProtect administration.

What you will find in this chapter:

- *Indentifying DbProtect Components*
- *DbProtect User Administration.*

Indentifying DbProtect Components

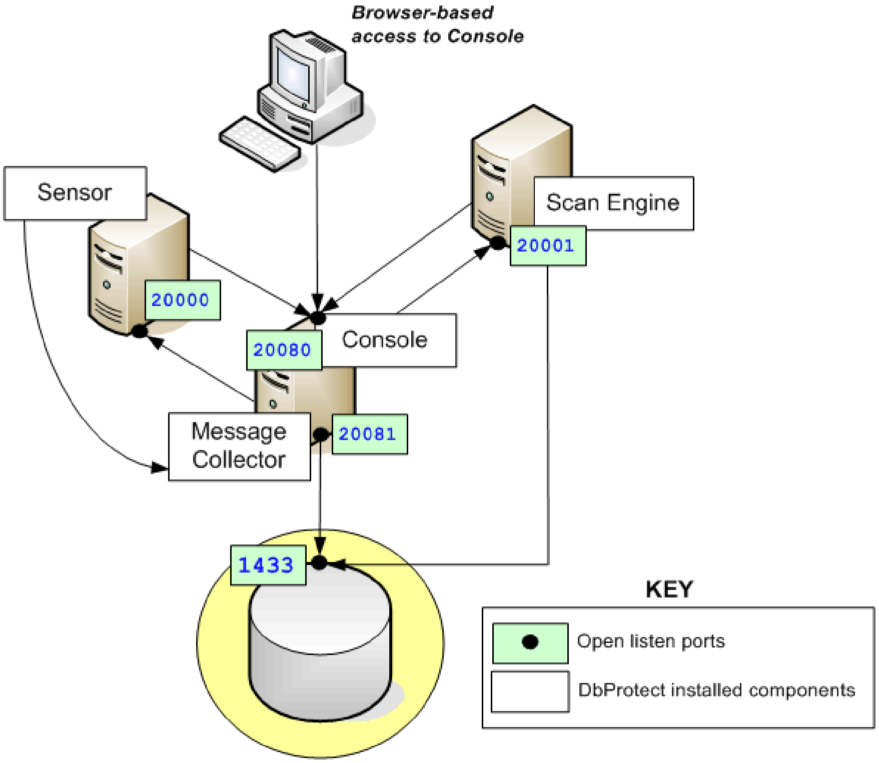
This section is intended to help you understand and identify the DbProtect software release components.

What you will find in this section:

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

Conceptual diagram

The following **conceptual diagram** illusrates how the DbProtect components and sub-components interact.



Console

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

For more information on:

- minimum system requirements and installation instructions for the Console, see the *DbProtect Installation Guide*
- working with DbProtect Audit and Threat Management and DbProtect Vulnerability Management, see the *DbProtect User’s 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, 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, see *Sensors*.

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, Linux, and Windows
- **DB2** on Linux, AIX, Solaris, and Windows.

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
	AIX
	SOLARIS
	WINDOWS
ORACLE	SOLARIS
	AIX
	HP-UX
	LINUX
	WINDOWS

For information on 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.

Note: The network-based Sensor only runs on the Windows OS, but the databases it monitors do **not** need to be running on Windows.

DB	OS
DB2	WINDOWS
SYBASE	
ORACLE	

For information on minimum system requirements and installation instructions for the Sensors, 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*.

DbProtect User Administration

For information on managing roles in DbProtect, see *DbProtect User Roles* in the *DbProtect User’s Guide*.

Chapter 3 - Performing ASAP Updates and DbProtect Upgrades

DbProtect allows you to:

- **ASAP Update** your **Scan Engines** so they will contain new Rules for Policies to improve detect vulnerabilities; for more information, see *Performing an ASAP Update of Rules in your Sensors*
- **upgrade** your Console, Sensors, and Scan Engines; for more information, see *Upgrading DbProtect Components*.

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.*

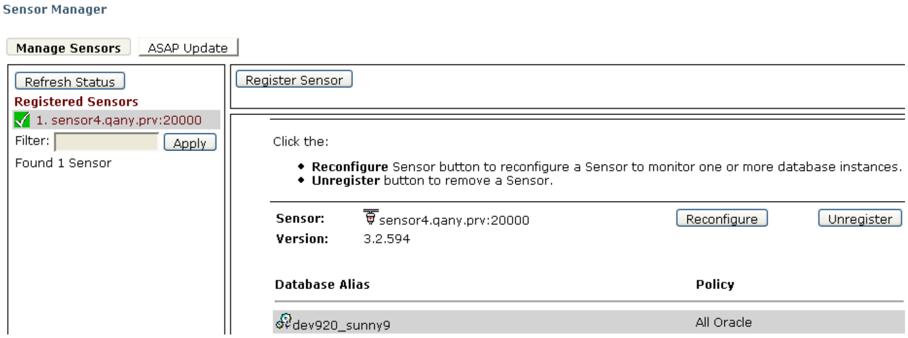
- the **Sensor** is **registered** (for more information, see *Registering a Sensor* in the *DbProtect User's Guide*)
- the Sensor does **not** already contain the latest available security Rules from the Application Security, Inc. security Rules **knowledgebase**.

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* in the *DbProtect User's Guide*.

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.



Registered Sensors

✓ 1. sensor4.qany.prv:20000

Found 1 Sensor

Click the:

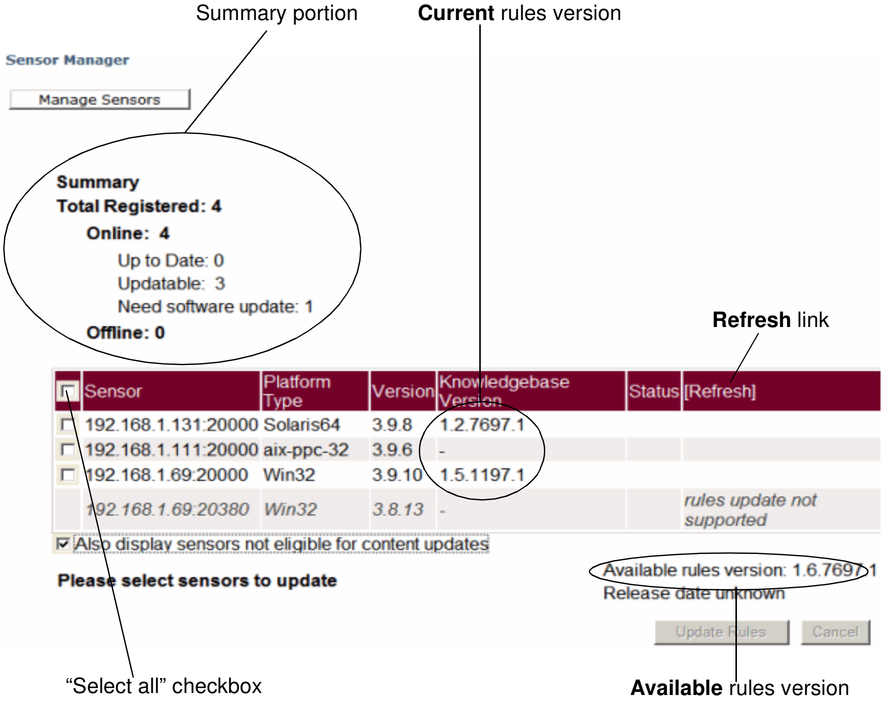
- **Reconfigure** Sensor button to reconfigure a Sensor to monitor one or more database instances.
- **Unregister** button to remove a Sensor.

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**.



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* in the *DbProtect User's Guide*
- **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 *Upgrading DbProtect Components*)
- 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*.

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 *Upgrading DbProtect Components*.

- **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 AppRadar 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* in the *DbProtect User's Guide*.

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.

Upgrading DbProtect Components

What you will find in this section:

- *Upgrading your DbProtect components*
- *Warning about pre-defined dictionary file content and location changes after a DbProtect component upgrade.*

Upgrading your DbProtect components

A DbProtect **upgrade** is similar to an ASAP Update, except when you upgrade a Console, Sensor, or Scan Engine, you just install a newer version over an older version. For more information on installing DbProtect components, see the *DbProtect Installation Guide*.

Warning about pre-defined dictionary file content and location changes after a DbProtect component upgrade

When you upgrade the Console to version 3.11 or greater, pre-defined dictionary files for Easily-Guessed Password Checks, which used to reside in `c:\Program Files\AppSecInc\AppDetective`, are automatically moved to a new location: `c:\Program Files\AppSecInc\Common Files`.

If you edit a pre-defined dictionary file (i.e. `sqlsvr-large-dictionary.txt`) and save it under the same name, and then upgrade your Console to version 3.11 or greater, not only will the `sqlsvr-large-dictionary.txt` file location change -- so will its content (i.e., the content is overwritten by the new dictionary file in Console version 3.11 or greater).

Workaround: Save your customized dictionary file as a different name (e.g, `sqlsvr-large-dictionary-mydictionary.txt`), not the default name (i.e., `sqlsvr-large-dictionary.txt`).

Chapter 4 - Starting and Stopping DbProtect

What you will find in this chapter:

- *Logging into the Console*
- *Starting and stopping the Sensors.*

Logging into the Console

Caution! Some older version of Google Desktop (5.1 and earlier) may cause problems when loading the 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 Console via a web browser. For more information, see the *Console - Minimum System Requirements* section in the *DbProtect Installation Guide*.

