



# **DbProtect 6.0**

## **Analytics User's Guide**

Last Modified January 25, 2010

Application Security, Inc.  
[www.AppSecInc.com](http://www.AppSecInc.com)  
[info@appsecinc.com](mailto:info@appsecinc.com)  
1-866-9APPSEC

# Contents

## **Introduction 2**

What is DbProtect Analytics? 3

DbProtect Analytics and Compliance Reporting 4

Customer Support 5

## **Using DbProtect Analytics 6**

Starting DbProtect Analytics 7

Navigating the DbProtect Analytics Portal 9

## **DbProtect Analytics Dashboards 11**

The Security Dashboard 12

The Compliance Dashboard 14

The Operations Dashboard 18

## **DbProtect Analytics Reports 22**

Navigating to the Reports 23

Running and Viewing Reports 24

Understanding the Reports 25

## **Appendices 35**

Appendix A: Resolving Problems Quickly 36

Appendix B: Key Issues 39

Appendix C: Troubleshooting Installation Errors 41

Appendix D: Troubleshooting Runtime Errors 48

# Introduction

DbProtect Analytics is an add-on component to the DbProtect Console and is an essential complement to the DbProtect suite of products. DbProtect Analytics includes new executive-level **Dashboards** for security, compliance, and operations, and a collection of **Reports** (including new compliance Reports for NIST 800-53, SOX, PCI DSS, HIPAA and DISA-STIG, and more).

DbProtect Analytics Dashboards provide better security and compliance transparency to executives and management. Dashboards are designed to support adhoc investigation with drill-through technology, combining assessment and monitoring data. Access to global views of data is secured by only making DbProtect Analytics available to users with credentials at the root level organization.

This guide explains how to install DbProtect Analytics, and provides an overview of each Dashboard and Report elements.

## **What you will find in this chapter:**

- *What is DbProtect Analytics?*
- *DbProtect Analytics and Compliance Reporting*
- *Customer Support.*

# What is DbProtect Analytics?

**DbProtect Analytics** provides a global view of your enterprise's database security posture. This content is designed for executives, security risk managers, IT administration, and any personnel involved in the enforcement of regulatory/corporate compliance policies and database patch administration.

DbProtect Analytics provides a convenient set of executive level Dashboards and key Reports that draw data from DbProtect's Vulnerability Management and Audit and Threat Management components.

# DbProtect Analytics and Compliance Reporting

The DbProtect Analytics **Compliance** Dashboard charts the compliance posture across your inventory of databases assessed and/or monitored by the DbProtect suite of products. In addition, DbProtect Analytics includes a set of Reports which displays vulnerability and threat data mapped using DbProtect's regulatory compliance mappings. Some key DbProtect Analytics compliance Reports include:

- Healthcare Services (HIPAA)
- Sarbanes-Oxley Act (SOX)
- Payment Card Industry (PCI) Data Security Standards
- Federal Information Security Management Act (FISMA)
- Defense Information Systems Agency - Database Security Technical Implementation Guide (DISA-STIG)
- National Institute of Standards and Technology (NIST).

# 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](mailto: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](mailto:support@appsecinc.com)

# Using DbProtect Analytics

What you will find in this chapter:

- *Starting DbProtect Analytics*
- *Navigating the DbProtect Analytics Portal.*

# Starting DbProtect Analytics


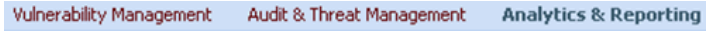
DbProtect Analytics is an add-on module to the DbProtect Console, which DbProtect Console users can **launch** through a simple sign-on process. In order to access DbProtect Analytics, you must first be **authenticated** as a member of the “root” organization in your DbProtect Console.

DbProtect Analytics consists of Dashboards and Reports that span your entire organization’s assets. Restricting access to only members of the “root” organization of your DbProtect Console is consistent with security best practices.

To launch and authenticate to DbProtect Analytics:

Step	Action
1	<p>Do one of the following:</p> <ul style="list-style-type: none"><li>Choose <b>Start &gt; All Programs &gt; AppSecInc &gt; DbProtect</b>.</li></ul> <p>OR</p> <ul style="list-style-type: none"><li>Open Internet Explorer 6.0 or greater with a minimum screen resolution of 1024x768.</li></ul> <p>THEN</p> <ul style="list-style-type: none"><li>Enter <a href="https://YourMachineName:InstallPort">https://YourMachineName:InstallPort</a> in the <b>Address</b> line, where: <a href="#">YourMachineName</a> is the computer name of your DbProtect Console machine and <a href="#">InstallPort</a> is the port number entered during installation (the default port is <a href="#">20080</a>).</li></ul> <p>A <b>Security Alert</b> 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. Accept to display the DbProtect Console login page.</p> <p><b>Note:</b> If you experience difficulty logging into DbProtect and connecting to DbProtect, you may need to troubleshoot the Java Runtime Environment (JRE) security settings on your Internet Explorer 6 or greater web browser. For more information on a workaround, see the <a href="#">DbProtect User’s Guide</a>.</p>



Step	Action
2	 <p>FIGURE: DbProtect Console login page</p> <p>Do the following:</p> <ul style="list-style-type: none"> <li>• In the <b>User Name:</b> field, enter your DbProtect user name.</li> <li>• In the <b>Password:</b> field, enter your DbProtect password.</li> <li>• Use the <b>Domain:</b> drop-down to select your domain, or manually enter a domain in the <b>Domain:</b> field.</li> </ul> <p><b>Caution!</b> If you cannot log in, it may be because you have not entered your full-qualified domain name in the <b>Domain:</b> field. If you need help determining your full-qualified domain name, see the <i>DbProtect User's Guide</i> or the <i>DbProtect Administrator's Guide</i>.</p> <p><b>Note:</b> 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.</p> <ul style="list-style-type: none"> <li>• Click the <b>Log In</b> button to authenticate to the DbProtect Console.</li> </ul>
3	 <p>FIGURE: DbProtect Console tabs</p> <p>Once you are logged into the DbProtect Console, an <b>Analytics and Reporting</b> tab displays once you are authenticated as a member of the "root" organization. This tab displays for all user types (i.e., View Users, Basic Users, Admins, and Super Admins) within the "root" organization.</p>
4	<p>Click the <b>Analytics and Reporting</b> tab to display the DbProtect Analytics portal. For information on navigating DbProtect Analytics, see <i>Navigating the DbProtect Analytics Portal</i>.</p>

# Navigating the DbProtect Analytics Portal

The DbProtect Analytics navigation header (shown below) displays on every DbProtect Analytics page, allowing you to navigate to the different parts of the DbProtect Analytics application.

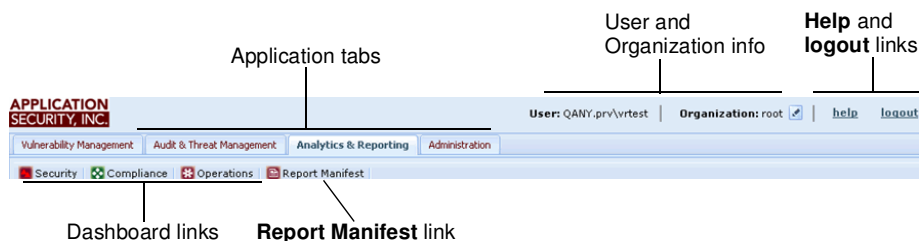


FIGURE: DbProtect Analytics navigation header

The DbProtect Analytics navigation header consists of the:

- **Dashboard links (Security, Compliance, and Operations)**; for more information, see *DbProtect Analytics Dashboards*
  - **Report Manifest link**, which allows you to access DbProtect Analytics Reports; for more information, see *DbProtect Analytics Reports*
  - **Application tabs**, which allow you to toggle between the different components of DbProtect. You can click the:
    - Vulnerability Management** tab to display and use DbProtect Vulnerability Management; for more information, see the *DbProtect User's Guide*.
    - Audit & Threat Management** tab to display and use DbProtect Audit & Threat Management; for more information, see the *DbProtect User's Guide*.
    - Analytics and Reporting** tab to use DbProtect Analytics and run DbProtect Analytics reports (explained in this guide)
    - The **Compliance Packs** tab to work with compliance packs, optional DbProtect add-ons that contain a regulatory compliance-level view of your database environment designed to help you track, manage, and meet compliance requirements; for more information, see the *DbProtect User's Guide*.
- Note:** The **Compliance Packs** application tab only displays on the Console once you successfully import a compliance regulation-specific content pack into DbProtect; for more information, see the *DbProtect User's Guide*.
- Administration tab** to import content packs and enable compliance pack functionality in DbProtect, and to view your DbProtect system information; for more information, see the *DbProtect User's Guide*.

- **User** and **Organization** information, which displays your **User/Organization information**, i.e., your logged-in **user ID** and your associated "effective" **Organization**.

Every User ID is associated with at least one Organization. If you are a Super User or an Admin User, and your User ID is associated with multiple Organizations, you can toggle between Organizations. For more information, on how Organizations and Users work in DbProtect, see the *DbProtect User's Guide*.

- **Help** and **Logout** links, which allow you to display the online help and log out of DbProtect, respectively.

# DbProtect Analytics Dashboards

DbProtect Analytics provides executive **Dashboards** which contain information targeted toward specific areas of interest in most organizations.

The Dashboards are categorized as follows: **Security**, **Compliance**, and **Operations**. Every three hours, DbProtect Analytics generates and caches the Dashboards. (This time interval is currently **not** user-configurable.) Each Dashboard is conveniently labelled with callouts to help you interpret the Report data. In addition, the Dashboards display supplemental data when you mouse over them.

If you want more immediate access to DbProtect Analytics results, you can click the **Reports Manifest** link to display the Reports section, which contains up-to-the-minute DbProtect Analytics report data; for more information, see *DbProtect Analytics Reports*.

In this chapter, you will learn more about the Dashboards and the elements they contain. Specifically, this chapter discusses:

- *The Security Dashboard*
- *The Compliance Dashboard*
- *The Operations Dashboard*.

# The Security Dashboard

The **Security Dashboard** consists of the following elements:

- *Vulnerabilities by Severity*
- *Threats by Severity*.