To log into the Console:

1. Do one of the following:

- Choose **Start** > **All Programs** > **AppSecInc** > **DbProtect**.
- 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

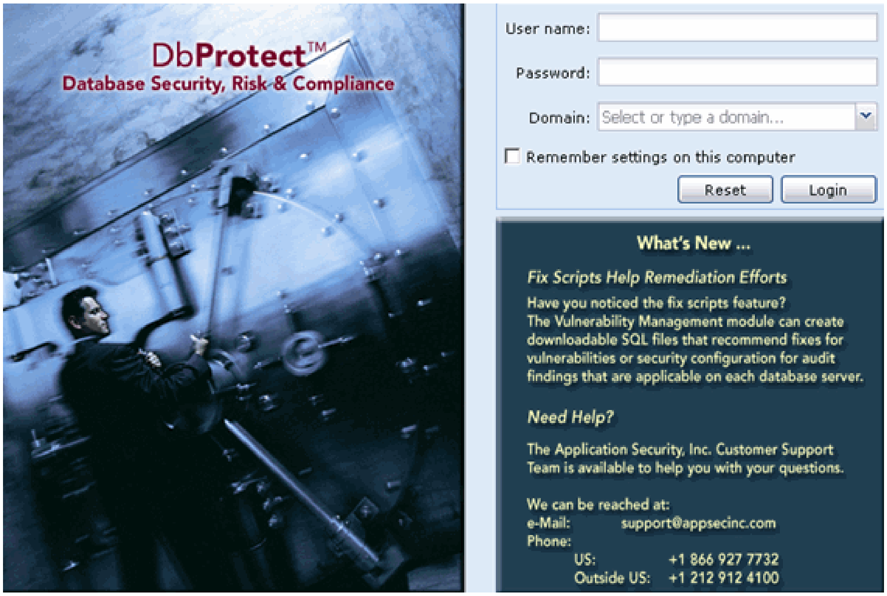
  -`InstallPort` is the port number entered during installation.

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

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

2. Click the **OK** button to display the 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: 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 Rest button to reset the entered **Username:**, **Password:** and **Domain:** login values.

4. Click the **Login** button to display the Console splash page.

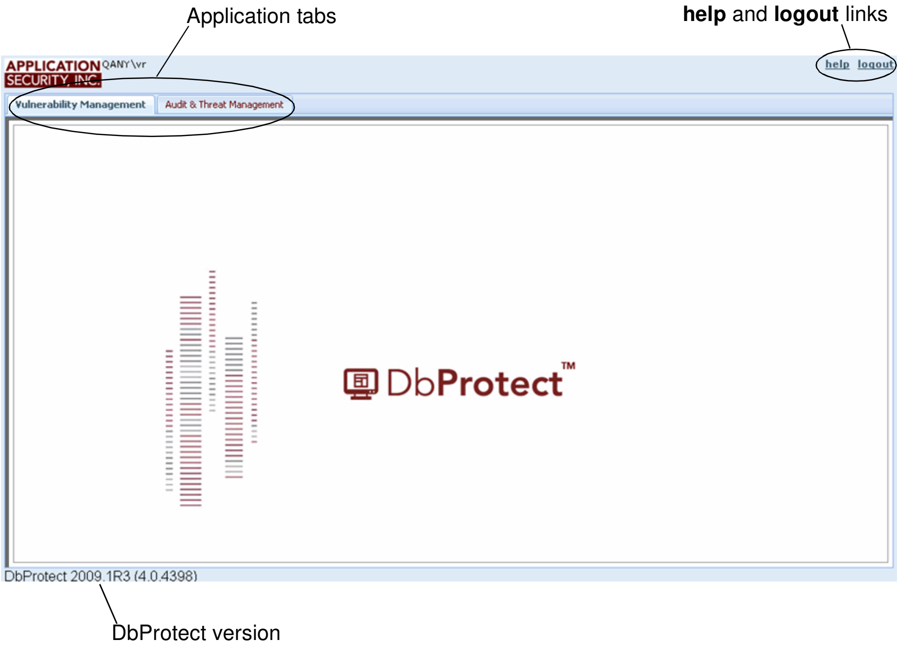


FIGURE: Console splash page

The Console splash page consists of:

- application tabs (**Vulnerability Management** and **Audit & Threat Management**) in the upper left corner
- **help** and **logout** links (in the upper right corner), which allow you to display the DbProtect online help and log out of DbProtect, respectively
- your DbProtect version (lower left corner).

5. In the application tabs portion of the Console splash page, you can click the:

- **Vulnerability Management** tab to display DbProtect Vulnerability Management
- **Audit & Threat Management** to display DbProtect Audit and Threat Management.

For more information on using DbProtect Vulnerability Management and DbProtect Audit and Threat Management, see the *DbProtect User's Guide*.

Starting and stopping the Sensors

What you will find in this help topic:

- *Starting and stopping the Sensors on Windows*
- *Starting and stopping the Sensors on *nix platforms.*

STARTING AND STOPPING THE SENSORS ON WINDOWS

There are four DbProtect services:

- `DbProtect Message Collector`
- `DbProtect Console`
- `DbProtect Scan Engine`
- `DbProtect Sensor`

You only need to start the `DbProtect Sensor` service in order for DbProtect to collect data from Sensors, and for you to connect to DbProtect. These services are configured to start whenever Windows starts.

There are several ways to start and stop the services on Windows.

Starting a Sensor from the command line

To start a Sensor from the command line:

1. Choose **Start** > **Run**.

The **Run** dialog box displays.

2. Enter `cmd.exe` in the **Open** field.

Click the **OK** button.

A command window displays.

3. Enter the following to start the service:

```
C:\> net start ServiceName
```

where `ServiceName` is one of the following:

- `DbProtect Message Collector`
- `DbProtect Console`
- `DbProtect Scan Engine`
- `DbProtect Sensor`

The following messages display:

```
The ServiceName service is starting.

The ServiceName service was started successfully.
```

Stopping a Sensor from the command line

To stop a Sensor from the command line:

1. Choose **Start** > **Run**.

The **Run** dialog box displays.

2. Enter `cmd.exe` in the **Open** field.

Click the **OK** button.

A command window displays.

3. Enter the following to stop the service:

```
C:\> net stop ServiceName
```

where `ServiceName` is one of the following:

- `DbProtect Message Collector`
- `DbProtect Console`
- `DbProtect Scan Engine`
- `DbProtect Sensor`

The following messages display:

```
The ServiceName service is stopping.

The ServiceName service was stopped successfully.
```

Starting a Sensor from the Control Panel

To start a Sensor from the Control Panel:

1. Choose **Start** > **Control Panel**.

The **Control Panel** dialog box displays.

2. Double click the **Administrative Tools** icon.

The **Administrative Tools** dialog box displays.

3. Double click the **Services** icon.

The Services dialog box displays.

4. Highlight any of the following services:

- `DbProtect Message Collector`
- `DbProtect Console`
- `DbProtect Scan Engine`
- `DbProtect Sensor`

5. Click the **Start** link.

A **Service Control** pop-up displays, and the service starts. The **Status** column in the Services dialog box should read **Started**.

Stopping a Sensor from the Control Panel

To stop a Sensor from the Control Panel:

1. Choose **Start** > **Control Panel**.

The **Control Panel** dialog box displays.

2. Double click the **Administrative Tools** icon.

The **Administrative Tools** dialog box displays.

3. Double click the **Services** icon.

The **Services** dialog box displays.

4. Highlight any of the following services:

- `DbProtect Message Collector`
- `DbProtect Console`
- `DbProtect Scan Engine`
- `DbProtect Sensor`

5. Click the **Stop** link.

A **Service Control** pop-up displays, and the service stops. The **Status** column in the **Services** dialog box should be blank.

STARTING AND STOPPING THE SENSORS ON *NIX PLATFORMS

To start and stop the Sensors on a *nix platform:

1. To **start** a host-based Sensor on a *nix platform, do the following:
   - Log in as the user you created in during the installation process (`appradar`, for example).
   - Once you are successfully authenticated as this user, go to the `/util` directory where you installed the host-based Sensor (for example: `/opt/ASIappradar/sensor/util`).
   - Run the command: `./appradar_start`
2. To **stop** a host-based Sensor on a *nix platform, do the following:
   - Log in as the user you created in during the installation process (`appradar`, for example).
   - Once you are successfully authenticated as this user, go to the `/util` directory where you installed the host-based Sensor (for example: `/opt/ASIappradar/sensor/util`).
   - Run the command: `./appradar_stop`

Chapter 5 - Monitoring the Health of DbProtect

What you will find in this chapter:

Monitoring the Health of Your Sensors

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 in accordance with its deployed Policies.

You can use the:

- **Sensor Manager** to determine whether your registered Sensors are "healthy"; for more information, see *Monitoring the Health of Your Sensors (Via the Sensor Manager)*
- **Dashboard** to determine whether your registered Sensors are "healthy"; for more information, see the *DbProtect User's Guide*.

A "healthy" Sensor also contains up-to-date Policies.

Hint: 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.

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:

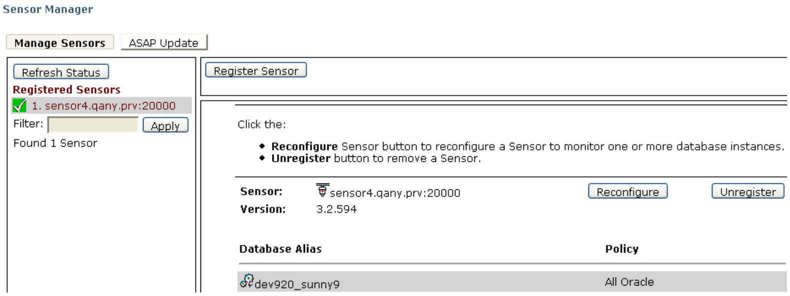
- **"up and running"** on the database SID or instance where it is registered
- **actively collecting/interpreting data and firing Alerts** to DbProtect in accordance with its deployed Policies.

To monitor the "health" of your Sensors via the **Sensor Manager**:

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 registered Sensors.



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. If the color-coded icon next to your registered Sensor is:

- **green**, then the Sensor is "healthy"
- **red**, then the Sensor is "unhealthy".

Note: Click the **Refresh Status** button to view the most current state of your Sensors' "health".

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:

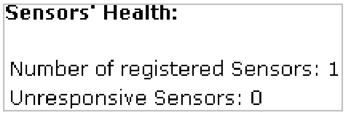
- **"up and running"** on the database SID or instance where it is registered
- **actively collecting/interpreting data and firing Alerts** to DbProtect in accordance with its deployed Policies.

To monitor the “health” of your Sensors via the **Dashboard**:

1. Do one of the following:

- Click the **Dashboard - Graphical Summary** workflow link on **Home** page.
- Click the **Dashboard** tab from anywhere on the page.

The **Dashboard** displays. The Sensor “health” portion of the **Dashboard** displays your registered Sensors.



Sensors' Health:

Number of registered Sensors: 1
Unresponsive Sensors: 0

FIGURE: **Dashboard** (Sensor “health” portion)

2. The **Sensors’ “health”** portion of the **Dashboard** allows you to view the:

- **Number of registered Sensors**
- **Unresponsive Sensors**.

An unresponsive Sensor is “unhealthy”.

Chapter 6 - Data Management

What you will find in this chapter:

- *DbProtect Backup*
- *DbProtect Restoration.*

DbProtect Backup

This section explains how to create a full, recoverable backup of your DbProtect system. It assumes you have working knowledge of Microsoft SQL Server.

What you will find in this section:

- *Which System Components Should I Back Up?*
- *DbProtect Component Backup.*

Which System Components Should I Back Up?

DbProtect is comprised of several system components distributed across your network. AppSecInc recommends you back up the following three DbProtect system components:

- **Console.** This system component is a unified, web-based front-end for DbProtect. DbProtect centralizes database security management across complex, heterogeneous environments. For more information, see **XREF**.

  By default, the Console is installed in the following directory: `C:\Program Files\AppSecInc\DbProtect`

- **Sensor.** These components monitor your Microsoft SQL Server (host-based) or Oracle server (network-based) for intrusion attempts. It can also audit normal usage. The Sensor fires Alerts of attempted and/or successful intrusions via a variety of methods. For more information, see **XREF**.

  By default, Sensors are installed in the following directory: `C:\Program Files\AppSecInc\AppRadar Sensor`
- **Data Repository.** This system component is a native Microsoft SQL Server database. It serves as the repository where essential DbProtect data is stored. This data includes DbProtect configuration details, Sensors registration data, and all Alerts sent by the Sensors to DbProtect.

DbProtect Component Backup

Note: In order to keep the system synchronized, AppSecInc recommends you back up all system components together.

What you will find in this help topic:

- *Backing Up the Data Repository*
- *Backing Up the Console*
- *Backing Up the Sensors.*

BACKING UP THE DATA REPOSITORY

Since the data repository is a SQL Server database, you can use the SQL Server backup utilities to back up the DbProtect database. For more information, see your SQL Server documentation.

1. Stop the following services:

`DbProtect`

`DbProtect Message Collector`

2. Back up the DbProtect database using Microsoft SQL Server backup utilities.

3. The Sensor captures new Alerts in the replay log; for more information, see *Replay Log Files*.

BACKING UP THE CONSOLE

To back up the Console:

1. Copy and retain the program files for the Console. You can back up:

- all files located in the following (default) directory: `<ROOT DIRECTORY>\AppSecInc\DbProtect`
- the following specific files:

```
-<ROOT DIRECTORY>\AppSecInc\DbProtect\GUI\licenses\*.*
-<ROOT DIRECTORY>\AppSecInc\DbProtect\GUI\keys\*.*
-<ROOT DIRECTORY>\AppSecInc\DbProtect\GUI\repository\*.*
-<ROOT DIRECTORY>\AppSecInc\DbProtect\Message
Collector\keys\*.*
```

where: `*.*` = all the files located in the folder.

BACKING UP THE SENSORS

To back up the Sensors:

1. Copy and retain the program files for the Sensors. You can back up:

    - all files located in the following (default) directory: `<ROOT DIRECTORY>\AppSecInc\DbProtect`
    - the following specific files:

      ```
      -<PROGRAM_ROOT>\AppSecInc\AppRadar Sensor\bin\*.pem
      -<PROGRAM_ROOT>\AppSecInc\AppRadar Sensor\bin\sensor
      -<PROGRAM_ROOT>\AppSecInc\AppRadar Sensor\conf\*.*
      -<PROGRAM_ROOT>\AppSecInc\AppRadar Sensor\Filters\*.*
      -<PROGRAM_ROOT>\AppSecInc\AppRadar Sensor\keys\*.*
      -<PROGRAM_ROOT>\AppSecInc\AppRadar Sensor\logs\*.*
      ```

    where:

    -`*.pem` = all `.pem` files located in the folder
    -`*.*` = all the files located in the folder.

DbProtect Restoration

To restore DbProtect:

1. Stop the following services:
   - `DbProtect Console`
   - `DbProtect Message Collector`
2. Restore DbProtect using Microsoft SQL Server database restoration procedures. For more information, see your Microsoft SQL Server documentation.

Note: The Sensor replays new Alerts from the replay log; for more information, see *Replay Log Files*.

3. Overwrite all existing DbProtect files with your backed-up files; for more information, see *DbProtect Backup*.
4. Overwrite all existing Sensor files with your backed-up files; for more information, see *DbProtect Backup*.
5. Re-start the following services:
   - `DbProtect Console`
   - `DbProtect Message Collector`

Appendices

What you will find in this chapter:

Appendix A: System Component Troubleshooting

You may occasionally encounter a system component-related issue. The following table lists a few, and explains how to troubleshoot them.

If:	Then:
You cannot connect to the Console	• Use your Ping utility to verify your Console machine can communicate with your Sensor machine.
	• On the Sensor machine, ensure the `DbProtect Sensor` service is running. If the service was stopped, try starting it again; for more information, see *Starting and stopping the Sensors*.
	Make sure the following DbProtect services are running: • `DbProtect Message Collector` • `DbProtect Console` For more information, see *Starting and stopping the Sensors*.
	If the DbProtect machine can communicate with the Sensor machine, and the services listed above are running, then:
	Email `support@appsecinc.com`. For faster resolution, attach the `.zip` files from DbProtect and Sensor. AppSecInc provides a utility called `collectinfo.bat` which automatically archives necessary log files.

If:	Then:
You are not receiving Alerts	• On the Sensor machine, ensure the `DbProtect Sensor` and `Message Collector` services are running. If the services were stopped, try starting it again; for more information, see *Starting and stopping the Sensors*. • Check the `appsensor.log` file for errors. It's located (by default) in `<sensor installation folder>\Program Files\AppSecInc\Sensor\logs`; for more information, see *Appendix E: DbProtect Log Files*. • Use the **Sensor Manager** or **Dashboard** to make sure the Sensor is "healthy"; for more information, see *Monitoring the Health of Your Sensors*. • Use the **Policy Manager** to ensure the Sensor's Policy is configured to send the given Alert; for more information, see the *DbProtect User's Guide*. • Make sure no Filters are deployed that might be preventing the Rule from firing; for more information, see *Filters* in the *DbProtect User's Guide*. • Next, check the `messagecollector.log` and `messagecollector_wrapper.log` files for errors; for more information, see *Appendix E: DbProtect Log Files*. • Go to the **Sensor Manager** page and click the **Unregister** button next to the Sensor. This allows you to un-register then re-register the Sensor. For more information, see the *DbProtect Installation Guide*. If clicking the **Unregister** button on the **Sensor Manager** page yields an error, you must manually remove the Sensor by executing the `force_unregister.bat` script (or `force_unregister` on Unix and Linux platforms). This script is located under the `utils` folder in the Sensor installation directory. The default location is `<sensor installation folder>\AppSecInc\Sensor\utils`. For more information, see the *DbProtect Installation Guide*. Check the `appradar_console.log` file for errors; for more information, see *Appendix E: DbProtect Log Files*. • Email `support@appsecinc.com`. For faster resolution, attach the `.zip` files from DbProtect and the Sensor. AppSecInc provides a utility called `collectinfo.bat` which automatically archives necessary log files.

If:	Then:
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.
The following error message displays: `Error Occurred. The Console database is not available at the moment. Please retry your request later.`	• Your back-end Microsoft SQL Server database instance is most likely down. • If your back-end database instance is up and running and you continue to receive this error message, email `support@appsecinc.com`. For faster resolution, attach the `.zip` files from DbProtect and the Sensor. AppSecInc provides a utility called `collectinfo.bat` which automatically archives necessary log files.
You encounter an error prompting you to delete an Oracle trace file.	This error message indicates your host-based Sensor for Oracle on a *nix platform either does not have permission to remove the Oracle trace file, or the trace file was removed already by another process. Oracle generates the trace file in its `udump` directory. A host-based Sensor for Oracle on a *nix platform reads the file, then generates the `sga-segments.log` in the Sensor's /logs directory (`<install directory>/ASIappradar/sensor/logs\`); for more information, see *Appendix E: DbProtect Log Files*. Then, the Sensor automatically deletes the trace file. The trace file is small and it is generated infrequently, so you can generally ignore the error. If the trace file exists, the user who owns the oracle process can safely delete it. Alternately, you can resolve the error by granting the host-based Sensor's user operating system "write" permission to the directory containing the trace file. This way, the Sensor can automatically delete the file on its own.

Appendix B: Troubleshooting the Java Run Time Environment (JRE) Security Settings on Internet Explorer 6 and 7

If you are experiencing difficulty logging in and connecting to DbProtect, you may need to troubleshoot the Java Runtime Environment (JRE) security settings on your Internet Explorer (IE) 6 or 7 web browser. This appendix explains how.

If your web browser is IE 6. Proper 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. To troubleshoot this problem, see *Enabling proper Active X controls and “enable third-party browser extensions” security settings (using IE 6)*.

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 troubleshoot this problem, see *Ensuring JRE 1.6 is Enabled and Temporarily Disabling Other JREs on Your Client Machine (Using IE 7).*

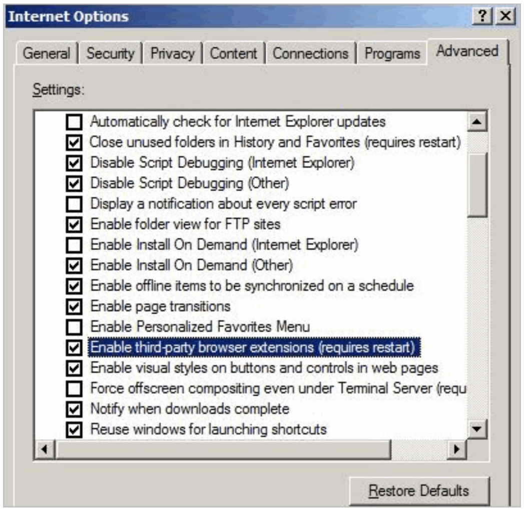
Enabling proper Active X controls and "enable third-party browser extensions" security settings (using IE 6)

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:

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`.