## Vulnerabilities by Severity

The **Vulnerabilities by Severity** Dashboard element computes the most recent result for any assessment test that was run against a Dashboard asset. If the test revealed a vulnerability, it is aggregated into this Dashboard according to its severity and category. For tests that return a list of objects in violation (such as accounts with weak passwords, or objects with inappropriate privilege grants), the test result only counts as one violation.

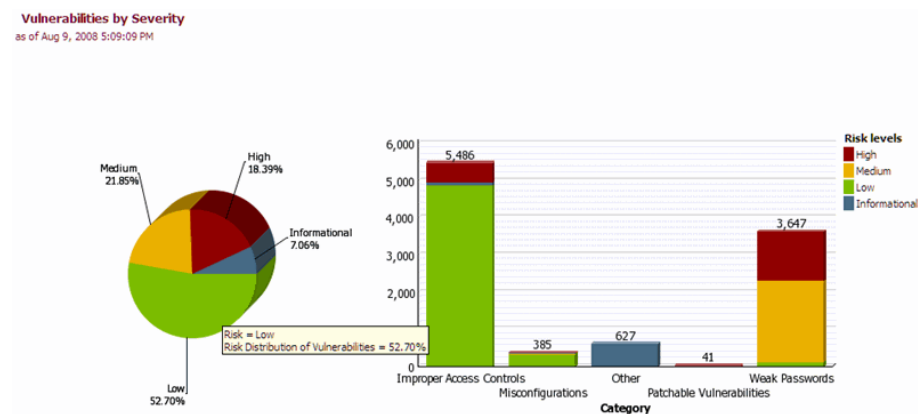


FIGURE: Vulnerabilities by Severity Dashboard element

## Threats by Severity

The **Threats by Severity** Dashboard element computes the distribution of monitored security events aggregated by severity and category. The Dashboard shows no informational events or internal system audit events since they are not considered security events.

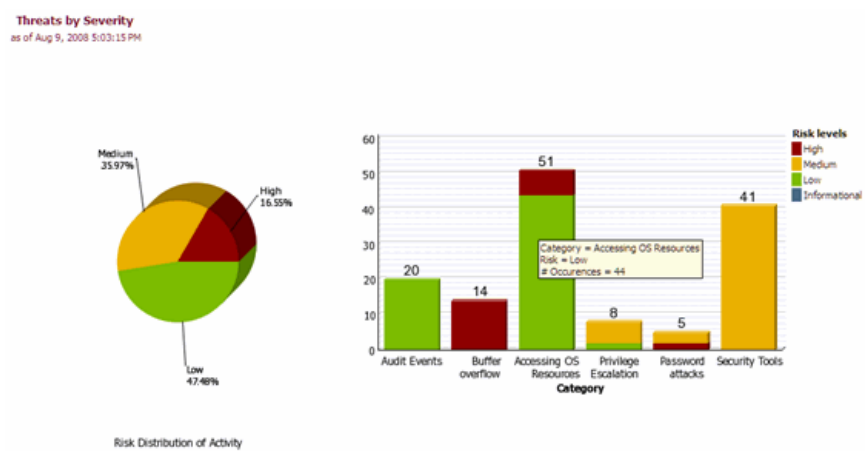


FIGURE: Threats by Severity Dashboard element

# The Compliance Dashboard

The **Compliance Dashboard** consists of the following elements:

- *Compliance Summary*
- *Compliance by Database*
- *Aging Scan Activity*
- *Compensating Controls*.

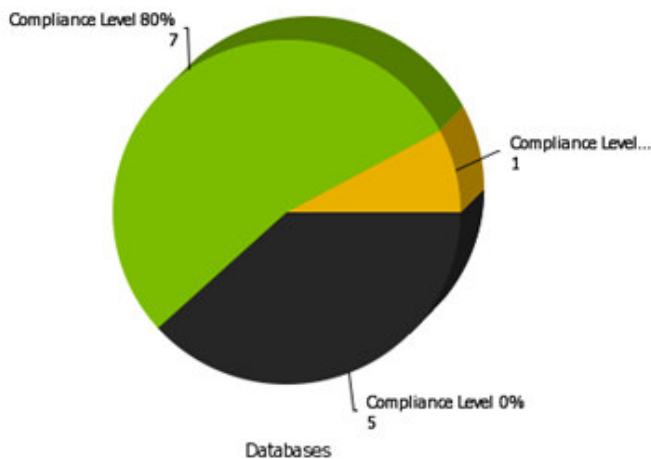
## Compliance Summary

The **Compliance Summary** Dashboard element provides a view of the managed databases that meet a set of criteria that are defined as compliance levels 1 through 5. The levels are:

- **(Best) Level 1.** No high/medium/low vulnerabilities found
- **Level 2.** At least one "low" level vulnerability found
- **Level 3.** At least one "medium" level vulnerability found
- **Level 4.** At least one "high" level vulnerability found
- **Level 5.** No tests were run in the past year.
- **(Worst) Level 6.** No tests were run (or results on record are more than one year old).

### Compliance Summary

For all Assets  
as of Oct 6, 2009 1:36:48 PM



Compliance Summary Dashboard element

## Compliance by Database

The **Compliance by Database** Dashboard element provides a view of the managed databases that meet a set of criteria that are defined as Compliance Levels 1 through 5. The levels are:

- **(Best) Level 1.** No high/medium/low vulnerabilities found
- **Level 2.** At least one "low" level vulnerability found
- **Level 3.** At least one "medium" level vulnerability found
- **Level 4.** At least one "high" level vulnerability found
- **Level 5.** No tests were run in the past year.
- **(Worst) Level 6.** No tests were run (or results on record are more than one year old).

In this Dashboard element, DbProtect Analytics charts each database type separately, displaying the proportion of compliant assets within each database type.

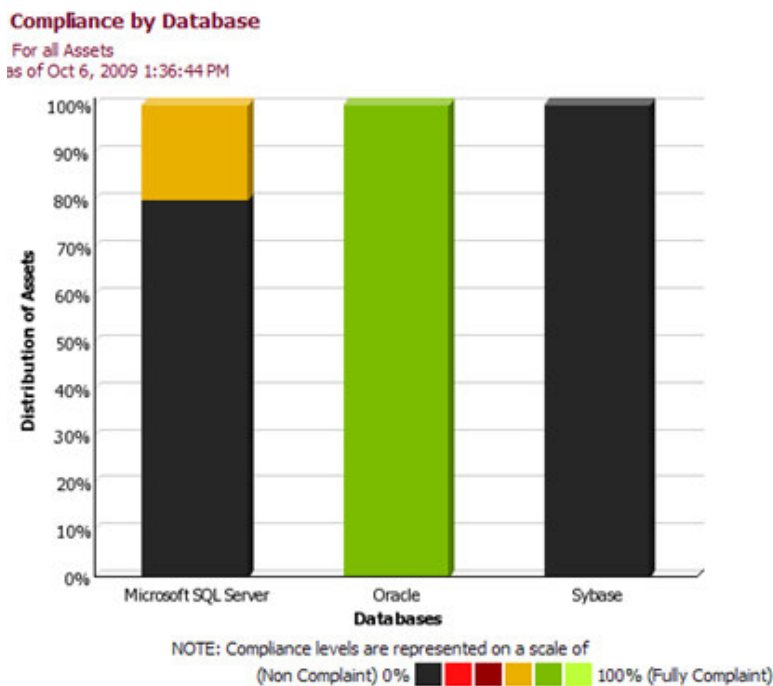


FIGURE: Compliance by Database Dashboard element



**Aging Scan Activity**

The **Aging Scan Activity** Dashboard element shows the number of assets distributed across the age of the most recent scan data recorded for those assets. The complete inventory of databases is categorized into buckets of scan ranges (such as 0-30 days, 30-60 days, etc.). The assets that fall into each range are then aggregated by type (such as Oracle, IBM DB2, etc.) and scan ranges. These are shown as a set of stacked points (one for each database type) plotted along a time axis (scan ranges). You should be able to discern your average scan age by looking for the median scan age in this plot with the highest number of assets.

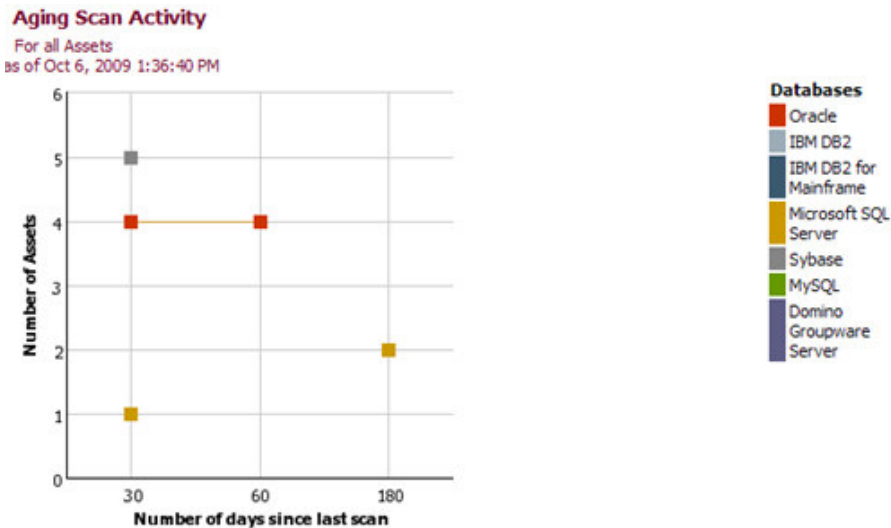


FIGURE: Aging Scan Activity Dashboard element

Compensating Controls

The **Compensating Controls** Dashboard element shows a distribution of database assets that have DbProtect Audit and Threat Management turned on. All other assets are classified with a monitoring status of **None/Unknown**.