Ensuring JRE 1.6 is Enabled and Temporarily Disabling Other JREs on Your Client Machine (Using IE 7)

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

1. Launch IE 7.
2. Do the following:
   - Choose: **Tools > Internet Options**.
   - Click the Advanced tab.

The **Settings** dialog box displays.

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.
7. Try to log back into the DbProtect Console; for more information. If you continue to experience trouble, contact AppSecInc Customer Support at `support@appsecinc.com`.

Appendix C: Understanding the Syslog Message Format (with Sample Syslog Message)

This appendix consists of the following topics:

- *Understanding the ArcSight CEF Format for Syslog Messages*
- *Modifying the Syslog Configuration*
- *Syslog Error Logging*
- *Syslog Message Format*
- *Sample Syslog Message*.

Understanding the ArcSight CEF Format for Syslog Messages

The 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.

Modifying the Syslog Configuration

You can modify the Syslog configuration **without** restarting the Sensor by deploying a new `sensor.xml` file.

Syslog Error Logging

The Syslog dispatcher does **not** send messages about its own status to the DbProtect Console or to the intended recipients of Syslog messages. Instead, DbProtect logs these errors on the Sensor side in the `appsensor.log` file. Since UDP is a connection-less protocol, the Syslog dispatcher receives no notification that its messages are being received, so it does not have any mechanism for replaying Alerts like the DbProtect Console dispatcher. If DbProtect:

- can resolve a hostname with an IP address, the Syslog dispatcher assumes the address is valid and sends Syslog alerts to it until instructed otherwise by the DbProtect Console
- **cannot** resolve a hostname, an error message is written to `appsensor.log`.

Syslog Message Format

Each Syslog message is UTF-8 encoded and has a maximum length of 1024 bytes. The DbProtect Syslog messages adhere to the following format:

```
<Pri>Time Hostname Prefix Extension
```

Where:

- `Pri` is the sum of the Syslog "priority" and "facility" codes, as defined by the Syslog network protocol standard. The facility DbProtect sends is always `LOG_USER` and the priority is either `LOG_ALERT` (for severity of **High**, **Medium**, and **Low**) or `LOG_INFO` (for any **Info** severities). The `LOG_USER` code maps to the number `8`, the `LOG_ALERT` code maps to `1`, and the `LOG_INFO` code maps to `6`, which means that the `Pri` should have either value `9` (for severity of **High**, **Medium**, or **Low**) or value `14` (for any other severity).
- `Time` is the local time when the Sensor detects an event, in the form: `Mmm DD HH:MM:SS`. For example, `Jun 15 15:00:00` or `Jun  9 07:00:00`. Note this is a fixed-width format, so if the day of the month is less than `10`, a space is prepended to force it to take up two characters. If the time of day is before `10:00`, a zero is prepended to the hour to force the hour to take up two characters. The current year is not included in the timestamp.
- `Hostname` is either the hostname or the IP address of the machine that the Sensor is running on.
- `Prefix` is a CEF-specific format that has the following structure: `CEF:CVER|VENDOR|PRODUCT|PVER|SIGNATURE_ID|NAME|SEVERITY|`

In the DbProtect implementation:

- `CVER` is the CEF version, hard-coded to `0`.
- `VENDOR` is hard-coded to `ASI`.
- `PRODUCT` is hard-coded to `AR`.
- `PVER`, the application version, is determined internally by the Sensor.
- `SIGNATURE_ID` is the rule ID, a non-negative integer of up to five digits, with no leading zeros.
- `NAME` is the AppSec Rule title, truncated a maximum of 128 bytes, if needed.
- `SEVERITY` is an integer determined by the AppSecInc risk level via the following mapping: **High** is mapped to `9`, **Medium** is mapped to `7`, **Low** is mapped to `5`, **Info** is mapped to `3`.
- `Extension` is a space-delimited list of key-value pairs. The CEF standard lists multiple predefined keys and also allows for user-defined keys. DbProtect uses some of both. Fields in the extension will appear in the exact order they are listed below. Each field in the extension has a maximum field length, which is expressed in bytes. The maximum field length is used to truncate the value section of each **key = value** field, if necessary. For example, if the value corresponding to the key **msg** is configured with a maximum field length of 10 and the actual value is `select * from sysobjects`, the entire field is printed in the Syslog message as `msg=select * f`.

The keys DbProtect uses in the extension are:

-`duser`. Database login used. Max length = 256.

-`suser`. Client's username. Max length = 256.

-`sntdom`. Client’s domain. Max length = 256.

-`src`. IP address or hostname being used by the client to connect to the database. Max length = 256.

-`dproc`. Either **MSS** (Microsoft SQL Server), **SYB** (Sybase), **DB2** (DB2), or **ORA** (Oracle).

-`cn1`. The number of rows affected by the request.

-`cs1`. CVE reference number. Max length = 256.

-`sourceServiceName`. Name of the client application being used to communicate with the database. Max length = 256.

-`cs2`. Name of the database instance being traced. Max length = 256.

-`cs3`. Name of the database, schema, or SID, depending on the target database type. Max length = 256.

-`msg`. Text of the SQL statement being executed. Max length = 256.

Sample Syslog Message

Below is an example of an Sensor Syslog message[1]:

```
<9>Jun 18 15:01:17 192.168.29.1 CEF:0|ASI|AR|3.3|647|SYS.DBMS_DLL
Buffer overflow|9|duser=user1 suser=awindsor sntdom=MSHOME
src=192.168.28.1 dproc=ORA cn1=0 cs1=CVE-2006-3701
sourceServiceName=myapp cs2=mydb cs3=mydb
msg=ALTER_TABLE_REFERENCEABLE tbl_long_name
```

If, after the truncation of individual fields in the prefix and extension, the entire Syslog message is longer than 1024 bytes, the Syslog message as a whole is truncated to 1024 bytes before being sent.

For example, if the **msg** field of the extension is 2048 bytes long but all other prefix and extension fields are 8 bytes long, the **msg** field is truncated to 256 bytes as explained above, and since the message now contains no more than 1024 bytes, no additional truncation is needed. However, if **cs2**, **cs3**, **sourceServiceName** and **msg** are all greater than 256 bytes, they are all truncated to 256 bytes individually, but now the entire message is longer than 1024 bytes and the actual Syslog message sent contains **only** the first 1024 bytes of the message.

[1] All examples above are meant to be examples of the syntax of Syslog alerts, not technically accurate Syslog messages. The examples may not match actual Alerts generated by the sensor for the same event.

If any of the keys in the extension are missing values at the time of message construction, the entire `key = value` expression for the key is omitted from the message. For example, the event that generated the Syslog message below had no CVE reference number, so no **cs1** field is present:

```
<9>Jun 18 16:00:33 192.168.29.1 CEF:0|ASI|AR|3.3|86|Generic use of
xp_cmdshell|5|duser=sa suser=awindsor sntdom=MSHOME
src=192.168.28.1 dproc=MSS cn1=7 sourceServiceName=SQL Query
Analyzer cs2=mydb cs3=dbo msg=exec xp_cmdshell "dir"
```

SELF-AUDIT ALERTS

The same Syslog message format described above is also used for Sensor self-audit Alerts, except with an empty extension. For example:

```
<9>Jun 18 16:08:05 192.168.29.1 CEF:0|ASI|AR|3.3|1003|Sensor
started|9|
```

These are only applicable to self-audit Alerts sent from the Sensor. These include: **Sensor stopped**, **Sensor started**, **Sensor registered**, **Sensor unregistered**, **ASAP on Sensor initiated**, and **Sensor configured**. Other self-audit Alerts sent from the DbProtect Console to itself are **not** sent via Syslog since they are not sent from the Sensor.

Appendix D: Modifying the Sensor "Listener" Port Number

Host-based and network-based Sensors listen on port `20000` for HTTPS traffic from DbProtect (e.g., reconfiguration or status requests) **unless** you configure them differently during installation, or you change the port number in the `sensor.xml` and `sensor_original.xml` files.

Note: While, technically speaking, you can follow the steps in this appendix to modify the listen port number for any Sensor on any operating system, these steps are only recommended for modifying the listen port number for host-based Sensors for Oracle (on Solaris, AIX, HP-UX, and Linux 3 or later) and host-based Sensors for DB2 (on Linux 3 or later). For all other host- and network-based Sensors running on Windows, AppSecInc recommends you specify the listen port number during Sensor installation; for more information, see the *DbProtect Installation Guide*.

One reason you may want to modify the port number in the `sensor.xml` and `sensor_original.xml` files is because you want to monitor multiple instances on an IBM DB2 server. To do so, you must install one host-based Sensor for DB2 for each instance you want to monitor. You must then modify the XML files for each host-based Sensor for DB2 installation and assign a unique port number to **each** host-based Sensor for DB2.

To modify a Sensor listen port number:

1. Make sure the Sensor is unregistered; for more information, see the *DbProtect User's Guide*.

Note: You may also need to **re-configure** and **re-deploy** your Sensor. If it's already configured, you should note the current configuration setup in order to re-configure your re-registered Sensor to match the original configuration. For more information, see the *DbProtect User's Guide*.

2. Open the `sensor.xml` and `sensor_original.xml` files located in `<installation dir>/ASIappradar/sensor/conf`.
3. Locate the following line:

`<appSensorRoot sensorType="host-based" alertProtocol="3" port="20000" ip="127.0.0.1" id="55555" displayName="AppRadar Sensor">` and change `port="20000"` to a new value.

`20000` is the default value; your port number may be different.

4. Re-start the Sensor.

Appendix E: DbProtect Log Files

This appendix explains:

- *DbProtect Log Files*
- *Sensor Log Files*
- *Scan Engine Log Files.*

DbProtect Log Files

DbProtect log files come in two categories:

- *Normal Operations Console Log Files*
- *DbProtect Installation and Upgrade Log Files.*

NORMAL OPERATIONS CONSOLE LOG FILES

Log file:	Description:	Location:
`DbProtect.log`	This is the main application log that is written to during system usage. Log entries are in the following format: `Sat 01 Jan 23:59:59 [ThreadIdentifer] LEVEL Component - Log Message` where the date and time are presented first, followed by the DbProtect thread identifier, the level of the log message (which will be either **INFO**, **WARN** or **ERROR**), the DbProtect Audit and Threat Management component and then the log message. Each log message entry can span multiple lines.	`\Program Files\AppSecInc\DbProtect\GUI\logs\`
`gui_wrapper.log`	Log for the component that manages the service life cycle of the DbProtect service.	

Log file:	Description:	Location:
localhost_appsecinc_log.*.txt and tomcat.log	Application logs for the Tomcat engine used by DbProtect.	\Program Files\AppSecInc\DbProtect\GUI\tomcat\logs\ and \Program Files\AppSecInc\DbProtect\Message Collector\tomcat\logs\
messagecollector_wrapper.log	Log for the component that manages the service life cycle of the Message Collector service.	\Program Files\AppSecInc\DbProtect\Message Collector\logs\
messagecollector.log	This is a log file for DbProtect. It tracks the error entries for the Alert-collecting component of DbProtect.	

DBPROTECT INSTALLATION AND UPGRADE LOG FILES

The following DbProtect installation and log files are related to installation and upgrade. The files are stored in the following directory: `<%UserProfile%>\Local Settings\Temp\` (e.g., `C:\Documents and Settings\<user>\Local Settings\Temp`).

Note: If you don't see this folder, it's because it's a hidden folder.

Once installation has completed successfully, you can ignore these files (or you can safely remove them).

The DbProtect installation and log files are:

- `Bootstrapper_3.11.1.log`
- `BackendInstaller_install_silent.log`
- `DBC_install.log`
- `LegacyUninstaller_install.log`
- `LegacyUninstaller_uninstall.log`
- `DbProtect_install.log`
- `MessageCollector_install.log`
- `DBC-uninstall-1.0.log`
- `DBC-uninstall-1.1.log`
- `DBC-uninstall-fix-1.1.log`
- `DBC-uninstall-fix-1.2.log`

Sensor Log Files

Sensor log files are stored in the following directory: `<%UserProfile%>\Local Settings\Temp\` (e.g., `C:\Documents and Settings\<user>\Local Settings\Temp`).

Note: If you don't see this folder, it's because it's a hidden folder.

The following table lists and explains the Sensor log files.

NORMAL OPERATIONS SENSOR LOG FILES

Log file:	Description:	Location:
`appsensor.log`	Sensor application log (created during normal operations). This file generally contains warnings and errors, and at the default **Warning** level the file size grows slowly. However, you can configure this file to include also debug messages for troubleshooting, if the AppSecInc Support Team asks you to set the level to **Debug** or **Development**. In this case, the file size grows rapidly. **Note:** This file "rolls over" at 100MB and does so a maximum of three times.	`<sensor installation folder>\Program Files\AppSecInc\Sensor\logs\`
`sga-segments.log`	A log file created by host-based Sensors for Oracle installed on *nix platforms (monitoring one or more Oracle instances). This log file describes shared memory segments in use by Oracle. The host-based Sensor requires this information so it may attach to those same shared memory segments in order to read database traffic. It extracts shared memory information by using an Oracle function which writes SGA information to a trace file. This occurs only when you start or re-configure the Sensor.	`<installatoon directory>/ASIappradar/sensor/logs`

REPLAY LOG FILES

Also in the logs directory are Sensor log files related to "store-&-forward", i.e., AppSecInc's method of storing Alerts temporarily in case DbProtect becomes unavailable. These are more commonly known as the **replay log files**. They come in two forms:

- `*.replay.log`, which contains Alerts to be forwarded to DbProtect when it becomes available
- `*.replay.log.bookmark`, which is a bookmark pointing to the replay log indicating where forwarding left off the last time it ran.

If DbProtect becomes unavailable, these files ensure your Alerts will continue to be logged. They store Alerts in binary form which are "replayed" to DbProtect when it is back online.

The growth rate of the Alert log files depends on Alert rate and size. An average replay log grows at rate of approximately 2k/second -- but only when the Sensor cannot communicate with DbProtect .

The number of and size of Alert log files depends on how many Alerts per second are being fired and how long the **Message Collector** component of DbProtect has been down. Once it's back online, the replay logs will **not** shrink in size, but rather they will disappear one file at a time.

Replay logs "roll over" at 500MB and continue to do so every 500MB until DbProtect becomes available.

SENSOR INSTALLATION AND UPGRADE LOG FILE

The Sensor `configuration.log` file is related to installation and upgrade. Once installation is completed, you can ignore these files (or you can remove them safely).

Scan Engine Log Files

Scan Engine log files are classified in two categories:

- *Scan Engine Installation and Update Log Files*
- *Scan Engine Application Log Files.*

SCAN ENGINE INSTALLATION AND UPDATE LOG FILES

The Scan Engine **installation and update log files** -- for versions 5.5 and above only -- are located in the `<%Temp%>` directory, e.g., `C:\Documents and Settings\<user>\Local Settings\Temp`

Hint: You can run the command `echo %TEMP%` to determine the name and location of your `Temp` directory.

The names of the installation and update log files are:

- `ScanEngineInstall.log`
- `ScanEngine_{GUID}.log` (e.g., `ScanEngine_{D164A132-DE80-4EE7-8EB1-BAF1DC605B6A}.log`).

SCAN ENGINE APPLICATION LOG FILES

Scan Engines of all supported versions include **application log files**. The locations of the application log files differ, depending on your Scan Engine version.

Note: For more information on supported Scan Engine versions, see *DbProtect Version Compatibility Matrix, and Determining the Current Version of Installed DbProtect Applications.*

The Scan Engine application log files are in located in the following supported version-specific locations:

- For Scan Engine **version 5.5 and above**, the Scan Engine application log files are located in the following folder: `<%UserProfile%>\<%Local Application Data%>\AppSecInc\AppDetective\logs\`

Hint: You can run the command `echo %USERPROFILE%` to determine the name and location of your `USERPROFILE` directory. The `<%Local Application Data%>` varies on different Windows versions. For example, on **Windows XP/2000/2003**: `C:\Documents and Settings\<UserName>\Local Settings\Application Data\AppSecInc\AppDetective\logs\`. On **Windows Vista/2008**: `C:\Users\<UserName>\AppData\Local\AppSecInc\AppDetective\logs\`

Note: If the Scan Engine runs as a `LocalSystem` account, `<UserName>` is `Default User` on **Windows XP/2000/2003** and `Default` on **Windows Visa/2008**.

- For supported Scan Engines **before version 5.5**, the Scan Engine application log files are located in one of the following locations (depending on your Scan Engine version): `C:\Program Files\AppSecInc\ScanEngine\logs` or `C:\Program Files\AppSecInc\adse\logs`
- The name of the Scan Engine application log file is: `adscanengine.exe.<PID>.log` (e.g., `adscanengine.exe.1508.log`).

Appendix F: CIDR Notation

In **CIDR notation**, an IP address is represented as `A.B.C.D /n`, where `/n` is called the IP prefix or network prefix. The IP prefix identifies the number of significant bits used to identify a network. For example, `192.9.205.22 /18` means, the first 18 bits are used to represent the network and the remaining 14 bits are used to identify hosts. Common prefixes are `8`, `16`, `24`, and 32.

The following table contains CIDR to Netmask Translation information

CIDR	Netmask (Dot Notation)	Number of Hosts
/1	128.0.0.0	
/2	192.0.0.0	
/3	224.0.0.0	
/4	240.0.0.0	
/5	248.0.0.0	
/6	252.0.0.0	
/7	254.0.0.0	
/8	255.0.0.0	
/9	255.128.0.0	
/10	255.192.0.0	
/11	255.224.0.0	
/12	255.240.0.0	
/13	255.248.0.0	
/14	255.252.0.0	
/15	255.254.0.0	
/16	255.255.0.0	
/17	255.255.128	
/18	255.255.192.0	
/19	255.255.224.0	
/20	255.255.240.0	

/21	255.255.248.0	
/22	255.255.252.0	
/23	255.255.254.0	
/24	255.255.255.0	256
/25	255.255.255.128	128
/26	255.255.255.192	64
/27	255.255.255.224	32
/28	255.255.255.240	16
/29	255.255.255.248	8
/30	255.255.255.252	4
/31	255.255.255.254	2
/32	255.255.255.255	1

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 Vulnerability Management 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

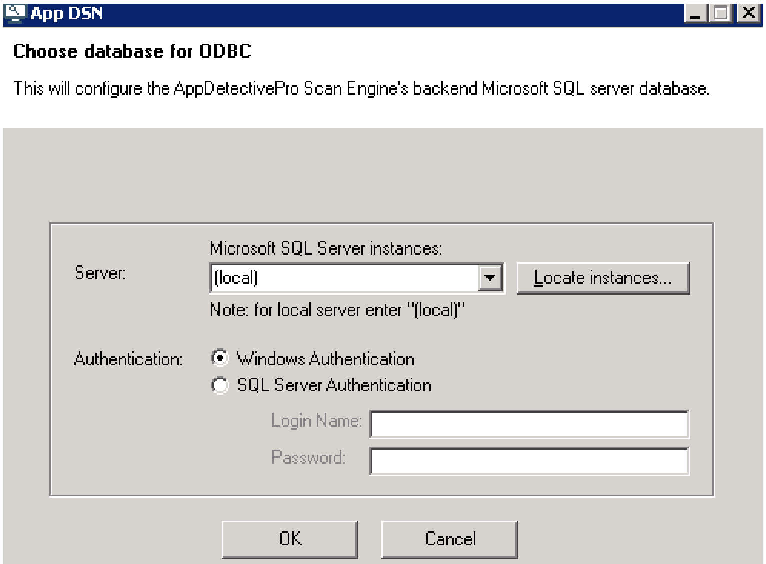
Again, you must use the AppDSN to repair the ODBC DSN entry on:

- the DbProtect Console host
- each installed Scan Engine host.