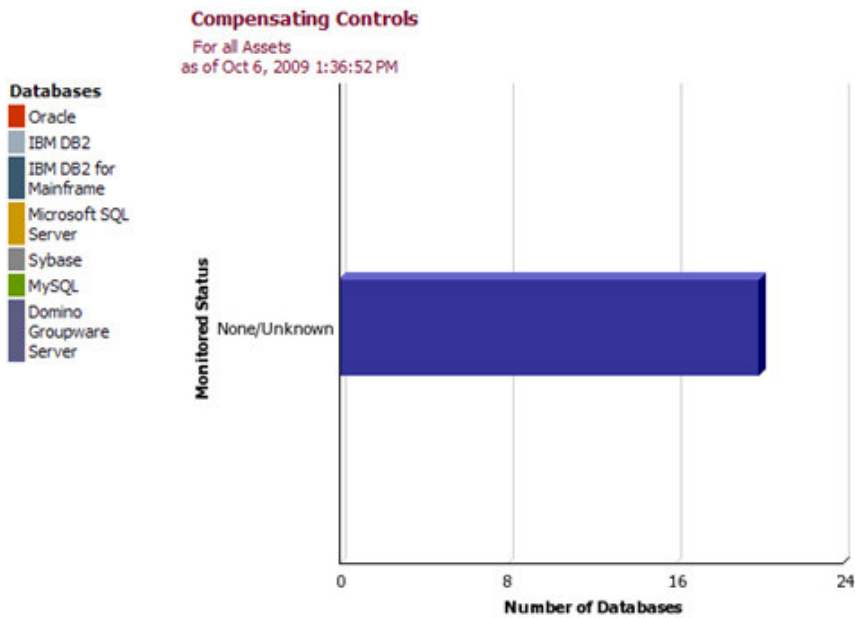


FIGURE: Compensating Controls Dashboard element

# The Operations Dashboard

The **Operations Dashboard** consists of the following elements:

- *Database Distribution*
- *Recent Scan Jobs*
- *Scan Policy Usage*
- *Inactivity Trends.*

## Database Distribution

The **Database Distribution** Dashboard element shows all discovered database instances aggregated by the type of asset (such as Oracle, IBM DB2, etc.). This inventory data does **not** include supplemental services such as Oracle listeners or Microsoft SQL Redirectors.

### Database Distribution

as of Aug 9, 2008 6:09:33 PM

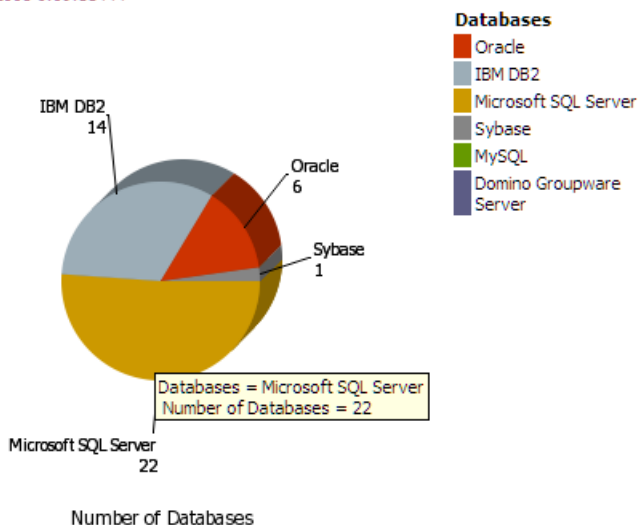


FIGURE: Database Distribution Dashboard element

Recent Scan Jobs

The **Recent Scan Jobs** Dashboard element shows a list of the most recent fifteen scan jobs. It serves as a quick snapshot of what jobs are being run, how often, status of the job, and the organization from which the job was executed.

Recent Scan Jobs

as of Aug 9, 2008 5:08:57 PM

Last Run	Organization	Job	Times Run	Status
5/27/08 4:46 PM EDT	root	oracle baseline	2	Completed
5/27/08 4:07 PM EDT	root	sunny2 audit	1	Completed
5/27/08 3:59 PM EDT	root	sunny2-pentest	1	Completed
12/27/07 12:22 PM EST	root	Local Audit	1	Completed
12/27/07 12:18 PM EST	root	Local Pen Test	1	Completed

FIGURE: Recent Scan Jobs Dashboard element

Scan Policy Usage

The **Scan Usage Policy** Dashboard element displays the aggregated usage counts for Vulnerability Management Policies. Since these Policies are categorized as Penetration Test and Audit Policies, the Dashboard aggregates the usage along the same categories. Within each category, the proportion of individual Policy usage is stacked to show the relative use. This serves as an easy reference point to determine whether Policies are being used for assessment which deviate from corporate mandates.

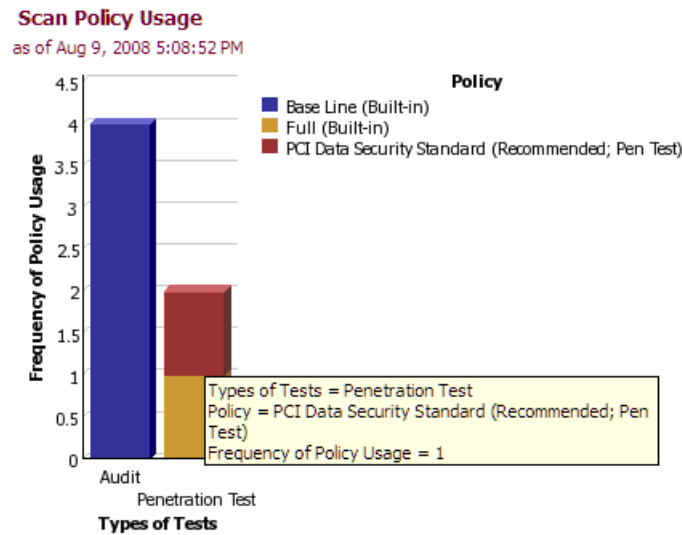


FIGURE: Scan Policy Usage Dashboard element

## Inactivity Trends

The **Inactivity Trends** Dashboard element provides an aggregation of inactivity alerts over the last twelve months system wide. It is a very high-level view of overall levels of detected inactivity. This allows easily identification of database assets that might be offline (or network unreachable), or have unusual usage patterns over time.

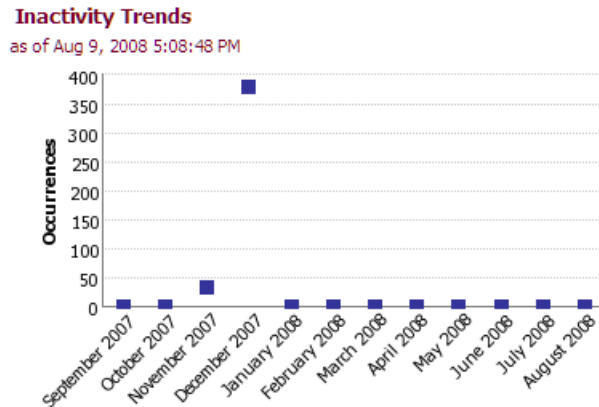


FIGURE: Inactivity Trends Dashboard element

# DbProtect Analytics Reports

This chapter consists of the following sections:

- *Navigating to the Reports*
- *Running and Viewing Reports*
- *Understanding the Reports.*

# Navigating to the Reports

You can click the **Report Manifest** link on any DbProtect Analytics portal page to access DbProtect Analytics Reports. The **Report Manifest** page is shown below.

DbProtect Analytics			
<a href="#">Security</a>	<a href="#">Compliance</a>	<a href="#">Operations</a>	<a href="#">Report Manifest</a>
Category	Subcategory	Report	
Risk Management	Assessment	<a href="#">Database Findings Detailed Review</a>	The detailed findings n information by databa server).
		<a href="#">Database Findings Detailed Review (with Knowledgebase Articles)</a>	This is a version of the knowledgebase article
		<a href="#">Database Findings Summary Review</a>	This report summarizes databases in the organ the depth issues within
		<a href="#">Database Findings Summary Review (with Knowledgebase Articles)</a>	This is a version of the knowledgebase article
		<a href="#">Database Inventory</a>	The inventory report l
		<a href="#">Database User Inventory</a>	This is an inventory re

FIGURE: **Report Manifest** page

Available DbProtect Analytics Reports are organized by category (e.g., **Risk Management**) and subcategory (e.g., **Assessment**), with a clickable link to generate each Report.



# Running and Viewing Reports

This sections explains what you need to know about *Running a Report* and *Viewing a Report*.

## Running a Report

To run a DbProtect Analytics Report, click the Report description (e.g., **Database Findings Detailed Review**) on the **Report Manifest** page. The Report runs, and displays in a separate window.

## Viewing a Report

Each DbProtect Analytics Report contains a drop-down icon in the upper right portion of the Report window. When you click the drop-down icon, the Report viewing options menu displays (shown below).



FIGURE: Report viewing options menu

You can click **View in HTML Format**, **View in PDF Format**, or **View in Excel Options** to view your Report in HTML, PDF, or Excel formats, respectively.

# Understanding the Reports

This section provides a description of each DbProtect Analytics Report. It consists of the following topics:

- *DbProtect Analytics Reports At-a-Glance*
- *Which DbProtect Analytics Reports Include Oracle Audit Vault Data?*
- *Risk Management*
- *Standards and Compliance*
- *System Information.*

**DbProtect  
Analytics Reports  
At-a-Glance**

The following table lists each available DbProtect Analytics Report (organized by category and subcategory), and provides a link to the Report detail.

Category	Subcategory	Report
Risk Management	Risk Management - Assessment	Database Findings Detailed Review Report
		Database Findings Detailed Review Report (with Knowledgebase Articles)
		Database Findings Summary Review Report
		Database Findings Summary Review Report (with Knowledgebase Articles)
		Database Inventory Report
		Job Findings Detailed Review Report (with Knowledgebase Articles)
		Job Findings Summary Review Report
		Weak Passwords Report
	Risk Management - Monitoring	Failed Logins Review Report
		Privileged Activity Report
		Threat Detailed Review Report
		Threat Detailed Review Report (with Knowledgebase Articles)
		Threat Summary Review Report
		Threat Summary Review Report (with Knowledgebase Articles)
		User Activity Report
	Risk Management - Policy Management	Available Policies Report
		Knowledgebase Detail Report
		Monitoring Configuration Report

Category	Subcategory	Report
Standards and Compliance	Standards and Compliance - Assessment	Compliance Report Wizard
		Health Insurance Portability and Accountability Act (HIPAA) - Vulnerability Assessment Report
		NIST 800-53 Report
		Payment Card Industry Data Security Standard (PCI DSS) - Vulnerability Assessment Report
		Sarbanes-Oxley (SOX) - Vulnerability Assessment Report
	Standards and Compliance - Monitoring	Payment Card Industry Data Security Standard (PCI DSS) - Activity Monitoring Report
		Sarbanes-Oxley (SOX) - Activity Monitoring Report
System Information	System Information - Diagnostics	Inactivity Alerts Report

## Which DbProtect Analytics Reports Include Oracle Audit Vault Data?

If you are using Oracle Audit Vault to audit your databases, then certain DbProtect Analytics Reports will include Oracle Audit Vault data. The specific DbProtect Analytics Reports that include Oracle Audit Vault data are:

- *Failed Logins Review Report*
- *Privileged Activity Report*
- *Threat Detailed Review Report*
- *Threat Detailed Review Report (with Knowledgebase Articles)*
- *Sarbanes-Oxley (SOX) - Vulnerability Assessment Report*
- *Payment Card Industry Data Security Standard (PCI DSS) - Activity Monitoring Report.*

In order to include Oracle Audit Vault data in your DbProtect Analytics Reports, you must properly install Oracle Audit Vault and register Oracle Audit Vault within DbProtect prior to running any DbProtect Analytics Reports that support Oracle Audit Vault data. For more information, see *Minimum Requirements for Using Oracle Audit Vault as a DbProtect Data Source* in the *DbProtect User's Guide*.

## Risk Management

This topic explains the DbProtect Analytics **Risk Management** Reports, organized in the following sub-categories:

- *Risk Management - Assessment*
- *Risk Management - Monitoring*
- *Risk Management - Policy Management.*

### **RISK MANAGEMENT - ASSESSMENT**

#### **Database Findings Detailed Review Report**

This Report provides a complete and detailed listing of the latest outside-in (Penetration) and inside-out (Audit) tests across all organizations. This Report groups the information by database instance providing deep visibility of issues within each database. The data and graph can be used to determine general trends, strengths and weaknesses of your database security.

#### **Database Findings Detailed Review Report (with Knowledgebase Articles)**

This Report provides a complete summary of the latest outside-in (Penetration) and inside-out (Audit) tests across all organizations. This Report groups the information by database instance providing deep visibility of issues within each database. The data and graph can be used to determine general trends, strengths and weaknesses of your database security. The last section of this Report includes an appendix of knowledgebase articles that correspond to the findings.

#### **Database Findings Summary Review Report**

This Report summarizes the collection of findings, the latest results from penetration tests and audits, across all the databases in the organization. This Report groups the information by database instance (or server) which represents the depth issues within each database instance (or server).

#### **Database Findings Summary Review Report (with Knowledgebase Articles)**

This Report provides a complete and detailed listing of the latest outside-in (Penetration) and inside-out (Audit) tests across all organizations. This Report groups the information by database instance providing deep visibility of issues within each database. The data and graph can be used to determine general trends, strengths and weaknesses of your database security. The last section of this Report includes an appendix of knowledgebase articles that correspond to the findings.

#### **Database Inventory Report**

This Report lists of all the discovered database instances (or servers). The network was inventoried by either an inventory import or by conducting a network sweep of IP addresses and investigating the responsive ports for the existence of applications using DbProtect AppDetective. This inventory information should be reviewed periodically to reconcile the systems against their business context. It is also important to evaluate the system versions and patch levels to ensure they are up to corporate standard.

### **Job Findings Detailed Review Report (with Knowledgebase Articles)**

This Report provides a complete and detailed listing of the latest outside-in (penetration) and inside-out (audit) tests for a selected job in a given organization. You can use the data and graphic to determine general trends, strengths and weaknesses of your database security. The last section of this report includes an appendix of knowledgebase articles that correspond to the findings.

### **Job Findings Summary Review Report**

This Report summarizes the collection of findings, the latest results from penetration tests and audits, across all the databases in the organization. It also summarizes the most recent information which represents the job execution initiated by administrator(s) of the organization.

### **Weak Passwords Report**

This Report shows all the occurrences of weak passwords. Weak passwords are vulnerabilities that have the potential for exploitation. They are much sought-after by hackers and can put your entire organization at risk. Weak passwords are easily guessable by a human or a computer within a finite timeframe. The longer the lifespan of a password, the weaker it becomes. Best practices suggest that regular password modifications combined with strong passwords helps to thwart the weak password threat.

## **RISK MANAGEMENT - MONITORING**

### **Failed Logins Review Report**

This activity Report provides a comprehensive history of failed database connection attempts. This Report should be reviewed periodically to examine whether an unauthorized threat existed or to investigate past incidents. Excessive login failures, patterned login failures, failures with non-existing accounts and default accounts, are some indicators of possible break-in attempts and should be cause for concern.

**Note:** If you are using Oracle Audit Vault to audit your databases, then this DbProtect Analytics Report will include Oracle Audit Vault data. In order to include Oracle Audit Vault data in your DbProtect Analytics Reports, you must properly install Oracle Audit Vault and register Oracle Audit Vault within DbProtect prior to running any DbProtect Analytics Reports that support Oracle Audit Vault data. For more information, see *Working with Oracle Audit Vault as a DbProtect Data Source* in the *DbProtect User's Guide*.

## Privileged Activity Report

This activity Report provides an audit trail of activity that is classified as privileged-- schema modifications, authorization changes, and administrative actions. This represents the privileged activity performed according to the active policy during the time of the recorded events. Regular reviews of privileged activity help to reduce the propagation of bad behavior and support the ability to thwart ongoing malicious activity. This can also be used in incident investigation. The authorized privileged activity can generally be matched to some change control reference, if your organization actively uses one.

**Note:** If you are using Oracle Audit Vault to audit your databases, then this DbProtect Analytics Report will include Oracle Audit Vault data. In order to include Oracle Audit Vault data in your DbProtect Analytics Reports, you must properly install Oracle Audit Vault and register Oracle Audit Vault within DbProtect prior to running any DbProtect Analytics Reports that support Oracle Audit Vault data. For more information, see *Working with Oracle Audit Vault as a DbProtect Data Source* in the *DbProtect User's Guide*.

## Threat Detailed Review Report

This threat Report provides a detailed view of all the security alerts that were generated across the organization. This is designed to provide the complete event details for the selected risk-events. Security Alerts are events that are classified with risk levels of **High**, **Medium**, and **Low**. These events should occur irregularly and be addressed in a timely manner. Any regularity of events should be questioned; it should become a candidate for policy change or process change.

**Note:** If you are using Oracle Audit Vault to audit your databases, then this DbProtect Analytics Report will include Oracle Audit Vault data. In order to include Oracle Audit Vault data in your DbProtect Analytics Reports, you must properly install Oracle Audit Vault and register Oracle Audit Vault within DbProtect prior to running any DbProtect Analytics Reports that support Oracle Audit Vault data. For more information, see *Working with Oracle Audit Vault as a DbProtect Data Source* in the *DbProtect User's Guide*.

## Threat Detailed Review Report (with Knowledgebase Articles)

This threat Report provides a complete detailed view of all the security alerts that were generated across the organization. This depth of information can be used to investigate issues raised by the **Threat Summary Review** Report. Security Alerts are events that are classified with risk levels of **High**, **Medium**, and **Low**. These events should occur irregularly and be addressed in a timely manner. Any regularity of events should be questioned; it should become a candidate for policy change or process change. The last section of this Report includes an appendix of knowledgebase articles that correspond to the findings.

**Note:** If you are using Oracle Audit Vault to audit your databases, then this DbProtect Analytics Report will include Oracle Audit Vault data. In order to include Oracle Audit Vault data in your DbProtect Analytics Reports, you must properly install Oracle Audit Vault and register Oracle Audit Vault within DbProtect prior to running any DbProtect Analytics Reports that support Oracle Audit Vault data. For more information, see *Working with Oracle Audit Vault as a DbProtect Data Source* in the *DbProtect User's Guide*.

### Threat Summary Review Report

This threat Report provides a summarized view of all the security alerts that were generated across the organization. This is designed to support high-level analysis of the risk-events that occurred within the environment. This summarized information can be used as a starting point for deeper investigation. Security Alerts are events that are classified with risk levels of **High**, **Medium**, and **Low**. These events should occur irregularly and be addressed in a timely manner. Any regularity of events should be questioned; it should become a candidate for policy change or process change.

### Threat Summary Review Report (with Knowledgebase Articles)

This is a version of the **Threat Summary Review Report** that includes an appendix of the relevant knowledgebase articles.

### User Activity Report

This activity Report provides an audit trail of user activity. This report provides activity details limited to a selection of users, or can provide full details on all user activity.

## RISK MANAGEMENT - POLICY MANAGEMENT

### Available Policies Report

This displays a listing of all policies that are available for use in the system. Policies are divided into three distinctive categories: 1) Penetration Tests; 2) Audits; and 3) Audit and Threat Management. The three Policy types are used to perform separate functions.

### Knowledgebase Detail Report

This Report shows knowledgebase articles for a selection of database types.

### Monitoring Configuration Report

This Report lists all of the database instances that have Audit and Threat Management turned on with their corresponding monitoring policy. The chart represents the distribution of active policies across all the monitored databases.



## Standards and Compliance

This topic explains the DbProtect Analytics **Risk Management** Reports, organized in the following sub-categories:

- *Standards and Compliance - Assessment*
- *Standards and Compliance - Monitoring.*

### STANDARDS AND COMPLIANCE - ASSESSMENT

#### Compliance Report Wizard

This is a Report that presents the results as it maps to your selected compliance policy. Use this wizard to generate details that meet the compliance standards described by your policies.