To use the AppDSN utility to 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**.

The **AppDSN** utility displays.



App DSN

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

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.

Important: This **must** be the same database DbProtect Vulnerability Management uses.

Hint: Click the **Locate instances...** button to search for/display all Microsoft SQL Server instances on your network.

2. Select to authenticate to the database server using: **Windows Authentication** (*strongly recommended*) or **SQL Server Authentication**.

If you select:

- **Windows Authentication**, then the `AppDetective 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:**

3. 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 Vulnerability Management 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* in the *DbProtect User's Guide*.
- 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* in the *DbProtect User's Guide*.

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.

Appendix H: 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.
5. Close your web browser and attempt to log into the DbProtect Console again.

Appendix I: Installing Certificates

Starting with DbProtect 2008.1 R2, Application Security, Inc. removed the **Certificates** tab from the **Configuration Manager Tool**. Formerly, this option allowed you to install your company's own certificate to eliminate browser messages that indicated issues with the "website's security certificate". Security concerns necessitated the removal of this option. However, as this appendix explains, you can install a custom certificate using command line tools provided with DbProtect.

This appendix consists of the following topics:

- *Overview*
- *Definitions*
- *Pre-installation*
- *Installation*
- *Converting to PEM format*
- *Post-installation.*

Overview

Importing a private key into DbProtect can be somewhat tricky. Your primary goal is to make sure you import the private key and certificate chain into the DbProtect keystore. **Problem:** there are numerous ways to deliver a certificate to the client.

Definitions

Some key **definitions** follow:

- `<CommonFiles>`. Location of the `AppSecInc\Common Files` folder, e.g., `C:\Program Files\AppSecInc\Common Files`
- `<DbProtect Home>`. Location of the instaleld DbProtect folder, e.g., `C:\Program Files\AppSecInc\DbProtect`
- `<Java Home>`. Location of an installed Java JRE. Application Security, Inc. recommends you use the one located at `<DbProtect Installation Directory>\JRE` or `[CommonFiles]\JRE` if you are running DbProtect 2009.1 or higher.
- `<OpenSSL Home>`. Location of the OpenSSL install folder.

Pre-installation

1. Backup the original keystore located in: `<DbProtect Installation Directory>\GUI\keys\key.store`
2. Locate the keystore password in the file `<DbProtect Installation Directory>\GUI\tomcat\conf\server.xml`. This appendix will refer to this file as: `[storepass]`.

Important: Your tool may prompt you to come up with aliases for the certificates you import. These aliases can be anything except for `"mykey"`. That is reserved for internal use.

The **keytool** and **Java** tools are both located in [Java Home]\bin. You can either enter full path to these tools (e.g., `C:\Program Files\AppSecInc\DbProtect\JRE\bin\keytool`), or you can add `<Java Home>\bin` to your path.

The **openssl** tool is located in `<OpenSSL Home>\bin`. You can either type the full path to these tools (e.g., `C:\OpenSSL\bin\openssl`), or you can add `<OpenSSL Home>\bin` to your path.

Installation

Assumption: You do not already have a certificate installed.

1. Open a command line, and `cd` to: `<DbProtect Installation Directory>\GUI\keys`
2. Enter: `keytool -genkey -alias user-cert -keystore key.store -storepass [storepass]`. The `user-cert` value can be an alias of your choice.
3. You are prompted to answer several questions. When prompted to enter:
   - your first and last name, enter the DbProtect hostname
   - a password, press <ENTER>.
4. Enter: `keytool -certreq -alias user-cert -file user-cert.csr -keystore key.store -storepass [storepass]`
5. Send the generated certificate request (`user-cert.csr`) to the either an internal certificate authority or a public certificate authority for signing. The certificate authority should respond with a signed certificate (`user-cert.pem`) and their own public certificate (`cacert.pem`). If your certificate authority does **not** send you a certificate in PEM format, see *Converting to PEM format.*
6. Save the signed certificate and root CA certificates to:`<DbProtect Installation Directory>\GUI\keys`
7. Enter: `keytool -import -alias root-ca -noprompt -file cacert.pem -keystore key.store -storepass [storepass]`

8. Enter: `keytool -import -alias user-cert -file user-cert.pem -keystore key.store -storepass [storepass]`

9. Enter: `keytool -delete -alias appsecinc-appradar -keystore key.store -storepass [storepass]`

   This removes the old certificate generated during Console installation; for more information, see the *DbProtect Installation Guide*.

Converting to PEM format

If your certificate you recieve from yout CA is **not** in PEM format, you can use **openssl** to convert it. Enter: `openssl x509 -in [certificate] -out [certificate].pem -outform PEM`

Post-installation

After installation you need to check that all of the certificates that you imported are in the keystore. Do the following:

1. Enter: `keytool -list keystore key.store -storepass [storepass]`
2. Make sure you see an entry for each certificate that you entered. You will see the alias you chose for the certificate, as well as the certificate thumbprint.
3. Ensure that there is an entry for DbProtect's `mykey` certificate.
4. Re-start the Console for the changes to take effect. Once the Console has started, you should be able to browse to the the DbProtect URL without seeing error messages about mismatched hostname or untrusted certificates. You should be able to log in and see all Sensors as "up and running" (green), and all Scan Engines as online.

Appendix J: 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, do the following:

1. Install a host-based Sensor for Oracle on **each node** in your Oracle RAC. For more information, go to the appropriate operating system-dependent topic in the *DbProtect Installation Guide*:
   - *Host-based Sensor for Oracle (on Solaris) - installation steps*
   - *Host-based Sensor for Oracle (on AIX) - installation steps*
   - *Host-based Sensor for Oracle (on HP-UX) - installation steps*
   - *Host-based Sensor for Oracle (on Red Hat Enterprise Linux) - installation steps*
   - *Host-based Sensor for Oracle (on Windows) - installation steps*
2. In the DbProtect Console, register each host-based Sensor for Oracle you installed in Step 1. 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)* in the *DbProtect User's Guide* for more information
   - 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)* in the *DbProtect User's Guide* for more information.

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)* in the *DbProtect User's Guide* for more information
- 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)* in the *DbProtect User's Guide* for more information.

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)* in the *DbProtect User's Guide* for more information

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)* in the *DbProtect User's Guide* for more information.

Appendix K: DbProtect System Event Logging

DbProtect reports user login and logout events to the Windows Event Log. This appendix consists of the following topics:

- *What is the Windows Event Log?*
- *DbProtect logged events*
- *Viewing DbProtect events*
- *Disabling DbProtect logging events*
- *Enabling DbProtect logging events.*

What is the Windows Event Log?

The Microsoft Windows operating system has a centralized log service that allows applications running under it to report events. The Windows Event Log has three log sources:

- system
- application
- security.

The Windows Event Viewer allows you to view events reported to the Windows Event Log. For more information about the the Windows Event Log and the Windows Event Viewer, go to `http://support.microsoft.com/kb/308427`

DbProtect logged events

DbProtect logs system events to the Windows Event Log. The events logged are:

- User Successful Login
- User Failed Login
- User Logout.

When an event occurs, DbProtect creates a Windows Event. The Windows one of these events occursEvent Viewer allows you to view these events.

Viewing DbProtect events

You can locate DbProtect events in the Windows Event Viewer under the "Application" log source. DbProtect specifies the Event Source as "DbProtect".

Disabling DbProtect logging events

By default, the writing of events to the Windows Event Log is enabled. It is possible to **disable** the writing of events to the Windows Event Log.

In order to disable the writing of events, follow the steps below:

1. Locate the `log4j.properties` file as described in *Appendix H: Manually Changing the Logging Level for the Console by Modifying the log4j.properties File* in the *DbProtect User's Guide*.
2. Open the file for editing.
3. Locate the following section in the file:

```
#---------------------------------------------------------------------
#
# This section handles appender settings for A (System Audit)
#
#---------------------------------------------------------------------
# Uncomment below to set Audit to be a RollingFileAppender
#log4j.appender.A=org.apache.log4j.RollingFileAppender
#log4j.appender.A.File=../../../GUI/logs/SystemAudit.log
#log4j.appender.A.layout=org.apache.log4j.PatternLayout
#log4j.appender.A.layout.ConversionPattern=%d{EEE dd MMM HH:mm:ss} -
%m%n
# Uncomment below to set Audit to write to the Windows event Log
log4j.appender.A=org.apache.log4j.nt.NTEventLogAppender
log4j.appender.A.source=DbProtect
log4j.appender.A.layout=org.apache.log4j.PatternLayout
log4j.appender.A.layout.ConversionPattern=%d{EEE dd MMM HH:mm:ss} -
%m%n
```

4. Comment the lower section (with the heading: `"Uncomment below to set Audit to write to the Windows event Log"`) by placing a `#` character at the start of the line. Do this for **all** lines in the section.
5. Uncomment the upper section (with the heading: `"Uncomment below to set Audit to be a RollingFileAppender"`) by removing the `#` character from the start of the line. Do this for **all** lines in the section.
6. Save the `log4j.properties` file.
7. Re-start the Console for the changes to take effect.