#### Health Insurance Portability and Accountability Act (HIPAA) - Vulnerability Assessment Report

This Report is an indicator of compliance with Health Insurance Portability and Accountability Act (HIPAA). This Report is based on the out-of-the-box policy that maps regulatory standards to the appropriate vulnerability checks. Use this Report as a gauge of compliance with regulatory compliance.

#### NIST 800-53 Report

This Report is an indicator of compliance with NIST 800-53. NIST 800-53 is the recommended guideline for security controls for a federal information system. This is applicable to all federal agencies and any government entity that follows the NIST standard. The NIST 800-53 guideline breaks down security controls into six categories: Access Control (AC), Audit and Accountability (AU), Identification and Authentication (IA), Configuration Management (CM), System and Communications Protection (SC), and System and Information Integrity (SI). This Report provides the results of vulnerability findings mapped to the six security control categories.

#### Payment Card Industry Data Security Standard (PCI DSS) - Vulnerability Assessment Report

This Report is an indicator of compliance with Payment Card Industry Data Security Standard (PCI DSS). This Report is based on the out-of-the-box policy that maps regulatory standards to the appropriate vulnerability checks. Use this Report as a gauge of compliance with regulatory compliance.

**Note:** If you are using Oracle Audit Vault to audit your databases, then this DbProtect Analytics Report will include Oracle Audit Vault data. In order to include Oracle Audit Vault data in your DbProtect Analytics Reports, you must properly install Oracle Audit Vault and register Oracle Audit Vault within DbProtect prior to running any DbProtect Analytics Reports that support Oracle Audit Vault data. For more information, see *Working with Oracle Audit Vault as a DbProtect Data Source* in the *DbProtect User's Guide*.

### **Sarbanes-Oxley (SOX) - Vulnerability Assessment Report**

This Report is an indicator of compliance with Sarbanes-Oxley (SOX). This Report is based on the out-of-the-box policy that maps regulatory standards to the appropriate vulnerability checks. Use this Report as a gauge of compliance with regulatory compliance.

**Note:** If you are using Oracle Audit Vault to audit your databases, then this DbProtect Analytics Report will include Oracle Audit Vault data. In order to include Oracle Audit Vault data in your DbProtect Analytics Reports, you must properly install Oracle Audit Vault and register Oracle Audit Vault within DbProtect prior to running any DbProtect Analytics Reports that support Oracle Audit Vault data. For more information, see *Working with Oracle Audit Vault as a DbProtect Data Source* in the *DbProtect User's Guide*.

## **STANDARDS AND COMPLIANCE - MONITORING**

### **Payment Card Industry Data Security Standard (PCI DSS) - Activity Monitoring Report**

This Report highlights database activity that pertains to Payment Card Industry Data Security Standard (PCI DSS) compliance. This Report is based on an out-of-the-box policy that maps regulatory standards to the appropriate Audit and Threat Management rules. Use this Report to summarize activity that may compromise compliance with this regulatory standard.

### **Sarbanes-Oxley (SOX) - Activity Monitoring Report**

This Report highlights database activity that pertains to Sarbanes-Oxley (SOX) compliance. This Report is based on an out-of-the-box policy that maps regulatory standards to the appropriate Audit and Threat Management rules. Use this Report to summarize activity that may compromise compliance with this regulatory standard.

## System Information

This topic explains the DbProtect Analytics **System Information** Report (i.e., the *Inactivity Alerts Report*), which belongs to the sub-category *System Information - Diagnostics*.

### SYSTEM INFORMATION - DIAGNOSTICS

#### Inactivity Alerts Report

Inactivity alerts are special diagnostic events that a Sensor sends when it does not detect any database activity for a pre-determined period of time. That period is configurable and should be evaluated for each environment to determine its appropriate value. Inactivity alerts can also be shut off. Inactivity at the database may or may not be considered normal behavior depending on its usage. Peak and Off-peak hours, weekend and holidays, business hours are all factors that contribute to normal occurrences of inactivity alerts. However, if the profile of the inactivity alerts change, then there is reasonable cause to investigate its shift. Under normal circumstances, you should be able associate shifts to an environmental change. Otherwise, this is an indicator that the monitoring system has been modified or is experiencing difficulty.

# Appendices

## What you will find in these appendices:

- *Appendix A: Resolving Problems Quickly*
- *Appendix B: Key Issues*
- *Appendix C: Troubleshooting Installation Errors*
- *Appendix D: Troubleshooting Runtime Errors.*

# Appendix A: Resolving Problems Quickly

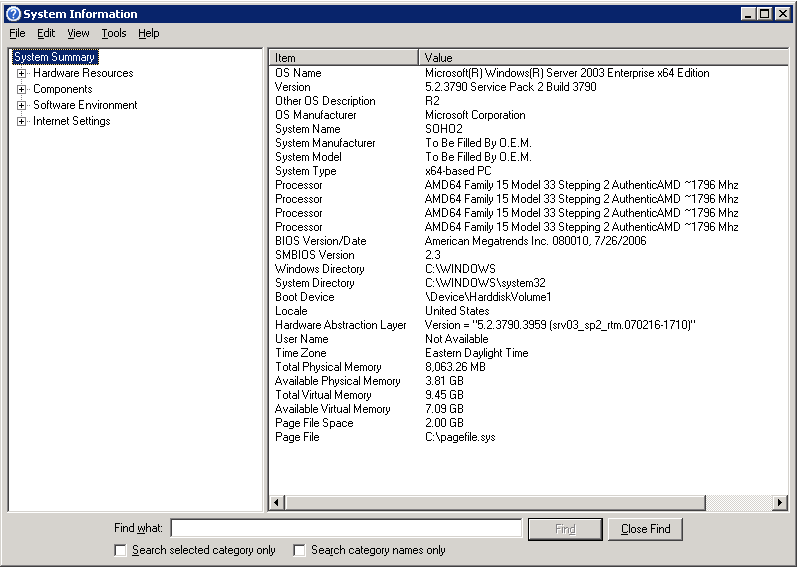
This appendix provides a list of items you should gather before you contact Application Security, Inc. Support ([support@appsecinc.com](mailto:support@appsecinc.com)). This information allows us to rapidly identify the source of a problem, and provide a quick resolution. Key information elements include:

- *Operating System Characteristics*
- *Log File to Troubleshoot Installation Problems*
- *Key Configuration and Log Files.*

## Operating System Characteristics

It is beneficial to find out your hardware and software system characteristics in order to help determine if they are causing the issues you are experiencing. One easy way to obtain this information is to run the built-in system information utility from Microsoft.

Do the following:

Step	Action																																																								
1	<p>Choose <b>Start &gt; Run &gt; msinfo32.exe</b>. A window similar to the one below displays.</p>  <table border="1"><thead><tr><th>Item</th><th>Value</th></tr></thead><tbody><tr><td>OS Name</td><td>Microsoft(R) Windows(R) Server 2003 Enterprise x64 Edition</td></tr><tr><td>Version</td><td>5.2.3790 Service Pack 2 Build 3790</td></tr><tr><td>Other OS Description</td><td>R2</td></tr><tr><td>OS Manufacturer</td><td>Microsoft Corporation</td></tr><tr><td>System Name</td><td>SDH02</td></tr><tr><td>System Manufacturer</td><td>To Be Filled By O.E.M.</td></tr><tr><td>System Model</td><td>To Be Filled By O.E.M.</td></tr><tr><td>System Type</td><td>x64-based PC</td></tr><tr><td>Processor</td><td>AMD64 Family 15 Model 33 Stepping 2 AuthenticAMD ~1796 Mhz</td></tr><tr><td>Processor</td><td>AMD64 Family 15 Model 33 Stepping 2 AuthenticAMD ~1796 Mhz</td></tr><tr><td>Processor</td><td>AMD64 Family 15 Model 33 Stepping 2 AuthenticAMD ~1796 Mhz</td></tr><tr><td>Processor</td><td>AMD64 Family 15 Model 33 Stepping 2 AuthenticAMD ~1796 Mhz</td></tr><tr><td>BIOS Version/Date</td><td>American Megatrends Inc. 080010, 7/26/2006</td></tr><tr><td>SMBIOS Version</td><td>2.3</td></tr><tr><td>Windows Directory</td><td>C:\WINDOWS</td></tr><tr><td>System Directory</td><td>C:\WINDOWS\system32</td></tr><tr><td>Boot Device</td><td>\Device\Harddisk\Volume1</td></tr><tr><td>Locale</td><td>United States</td></tr><tr><td>Hardware Abstraction Layer</td><td>Version = "5.2.3790.3959 (srv03_sp2_rtm.070216-1710)"</td></tr><tr><td>User Name</td><td>Not Available</td></tr><tr><td>Time Zone</td><td>Eastern Daylight Time</td></tr><tr><td>Total Physical Memory</td><td>8,063.26 MB</td></tr><tr><td>Available Physical Memory</td><td>3.81 GB</td></tr><tr><td>Total Virtual Memory</td><td>9.45 GB</td></tr><tr><td>Available Virtual Memory</td><td>7.09 GB</td></tr><tr><td>Page File Space</td><td>2.00 GB</td></tr><tr><td>Page File</td><td>C:\pagefile.sys</td></tr></tbody></table>	Item	Value	OS Name	Microsoft(R) Windows(R) Server 2003 Enterprise x64 Edition	Version	5.2.3790 Service Pack 2 Build 3790	Other OS Description	R2	OS Manufacturer	Microsoft Corporation	System Name	SDH02	System Manufacturer	To Be Filled By O.E.M.	System Model	To Be Filled By O.E.M.	System Type	x64-based PC	Processor	AMD64 Family 15 Model 33 Stepping 2 AuthenticAMD ~1796 Mhz	Processor	AMD64 Family 15 Model 33 Stepping 2 AuthenticAMD ~1796 Mhz	Processor	AMD64 Family 15 Model 33 Stepping 2 AuthenticAMD ~1796 Mhz	Processor	AMD64 Family 15 Model 33 Stepping 2 AuthenticAMD ~1796 Mhz	BIOS Version/Date	American Megatrends Inc. 080010, 7/26/2006	SMBIOS Version	2.3	Windows Directory	C:\WINDOWS	System Directory	C:\WINDOWS\system32	Boot Device	\Device\Harddisk\Volume1	Locale	United States	Hardware Abstraction Layer	Version = "5.2.3790.3959 (srv03_sp2_rtm.070216-1710)"	User Name	Not Available	Time Zone	Eastern Daylight Time	Total Physical Memory	8,063.26 MB	Available Physical Memory	3.81 GB	Total Virtual Memory	9.45 GB	Available Virtual Memory	7.09 GB	Page File Space	2.00 GB	Page File	C:\pagefile.sys
Item	Value																																																								
OS Name	Microsoft(R) Windows(R) Server 2003 Enterprise x64 Edition																																																								
Version	5.2.3790 Service Pack 2 Build 3790																																																								
Other OS Description	R2																																																								
OS Manufacturer	Microsoft Corporation																																																								
System Name	SDH02																																																								
System Manufacturer	To Be Filled By O.E.M.																																																								
System Model	To Be Filled By O.E.M.																																																								
System Type	x64-based PC																																																								
Processor	AMD64 Family 15 Model 33 Stepping 2 AuthenticAMD ~1796 Mhz																																																								
Processor	AMD64 Family 15 Model 33 Stepping 2 AuthenticAMD ~1796 Mhz																																																								
Processor	AMD64 Family 15 Model 33 Stepping 2 AuthenticAMD ~1796 Mhz																																																								
Processor	AMD64 Family 15 Model 33 Stepping 2 AuthenticAMD ~1796 Mhz																																																								
BIOS Version/Date	American Megatrends Inc. 080010, 7/26/2006																																																								
SMBIOS Version	2.3																																																								
Windows Directory	C:\WINDOWS																																																								
System Directory	C:\WINDOWS\system32																																																								
Boot Device	\Device\Harddisk\Volume1																																																								
Locale	United States																																																								
Hardware Abstraction Layer	Version = "5.2.3790.3959 (srv03_sp2_rtm.070216-1710)"																																																								
User Name	Not Available																																																								
Time Zone	Eastern Daylight Time																																																								
Total Physical Memory	8,063.26 MB																																																								
Available Physical Memory	3.81 GB																																																								
Total Virtual Memory	9.45 GB																																																								
Available Virtual Memory	7.09 GB																																																								
Page File Space	2.00 GB																																																								
Page File	C:\pagefile.sys																																																								

**FIGURE: System Information window**

Key information elements here for Application Security, Inc. Support are:

- **Total / Available Physical Memory**
- **Total / Available Virtual Memory**
- **Page File Space**
- **OS Name**
- **Version**
- **Locale.**

**Log File to Troubleshoot Installation Problems**

In the event that you have problems installing DbProtect Analytics, Application Security, Inc. Support will instruct you to run the installer, starting it from the command line as follows: `msiexec /i DbPAnalytics_1.0.xxxx.yy.msi /l*x installer.log`

**Caution!** Since this is a technical “dump” of your install process, sometimes there may be credential information recorded in this manually generated log file. Review the contents of this log to remove any sensitive credential information before sending it to any Support professionals.

Remember, this log is only generated upon request, with manual intervention. Such sensitive credential information is **not** recorded during the routine operation of the DbProtect Analytics installer.

## Key Configuration and Log Files

Sometimes it may be necessary for Support personnel to investigate a problem in more detail. In order to help us in this process, it is beneficial to collect the following files/directories with key information.

```
<DbProtect Installation Root>/Reporting/media/c8/logs
```

```
<DbProtect Installation Root>/Reporting/media/c8/configuration/  
cogstartup.xml
```

```
<DbProtect Installation Root>/GUI/logs
```

```
<DbProtect Installation Root>/GUI/tomcat/conf/wrapper.conf
```

```
<DbProtect Installation Root>/GUI/tomcat/conf/Catalina/localhost
```

```
<DbProtect Installation Root>/GUI/tomcat/logs
```

In addition to these, it is also useful to record how the DbProtect Console and Analytics services are run. To verify this, do the following:

- Choose **Start > Control Panel > Administrative Tools > Services**.
- Locate the services **DbProtect Console** and **Cognos 8**.
- Right-click the service name and select **Properties** to display the **Properties** dialog box.
- Click the **Log On** tab.

Record the current selection for **Local System Account**, or the account specified under **This account**.

# Appendix B: Key Issues

This appendix consists of the following topics:

- *Installation, Uninstallation, and Repair*
- *Credential Management*
- *Service Creation*
- *Reports.*

## Installation, Uninstallation, and Repair

- To uninstall DbProtect Analytics via the Start Menu (recommended), choose: **Start > Program Files > AppSecInc > DbProtect > Uninstall Analytics.**
- When you uninstall DbProtect Analytics -- either from the Start Menu or the Control Panel -- you **must** manually address some intentional cleanup items. The following steps need to be completed in order to cleanly remove all artifacts from a DbProtect Analytics installation:
  - Remove the [DbpAnalytics](#) database (created at time of installation on the same database instance as the DbProtect Console Data Repository). You may do this from any of the Microsoft SQL Server tools (such as Microsoft SQL Management Studio or Query Analyzer). Do the following: 1.) Log in to the Microsoft SQL Server instance with appropriate privileges allowing you to drop databases. 2.) Locate the database [DbpAnalytics](#) in the Object Explorer. 3.) Right click the database [DbpAnalytics](#) and select **Delete**.
  - Remove any files and folders that remain in the [<DbProtect Console Root>/Reporting](#) folder. You may also remove the [Reporting](#) folder.
- Uninstall fails if any DbProtect Console browser windows are open. Ensure all DbProtect Console browser windows are closed prior to uninstalling.

## Credential Management

DbProtect Analytics allows for both SQL and Windows authentication modes. If you are using SQL authentication, there is currently no UI for credential management. Contact the Application Security, Inc. Support team to obtain a specific utility and instructions to affect this type of credential change.

## Service Creation

The DbProtect Analytics installer prompts the user for service log on credentials. If a user is specified but not domain-qualified (as domain\user, for local users, use the host name instead of the domain), the service credential setting is reverted to **Log On as Local System**. Open the **Services** dialog box (choose **Start > Control Panel > Administrative Tools > Services**) and set the appropriate account credentials from the Log On tab, after you complete the installation.



## Reports

DbProtect Analytics includes a set of export options that allows you to save report data in a number of XLS/CSV formats. If you see a flash, but do not successfully export any content when you select one of these options, ensure the following:

- You do not have an active pop up blocker that is closing the window.

OR

- Your browser's security settings allow the DbProtect Console site to open windows and download file content. You may need to add the DbProtect Console site to your list of trusted sites.

OR

- In the case of generating an Excel spreadsheet (XLS) report, make sure you have enabled **Automatic prompting for file downloads** within Internet Explorer. To do so, choose: **Internet Options > Security Tab > Custom Level > Downloads > Automatic prompting for file downloads > Enable.**

# Appendix C: Troubleshooting Installation Errors

This appendix explains how to troubleshoot common DbProtect Analytics **installation** errors. It consists of the following topics:

- *"The Setup Wizard determined that this is not enough space to install DbProtect Analytics"*
- *"Your machine has XXX MB of physical memory; at least YYY GB is required to install DbProtect Analytics"*
- *"Your machine has XXX MB of physical memory; at least YYY GB is recommended to install DbProtect Analytics"*
- *"This account does not have logon as service right or account privileges could not be obtained"*
- *"DbProtect Analytics Setup Wizard was interrupted"*
- *"DbProtect Analytics Setup Wizard ended prematurely".*

**"The Setup Wizard determined that this is not enough space to install DbProtect Analytics"**

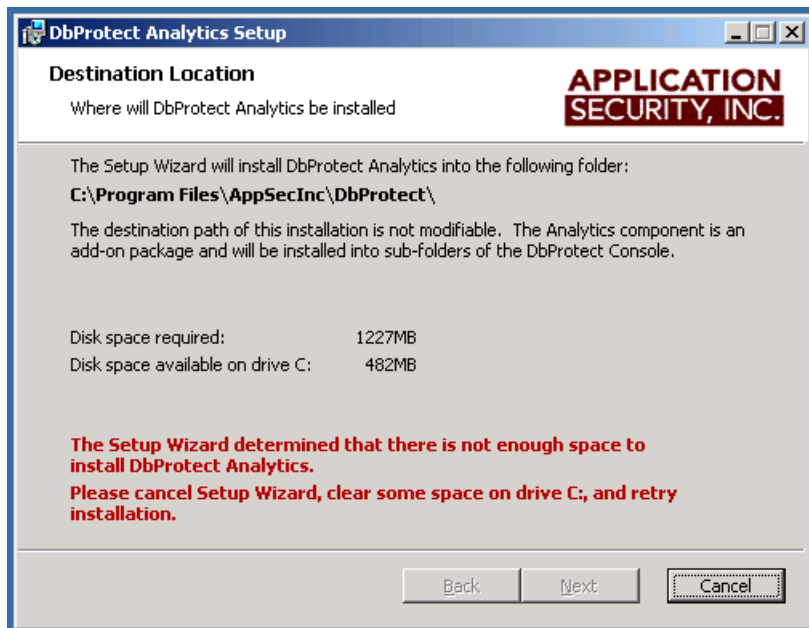


FIGURE: "The Setup Wizard determined that this is not enough space to install DbProtect Analytics" error message

DbProtect Analytics is installed as an add-on component to DbProtect Console, in the same drive location as the DbProtect Console. For more information, see the *DbProtect Installation Guide*.