Enabling DbProtect logging events

By default, the writing of events to the Windows Event Log is enabled. If you disabled it at your site and now want to **enable** it, follow the steps below:

1. Locate the `log4j.properties` file as described in *Appendix H: Manually Changing the Logging Level for the Console by Modifying the log4j.properties File* in the *DbProtect User's Guide*.
2. Open the file for editing.
3. Locate the following section in the file:

```
#---------------------------------------------------------------------
#
# This section handles appender settings for A (System Audit)
#
#---------------------------------------------------------------------
# Uncomment below to set Audit to be a RollingFileAppender
log4j.appender.A=org.apache.log4j.RollingFileAppender
log4j.appender.A.File=../../../GUI/logs/SystemAudit.log
log4j.appender.A.layout=org.apache.log4j.PatternLayout
log4j.appender.A.layout.ConversionPattern=%d{EEE dd MMM HH:mm:ss} -
%m%n
# Uncomment below to set Audit to write to the Windows event Log
#log4j.appender.A=org.apache.log4j.nt.NTEventLogAppender
#log4j.appender.A.source=DbProtect
#log4j.appender.A.layout=org.apache.log4j.PatternLayout
#log4j.appender.A.layout.ConversionPattern=%d{EEE dd MMM HH:mm:ss} -
%m%n
```

4. Uncomment the lower section (with the heading: `"Uncomment below to set Audit to write to the Windows event Log"`) by removing the `#` character from the start of the line. Do this for **all** lines in the section.
5. Comment the upper section (with the heading: `"Uncomment below to set Audit to be a RollingFileAppender"`) by placing a `#` character at the start of the line. Do this for **all** lines in the section.
6. Save the `log4j.properties` file.
7. Re-start the Console for the changes to take effect.

Appendix L: 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 J: 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)* in the *DbProtect Installation Guide*.

Sensor configuration steps (Oracle Fail Safe)

To monitor Oracle databases in an 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* in the *DbProtect User’s Guide*.
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)* in the *DbProtect User’s Guide*, where you 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)* in the *DbProtect User’s Guide*, 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)* in the *DbProtect User’s Guide*, 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 <sensor installation folder>\sensor\conf\overrides directory to the <sensor 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 Sensor Cluster** resource offline, then bring it online again in the Cluster Administrator on either custer node.

18. Once the host-based Sensor for Oracle (on Windows) restarts, a new file displays in your Sensor installation's <sensor installation folder>\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 M: Configuring Your Host-Based Sensor for Oracle or DB2 (Installed on a *nix Platform) to Start Automatically Upon System Reboot

In most cases when you configure an Oracle or DB2 database on a *nix server, the server is set up to automatically start the database and bring up Oracle or DB2 upon system restart/reboot. In such cases, you can also have your host-based Sensor for Oracle or DB2 automatically come up when the server (where the Sensors are installed) gets rebooted.

This appendix explains how to configure your host-based Sensor for Oracle on a *nix platform (i.e., Solaris, AIX, or Red Hat Enterprise Linux) or DB2 on a *nix platform (i.e., (i.e., Solaris, AIX, HP-UX, or Red Hat Enterprise Linux) to automatically start up whenever you restart your system. In order to accomplish this goal, you **must** customize the startup file (located in your `ASIappradar/sensor/utils` directory) to fit your *nix environment.

To configure your host-based Oracle or DB2 Sensors (installed on a *nix platform) to start automatically upon system reboot:

1. Rename the `appradar_startup.sh` (for example, `arstart`).
2. Make the following modifications to the new `arstart` file.

```
user=aroracle
SENSOR_DIR="/home/aroracle/sensor378/ASIappradar/sensor"
prog=appradar_sensor
```

Replace the account `aroracle` with whatever account name you use to run your host-based Sensor for Oracle or DB2 (installed on a *nix platform).

3. Copy the modified file (`arstart` in this example) from the `utils` subdirectory to the appropriate platform-specific subdirectory (listed in the following table).

*nix Platform	Symbolic Links Commands
AIX (Oracle and DB2)	`/etc/arstart`
HP-UX (DB2 only)	`/sbin/init.d/arstart`
Red Hat Enterprise Linux (Oracle and DB2)	`/etc/init.d/arstart`
Solaris (Oracle and DB2)	`/etc/init.d/arstart`

4. If you are running a host-based Sensor for:
   - **Oracle**, then change the group of the `arstart` file to the Oracle DBA group (typically `dba`), and set the permissions to `750`. To do so, run the following respective commands:

     ```
     -# chgrp dba arstart
     -# chmod 750 arstart
     ```

   - **DB2**, change the group to the DB2 admin group (usually `db2grp1`) by running the following command: `# chgrp db2grp1 arstart`

5. Create symbolic links to the `arstart` script in the appropriate run-level script directories (as per the following examples).

*nix Platform	Symbolic Links Commands

AIX (Oracle and DB2)	`# ln -s /etc/arstart /etc/rc.d/rc2.d/S99arstart`
	`# ln -s /etc/arstart /etc/rc.d/rc2.d/K01arstart`

HP-UX (DB2 only)	`# ln -s /sbin/init.d/arstart /sbin/rc3.d/S990arstart`
	`# ln -s /sbin/init.d/arstart /sbin/rc3.d/K001arstart`

*nix Platform	Symbolic Links Commands

AIX (Oracle and DB2)	`# ln -s /etc/arstart /etc/rc.d/rc2.d/S99arstart`
	`# ln -s /etc/arstart /etc/rc.d/rc2.d/K01arstart`

Red Hat Enterprise Linux (Oracle and DB2)	`# ln -s /etc/init.d/arstart /etc/rc.d/rc3.d/S99arstart`
	`# ln -s /etc/init.d/arstart /etc/rc.d/rc5.d/K01arstart`
	`# ln -s /etc/init.d/arstart /etc/rc.d/rc5.d/S99arstart`
	`# ln -s /etc/init.d/arstart /etc/rc3.d/K01arstart`

Solaris (Oracle and DB2)	`# ln -s /etc/init.d/arstart /etc/rc3.d/S99arstart`

Note: The specific link names (e.g., `S99arstart`) are dependent on the specific configuration of your database server. You **must** execute the `arstart` script right after the startup script for Oracle (typically `dbora`) or DB2 (typically `db2start`).

Appendix N: Remote-Deploying DbProtect Components on Windows in Your Enterprise

You can use a third-party tool -- such as **Microsoft Operations Manager (MOM) --** to install and/or remote-deploy the DbProtect components (i.e., the DbProtect Console, Scan Engines, and Sensors) without user intervention ("silently") on Windows. Specifically, such tools allow you to remote-deploy individual **installer packages (MSIs)** to specified target hosts.

Note: You can also deploy DbProtect components on Windows individually using a command line, without any user interaction with third-party tools.

This appendix consists of the following topics:

- *Understanding the DbProtect component setup files*
- *Common DbProtect component setup file command line parameters*
- *Installing DbProtect Console via the command line (with default options)*
- *Extracting individual MSIs from the component setup files*
- *DbProtect Console component MSIs: installation prerequisites and command line arguments*
- *Scan Engine MSI: installation prerequisites and command line arguments*
- *Sensor MSI: installation prerequisites and command line arguments*
- *Using msiexec to to install the MSIs.*

Understanding the DbProtect component setup files

Each DbProtect component uses of a setup bootstrapper which, in turn, contains one or individual MSIs. The names of the component bootstrappers are:

- **DbProtect Console**: `DbProtect_Console_Setup.exe`
- **Sensor**: `AppRadar Sensor_<ver>_<Windows version>.exe` (e.g., `AppRadar Sensor_3.10.5_Win32.exe`
- **Scan Engine**: `appdetective_scanengine_setup_<ver>_en-US.exe` (e.g., `appdetective_scanengine_setup_6.2.8051.0_en-US.exe`

Each component bootstrapper can detect which prerequisites **must** be installed on your system. (For example, if you are installing the DbProtect Console, and you already have the required Microsoft .NET 2.0 Framework installed, then the `DbProtect_Console_Setup.exe` bootstapper does **not** install the Microsoft .NET framework; for more information, see *Chapter 5 - Installing the DbProtect Components and Logging Into the Console*.

For more information on installation prerequisites and optional command line argument installation parameters for the:

- **DbProtect Console** component, see *DbProtect Console component MSIs: installation prerequisites and command line arguments*
- **Scan Engine** component, see *Scan Engine MSI: installation prerequisites and command line arguments*
- **Scan Engine** component, see *Sensor MSI: installation prerequisites and command line arguments*.

Common DbProtect component setup file command line parameters

All DbProtect component setup files support the same common **command line parameters** (explained in the table below).

Common bootstrapper command line parameter	Allows you to:
`/?`	Display a help screen.
`/help`	
`/qb`	Force basic user interface (UI) mode.
`/nq`	Force full UI mode.
`/Log`	Enable logging.
`/LogFile [path]`	Specify a log file.
`/ConfigFile [path]`	Specify a configuration file.
`/ExtractCab`	Extract embedded components.
`/DisplayCab`	Display a list of embedded components.

Common bootstrapper command line parameter	Allows you to:
`/ComponentArgs ["name":"value" ...]`	Pass optional parameters to a DbProtect component MSI. To see a list of optional parameters for the: • DbProtect Console MSIs, see *DbProtect Console component MSIs: installation prerequisites and command line arguments* • Scan Engine MSI, see *Scan Engine MSI: installation prerequisites and command line arguments* • Sensor MSI, see *Sensor MSI: installation prerequisites and command line arguments.*

Installing DbProtect Console via the command line (with default options)

To install DbProtect Console with no user interaction, using **all** default options, run the following command: `DbProtect_Console_Setup.exe /qb`

Extracting individual MSIs from the component setup files

You can extract the individual MSIs (and third-party prerequisites) from each component setup file and install each MSI individually. To extract individual MSIs from a DbProtect component setup file, open a command prompt and run the following commands:

1. To extract individual MSIs from the:
   - **DbProtect Console** component setup file, run the following command: `DbProtect_Console_Setup.exe /ExtractCab`, then see *DbProtect Console component MSIs: installation prerequisites and command line arguments*
   - **Sensor** component setup file, run the following command: `AppRadar Sensor_<ver>_<Windows version>.exe /ExtractCab` (e.g., `AppRadar Sensor_3.10.5_Win32.exe /ExtractCab`, then see *Sensor MSI: installation prerequisites and command line arguments.*
   - **Scan Engine** component setup file, run the following command: `appdetective_scanengine_setup_<ver>_en-US.exe /ExtractCab` (e.g., `appdetective_scanengine_setup_6.2.8051.0_en-US.exe /ExtractCab`, then see *Scan Engine MSI: installation prerequisites and command line arguments*

Running any of the MSI extraction commands above creates a folder called: `SupportFiles` in your current directory. This folder contains the individual DbProtect MSIs (and third-party prerequisites) necessary to complete your silent installation.