**"Your machine has  
XXX MB of  
physical memory;  
at least YYY GB is  
required to install  
DbProtect  
Analytics"**

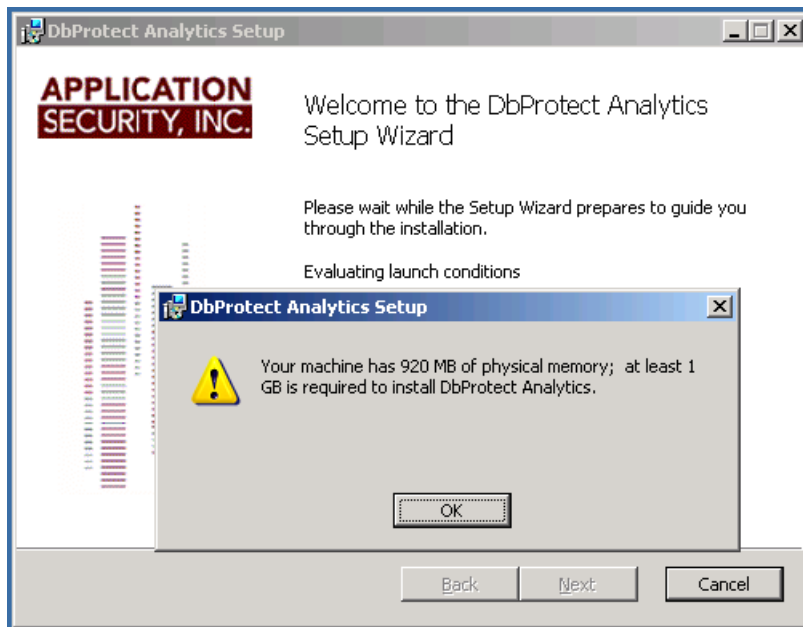
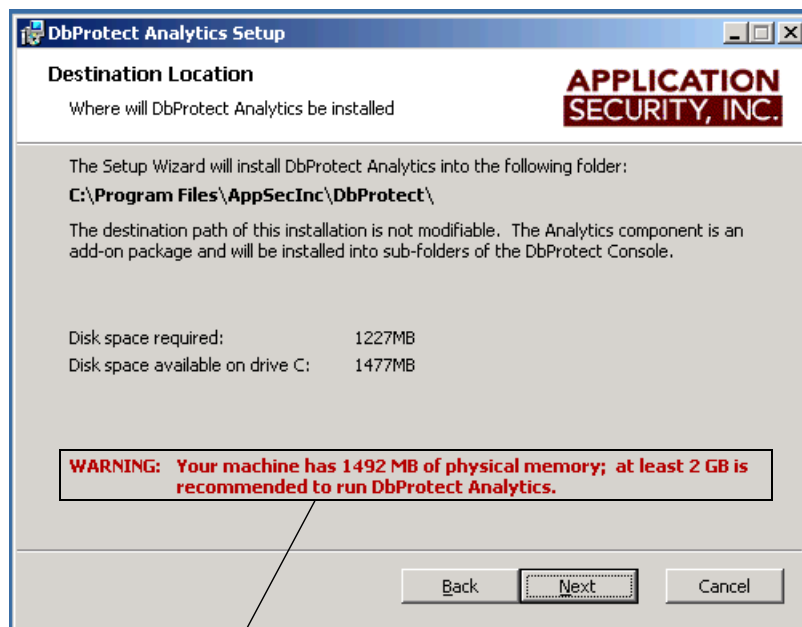


FIGURE: "Your machine has XXX MB of physical memory; at least YYY GB is required to install DbProtect Analytics" error message

DbProtect Analytics enforces that at least 1 GB of RAM is present to complete the installation. This allows you to complete the installation process, but may yield poor performance except with very small data sets. Make sure you meet all the physical hardware requirements before you install. For more information, see the *DbProtect Installation Guide*.

**"Your machine has  
XXX MB of  
physical memory;  
at least YYY GB is  
recommended to  
install DbProtect  
Analytics"**



Memory warning

FIGURE: "Your machine has XXX MB of physical memory; at least YYY GB is recommended to install DbProtect Analytics" error message

There is enough memory to proceed with the installation; however, it is below the recommended hardware configuration. Please make sure you meet all the physical hardware requirements before you install. For more information, see the *DbProtect Installation Guide*.

"This account does not have logon as service right or account privileges could not be obtained"

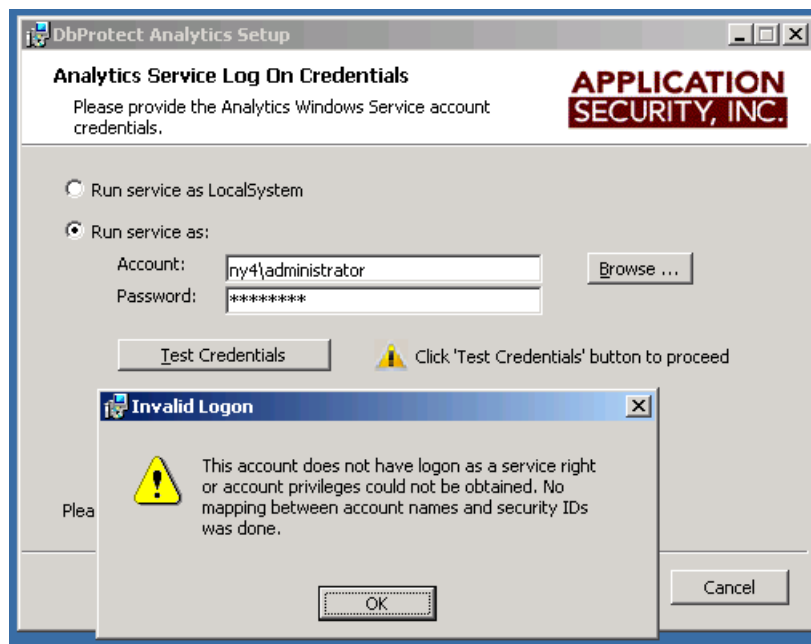


FIGURE: "This account does not have logon as service right or account privileges could not be obtained" error message

DbProtect Analytics runs as a service called *Cognos 8*. The credentials you enter into the installer for a runtime user are used to run this service. The account you are using to run the installer needs to have the necessary privileges to check for the **Log on as a service** rights. The specified runtime user needs to have these rights granted to them. Make sure you have the necessary privileges and accounts listed in *What You Will Need*.

**"DbProtect  
Analytics Setup  
Wizard was  
interrupted"**

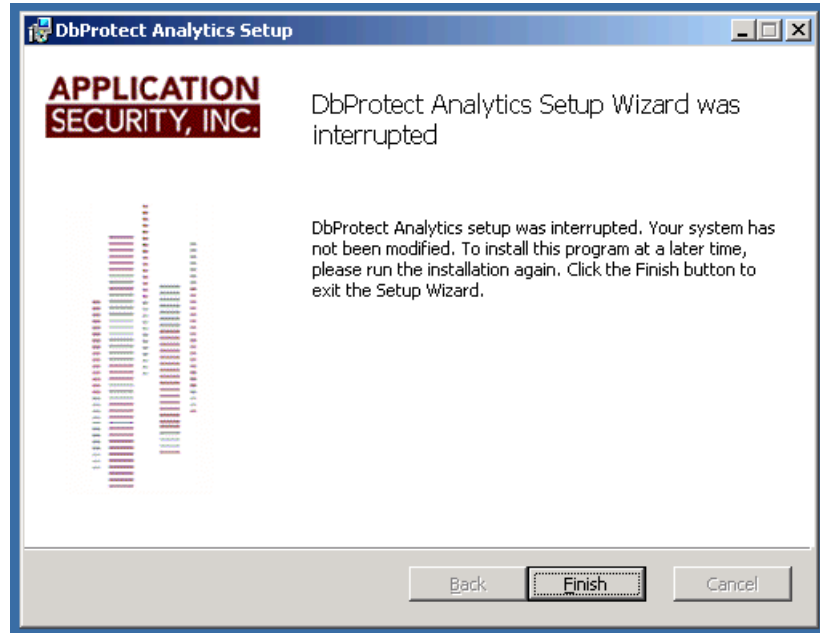


FIGURE: "DbProtect Analytics Setup Wizard was interrupted" error message

This screen confirms that you have aborted an in-progress DbProtect Analytics installation. If you received this unexpectedly, click the **Finish** button, then confirm the installation has exited by checking the **Task Manager**. Once the installer process has exited, you may restart the installation.

**“DbProtect  
Analytics Setup  
Wizard ended  
prematurely”**

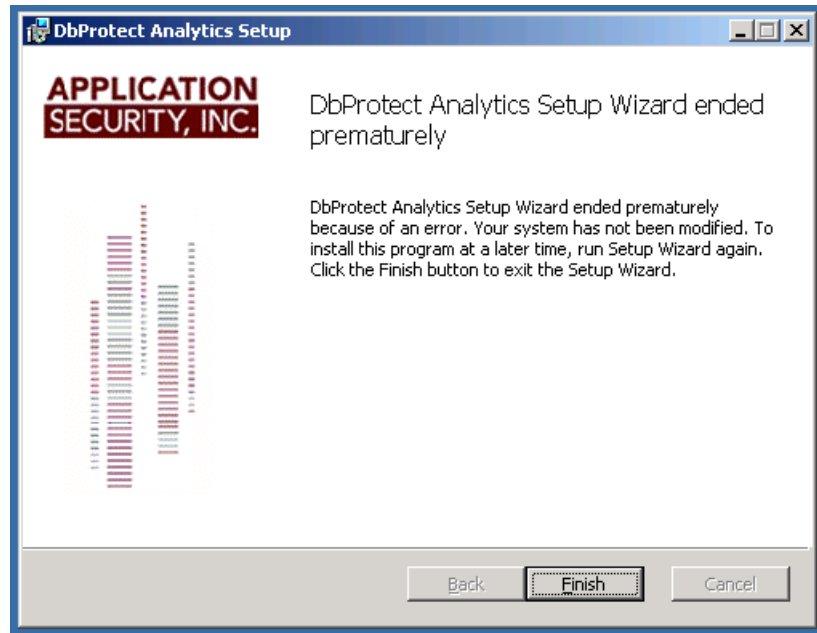


FIGURE: “DbProtect Analytics Setup Wizard ended prematurely” error message

This screen confirms that the DbProtect Analytics installation has failed. There are many environmental factors that might lead to a failure. Typically, these failures are related to login rights, either for the database instance, or on the host. Please make sure you have the necessary privileges and accounts enumerated in the section *What You Will Need*.



# Appendix D: Troubleshooting Runtime Errors

This appendix explains how to troubleshoot common DbProtect Analytics **runtime** errors. It consists of the following topics:

- *You Do Not See the Analytics Tab in DbProtect Console*
- *Your Browser Displays the "Cannot find server" Page*
- *The Message "CAM-AAA-1079 The 3rd party provider returned an unrecoverable exception" Displays When You Navigate to the Analytics tab, from DbProtect Console*
- *Upon Navigating to the Analytics Tab Within DbProtect Console, the Message "The Cognos gateway is unable to connect to the Cognos BI server" Displays*
- *The "Your report is running, please wait ..." Page Displays for a Long Time*
- *The Message "RSV-XXX-XXXX The request 'asynchWait\_Request' failed because the Conversation was already canceled" Appears in Place of a Report or Dashboard*
- *The Message "RSV-XXX-XXXX The absolute affinity request 'asynchWait\_Request' failed, the requested session does not exist" Displays in Place of a Report or Dashboard*
- *Excel Spreadsheet Report Generation Fails With a DPR-ERR-2079 Firewall Security Rejection Error Message*

## You Do Not See the Analytics Tab in DbProtect Console

Access to DbProtect Analytics is restricted to users of DbProtect AppDetective that belong to the "root" organization. This is intentional, in the interest of maintaining the current level of access rights and privacy enforced within DbProtect. Identify a suitable user and authenticate to DbProtect Console (AppDetective) as that user. For more information, see *Using DbProtect Analytics*.

## Your Browser Displays the "Cannot find server" Page

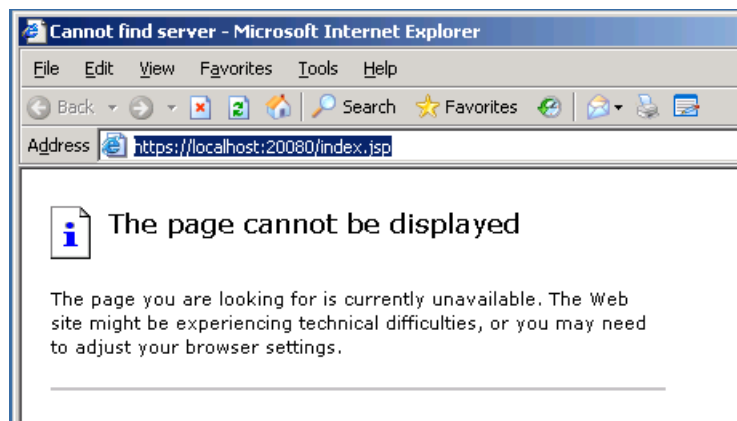


FIGURE: "Cannot find server" page

This error typically confirms that either the [DbProtect Console](#) service is not running or unreachable. Verify the DbProtect services are running on the host for DbProtect Console. Also confirm the server port for browser access is entered correctly. The default port is [20080](#).

## The Message "CAM-AAA-1079 The 3rd party provider returned an unrecoverable exception" Displays When You Navigate to the Analytics tab, from DbProtect Console

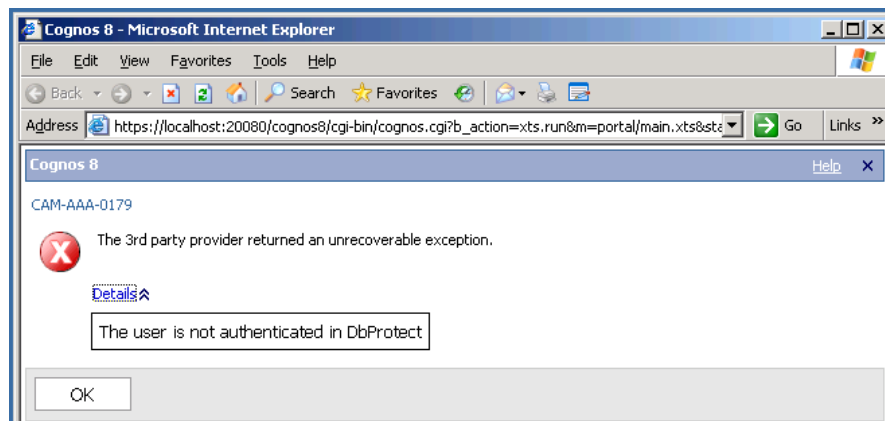


FIGURE: "CAM-AAA-1079 The 3rd party provider returned an unrecoverable exception" error message

This error typically confirms that you have tried to navigate to DbProtect Analytics without first authenticating to DbProtect Console. Since DbProtect Analytics is an add-on portal within DbProtect Console, only authenticated users are allowed to access the Analytics portal. Please identify a suitable user and authenticate to DbProtect Console as that user. Then select the **Analytics** tab to navigate to DbProtect Analytics. For more information, see *Navigating the DbProtect Analytics Portal*.

Upon Navigating to the Analytics Tab Within DbProtect Console, the Message “The Cognos gateway is unable to connect to the Cognos BI server” Displays

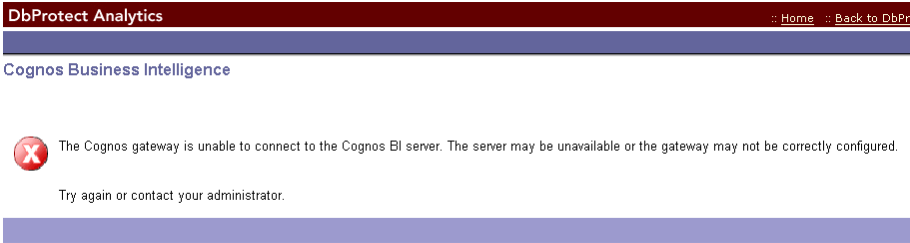


FIGURE: “The Cognos gateway is unable to connect to the Cognos BI server” error message

If the error message “The Cognos gateway is unable to connect to the Cognos BI server” displays, the server may be unavailable or the gateway may not be correctly configured. Try again or contact your administrator.

This error typically confirms that the DbProtect Analytics service (Cognos 8) is not running. This may be because it was not net to start up automatically, or the service user did not have the necessary rights. Start the service, exit, log back in to DbProtect Console, and navigate to DbProtect Analytics. If you need to validate the runtime user's privileges, see *What You Will Need*.

The “Your report is running, please wait ...” Page Displays for a Long Time

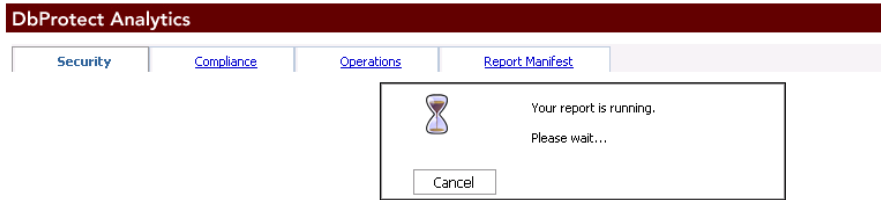


FIGURE: “Your report is running, please wait” page

This page displays when DbProtect Analytics is preparing a Report or computing a Dashboard. If you have just installed DbProtect Analytics, you will probably see an initial lag in the loading of Dashboards. This is because the pre-generated Dashboards are not yet available, thus requiring DbProtect Analytics to compute the Dashboards on-demand.

DbProtect Analytics regenerates the Dashboards every three hours. This allows the portals to load quickly, since it just serves the Dashboards from already-generated version on the DbProtect Analytics server.

If this message displays for a long time on your Reports and Dashboards (after your first day of installing and using DbProtect Analytics), you should verify your hardware configuration; for more information, see the *DbProtect Installation Guide*.

**The Message "RSV-XXX-XXXX The request 'asynchWait\_Request' failed because the Conversation was already canceled" Appears in Place of a Report or Dashboard**

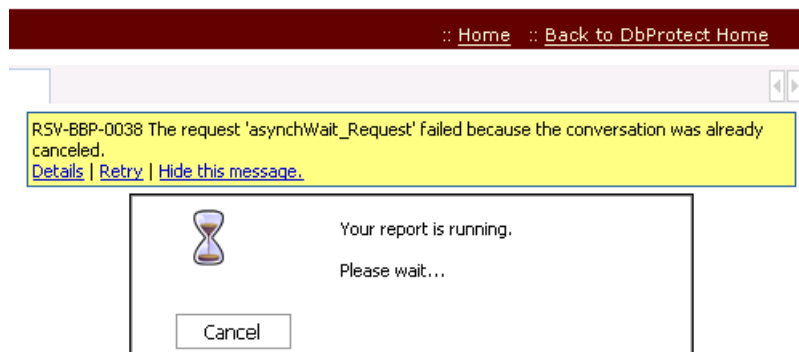


FIGURE: "RSV-XXX-XXXX The request 'asynchWait\_Request' failed because the Conversation was already canceled" error message

This message often displays when the host running DbProtect Console and DbProtect Analytics is starved of resources, or the SQL Server database repository is slow or non-responsive.

If this is a sporadic problem, click on the **Retry** link. This re-issues the request and the element or page should repaint normally. If this is a regular problem, consider whether your hardware environment continues to be within the recommended parameters. If you are operating on large data sets, it is important you have enough processor and memory resources, both on the host running DbProtect Analytics as well as the host running SQL Server. You should verify your hardware configuration; for more information, see the *DbProtect Installation Guide*.

**The Message "RSV-XXX-XXXX The absolute affinity request 'asynchWait\_Request' failed, the requested session does not exist" Displays in Place of a Report or Dashboard**

This message displays when the browser's session with DbProtect Analytics has timed out. Your browser may have been idle for a long time, or you may have participated in navigation that caused the DbProtect Analytics session to be abandoned. Close the browser, or locate a valid DbProtect Console browser session, and navigate to DbProtect Analytics; for more information, see *Navigating the DbProtect Analytics Portal*.

## **Excel Spreadsheet Report Generation Fails With a DPR- ERR-2079 Firewall Security Rejection Error Message**

This message displays if you are trying to generate an Excel spreadsheet (XLS) report, and you have **not** enabled **Automatic prompting for file downloads** within Internet Explorer.

To do so, choose: **Internet Options > Security Tab > Custom Level > Downloads > Automatic prompting for file downloads > Enable**.