DbProtect Console component MSIs: installation prerequisites and command line arguments

The **DbProtect Console** component setup file contains the following MSIs:

- **Console MSI** and the **Message Collector MSI**; for more information, see *The Console MSI and the Message Collector MSIs and command line arguments*
- **Database Component MSI**; for more information, see *Database Component MSI and command line arguments*
- **SHATTER Knowledgebase MSI**; for more information, see *SHATTER Knowledgebase MSI and command line arguments*.

THE CONSOLE MSI AND THE MESSAGE COLLECTOR MSIS AND COMMAND LINE ARGUMENTS

The **Console MSI** and the **Message Collector** MSIs are called `DbProtectInstaller.msi` and `MessageCollector.msi`, respectively. These files are stored at the same root level as the `SupportFiles` directory (created after you extract the MSIs, explained in *Extracting individual MSIs from the component setup files*).

The **prerequisites** for installing the **Console MSI** and **Message Collector MSI** follow:

- Microsoft Visual Studio CRT 2005 SP1
- Microsoft .NET 2.0 Framework
- MDAC 2.6.

As explained in *Common DbProtect component setup file command line parameters*, the `/ComponentArgs ["name":"value" ...]` command allows you to pass optional parameters to a **Console MSI** and the **Message Collector** component MSIs. The following table lists the **optional command line arguments** for the **Console MSI** and **Message Collector MSI**:

Console and Message Collector MSI command line argument	Description of `<value>`
`INSTALLLOCATION=<value>`	Defines the target directory where the DbProtect Console and/or Message Collector components should be installed.
`RUNTIME_DATABASE_LOGON_TYPE =<value>`	Database authentication type at runtime, either `SqlAuth` or `WinAuth`.
`RUNTIME_DATABASE_USERNAME =<value>`	Username to access the database at runtime.
`RUNTIME_DATABASE_PASSWORD =<value>`	Password to access the database at runtime.
`SERVICE_LOGON_TYPE=<value>`	Service logon type (either `ServiceLocalSystem` or `ServiceAccount`).
`SERVICE_USERNAME=<value>`	Service username when not using local system.

Console and Message Collector MSI command line argument	Description of `<value>`
`SERVICE_PASSWORD=<value>`	Service user password when not using local system
`CONSOLE_HOST=<value>`	Host name for the `DbProtect Console` or `Message Collector` service to listen to. Default value is: `localhost`.
`PORTNUMBER=<value>`	Port for the `DbProtect Console` or `Message Collector` service to listen to. **Note:** All DbProtect port numbers have defaults. **DbProtect Console**: `20080`, **Message Collector**: `20081`, **Sensor**: `20000`, **Scan Engine**: `20001`. For more information, see *Port considerations*.

DATABASE COMPONENT MSI AND COMMAND LINE ARGUMENTS

The **Database Component MSI** is called: `DatabaseInstaller.msi`. This file is stored under `SupportFiles/SchemaComponent` (created after you extract the DbProtect Console component, explained in *Extracting individual MSIs from the component setup files*).

The **prerequisites** for installing the **Database Component MSI** follow:

- Microsoft Visual Studio CRT 2005 SP1
- Microsoft .NET 2.0 Framework
- MDAC 2.6.

As explained in *Common DbProtect component setup file command line parameters*, the `/ComponentArgs ["name":"value" ...]` command allows you to pass optional parameters to a DbProtect component MSI. The following table lists the The following table lists the **optional command line arguments** for the **Database Component MSI**:

Database Component MSI optional installation parameter	Description
`INSTALLLOCATION=<path>`	Defines the target directory where the Database Component should be installed.

SHATTER KNOWLEDGEBASE MSI AND COMMAND LINE ARGUMENTS

The **SHATTER Knowledgebase MSI** is called: `DataComponent.msi`. This file is stored under `SupportFiles/DataComponent` (created after you extract the MSIs, explained in *Extracting individual MSIs from the component setup files*).

The **prerequisites** for installing the **SHATTER Knowledgebase MSI** follow:

- Microsoft Visual Studio CRT 2005 SP1
- Microsoft .NET 2.0 Framework
- Database Component.

As explained in *Common DbProtect component setup file command line parameters*, the `/ComponentArgs ["name":"value" ...]` command allows you to pass optional parameters to a DbProtect component MSI. The following table lists the **optional command line arguments** for the **SHATTER Knowledgebase MSI**:

SHATTER Knowledgebase MSI command line argument	Description of `<value>`
`INSTALLLOCATION=<value>`	Defines the target directory where the SHATTER Knowledgebase should be installed.

Scan Engine MSI: installation prerequisites and command line arguments

The **Scan Engine MSI** is called: `ScanEngine.msi`. This file is stored under `SupportFiles` (created after you extract the MSIs, explained in *Extracting individual MSIs from the component setup files*).

The **prerequisites** for installing the **Scan Engine MSI** follow:

- Microsoft Visual Studio CRT 2005 SP1
- Microsoft .NET 2.0 Framework
- MDAC 2.6.

As explained in *Common DbProtect component setup file command line parameters*, the `/ComponentArgs ["name":"value" ...]` command allows you to pass optional parameters to a DbProtect component MSI. The following table lists the **optional command line arguments** for the **Scan Engine MSI**:

Scan Engine MSI command line argument	Description of `<value>`
`INSTALLLOCATION=<path>`	Defines the target directory where the Scan Engine should be installed.

Sensor MSI: installation prerequisites and command line arguments

The **Sensor MSI** is called: `service_installer.msi`. This file is stored under `SupportFiles` (created after you extract the MSIs, explained in *Extracting individual MSIs from the component setup files*).

The **prerequisites** for installing the Sensor MSI follow:

- Microsoft Visual Studio CRT 2005 SP1
- Microsoft .NET 2.0 Framework
- MDAC 2.6.

As explained in *Common DbProtect component setup file command line parameters*, the `/ComponentArgs ["name":"value" ...]` command allows you to pass optional command line parameters to a DbProtect component MSI.

The following table lists the **optional command line arguments** for the **Sensor MSI**:

Sensor MSI command line argument	Description of `<value>`
`INSTALLLOCATION=<value>`	The full target directory path where the Sensor should be installed.
`SENSOR_TYPE=<value>`	`Host-based` or `network-based`.
`SERVICE_LOGON_TYPE=<value>`	Service logon type. Either `ServiceLocalSystem` or `ServiceAccount`.
`SERVICE_USERNAME=<value>`	Service username (when not using local system).
`SERVICE_PASSWORD=<value>`	Service user password (when not using local system).
`PORTNUMBER=<value>`	Port for the `DbProtect Console` or `Message Collector` service to listen to. **Note:** All DbProtect port numbers have defaults. **DbProtect Console**: `20080`, **Message Collector**: `20081`, **Sensor**: `20000`, **Scan Engine**: `20001`. For more information, see *Port considerations*.

Using msiexec to to install the MSIs

`msiexec` allows you to install, modify, and perform operations on a Windows installer from the command line. Run the following command to silently pass installation parameters to the DbProtect MSIs via the DbProtect component setup files:

`msiexec /i service_installer.msi /l*v install.log /qb` (or `/qn`) `/name=value`

Where:

- `/qb` provides a basic UI
- `/qn` provides no UI

- `name=value` allows you to pass optional parameters to your component MSIs as command line arguments.

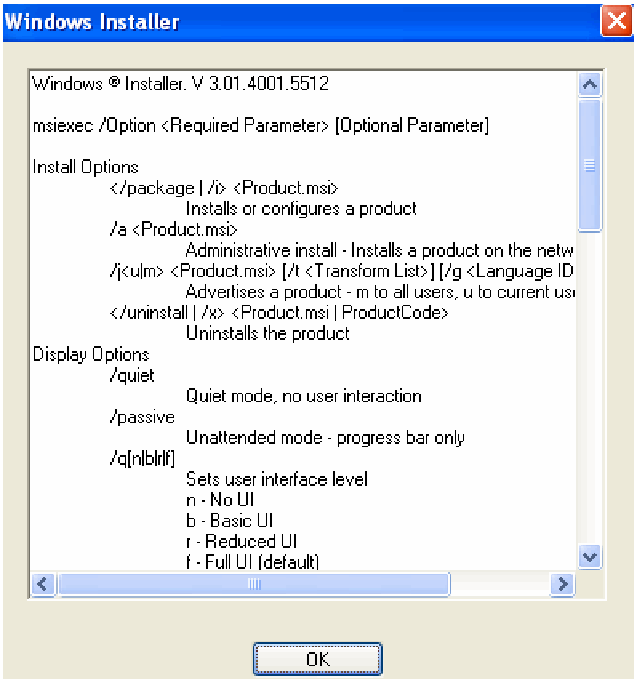
Acceptable installation command line arguments are specific for each installer component MSI. For a list of:

-**DbProtect Console** component MSI command line arguments, see *DbProtect Console component MSIs: installation prerequisites and command line arguments*

-**Scan Engine** component MSI command line arguments, see *Scan Engine MSI: installation prerequisites and command line arguments*

-**Sensor** component MSI command line arguments, see *Sensor MSI: installation prerequisites and command line arguments.*

Hint: You can run `msiexec /?` to display a Windows Installer dialog box that includes all `msiexec` options (install, display, restart, logging, update, repair, etc.).



```
Windows ® Installer. V 3.01.4001.5512

msiexec /Option <Required Parameter> [Optional Parameter]

Install Options
        </package | /i> <Product.msi>
                Installs or configures a product
        /a <Product.msi>
                Administrative install - Installs a product on the netw
        /j<u|m> <Product.msi> [/t <Transform List>] [/g <Language ID
                Advertises a product - m to all users, u to current us
        </uninstall | /x> <Product.msi | ProductCode>
                Uninstalls the product
Display Options
        /quiet
                Quiet mode, no user interaction
        /passive
                Unattended mode - progress bar only
        /q[n|b|r|f]
                Sets user interface level
                n - No UI
                b - Basic UI
                r - Reduced UI
                f - Full UI (default)
```

FIGURE: **Windows Installer** dialog box with msiexec options