

# **Idera SharePoint audit - Administration Guide**

Idera

**Version 2.5**



## Purpose and audience of document

This document describes the installation steps, general administrative topics and day to day usage of Idera SharePoint audit.

The intended audience is anyone involved in the installation, administration and use of this solution.

## Disclaimer

Idera – a division of BBS Technologies, Inc., DTx, IntelliCompress, Point admin toolset, Pointbackup, Pointcheck, PowerShellPlus, SharePoint diagnostic manager, SharePoint backup, SharePoint performance monitor, SQLcheck, SQL change manager, SQLconfig, SQL comparison toolset, SQL compliance manager, SQLcompliance, SQLcm, SQL defrag manager, SQL diagnostic manager, SQLdm, SQL mobile manager, SQLpermissions, SQLsafe, SQLsafe Freeware Edition, SQLsafe Lite, SQLscaler, SQLschedule, SQL schema manager, SQLsecure, SQLsmarts, SQLstats, SQLtool, SQL toolbox, SQL virtual database, SQLvdb, virtual database, Idera, BBS Technologies and the Idera logo are trademarks or registered trademarks of BBS Technologies, Inc., or its subsidiaries in the United States and other jurisdictions. All other company and product names may be trademarks or registered trademarks of their respective companies. © 2011 BBS Technologies, Inc., all rights reserved.

THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT ARE FURNISHED UNDER AND ARE SUBJECT TO THE TERMS OF A LICENSE AGREEMENT. EXCEPT AS EXPRESSLY SET FORTH IN SUCH LICENSE AGREEMENT, BBS TECHNOLOGIES, INC., PROVIDES THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. SOME STATES DO NOT ALLOW DISCLAIMERS OF EXPRESS OR IMPLIED WARRANTIES IN CERTAIN TRANSACTIONS; THEREFORE, THIS STATEMENT MAY NOT APPLY TO YOU. YOU ARE ENCOURAGED TO READ THE LICENSE AGREEMENT BEFORE INSTALLING OR USING THIS DOCUMENTATION OR SOFTWARE.

Some companies, names, and data in this document are used for illustration purposes and may not represent real companies, individuals, or data.

This document could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein. These changes may be incorporated in new editions of this document. BBS Technologies, Inc., may make improvements in or changes to the software described in this document at any time.

© 2003-2011 BBS Technologies, Inc., all rights reserved.

U.S. Government Restricted Rights: The software and the documentation are commercial computer software and documentation developed at private expense. Use, duplication, or disclosure by the Government is subject to the terms of the BBS Technologies, Inc., standard commercial license for the software, and where applicable, the restrictions set forth in the Rights in Technical Data and Computer Software clauses and any successor rules or regulations.

## Contents

1	Introduction	6
1.1	Prerequisites	6
1.2	Improvements over standard SharePoint Auditing	7
2	Deployment	8
2.1	Upgrading from Muhimbi SharePoint Audit 2.0	8
2.2	Installation	9
2.2.1	Installing	9
2.2.2	the Windows Service	9
2.2.3	Installing / upgrading the SharePoint Front End	10
2.2.4	Feature Activation / Deactivation	10
2.2.5	Installing the License	11
2.3	Un-installation	11
2.3.1	Un-installing the Audit service	11
2.3.2	Un-installing the SharePoint Front End via the command line	11
2.3.3	Un-installing the SharePoint Front End via Central Administration	11
3	General Usage	13
3.1	Initial Configuration	13
3.1.1	Creating the database	13
3.1.2	Configuring the audit log crawlers	14
3.1.3	Changing the Audit Service's Config file.	16
3.2	Administering audit settings	17
3.2.1	Farm Level settings	18
3.2.2	Web Application Level settings	20
3.2.3	Site collection Level settings	22
3.3	Monitoring the audit system	23
3.4	Viewing audit logs	25
3.4.1	Web Application Level	25
3.4.2	Site collection Level	29
3.4.3	List Level	29
3.4.4	Folder and Item level	30
3.5	Running Reports	31
3.5.1	Exporting Audit data to Excel	31
3.5.2	Running predefined reports	32
3.5.3	Creating custom reports	33
4	Troubleshooting & Other common tasks	35
4.1	Windows Event Log	35
4.2	SharePoint Trace Log	35
4.3	SharePoint audit log	35
4.4	Audit Service trace log	36
4.5	Common issues & Errors	36
4.5.1	Your account is not allowed to deploy SharePoint Solutions	36
4.5.2	Authentication information is not being logged or not correctly	36
4.5.3	Errors on newly added servers	36
4.5.4	An evaluation message is displayed in the User Interface	36
4.5.5	'Unknown Error' or 'resource object not found'	37
4.5.6	Viewing audit logs is slow	38
	Appendix – Service and Database Accounts	39
	Audit Service account	39
	SharePoint Privileges	39
	Database Privileges – Windows Authentication	39

Database Privileges – SQL Authentication	39
Security settings for Central Administration pages	40
SharePoint Privileges	40
Database Privileges – Windows Authentication	40
Database Privileges – SQL Authentication	40
Security settings for Individual Site collections	41
SharePoint Privileges	41
Database Privileges – Windows Authentication	41
Database Privileges – SQL Authentication	41

## 1 Introduction

This document describes the installation steps, general administrative topics and day to day usage of Idera SharePoint audit.

The intended audience is anyone involved in the installation, administration and use of this solution. It is assumed that the audience has some familiarity with administering SharePoint and SQL Server, and have been given the privileges to install and deploy solutions to the SharePoint farm and administer SQL Server.

For more details about this product please see:

[www.idera.com/Products/SharePoint/SharePoint-audit/](http://www.idera.com/Products/SharePoint/SharePoint-audit/)

### 1.1 Prerequisites

The solution has been designed to work on an as wide as possible number of platforms. The prerequisites are as follows:

Operating Systems	Windows Server 2003 32 / 64 bit (including R2) Windows Server 2008 32 / 64 bit (including R2)
SharePoint versions	WSS 3.0 SP1 + July 2008 Infrastructure upgrade MOSS2007 SP1 + July 2008 Infrastructure upgrade SP Foundation 2010 / SP Server 210
SQL versions	Microsoft SQL Server 2005 or Microsoft SQL Server 2008 Enterprise, Standard, or Express Edition.
Browser versions	Administrators / End users: Internet Explorer 6, 7, 8 End users only: Firefox, Chrome, Safari.
Memory	This depends on the amount of audit log data being tracked. We recommend a minimum of 1.5GB of total memory per SharePoint server.
CPU	Any CPU that can comfortably run your SharePoint environment will be suitable. We recommend one or more multi-core CPUs.
Disk Space	This product requires 5MB of disk space.

## 1.2 Improvements over standard SharePoint Auditing

SharePoint ships with basic auditing capabilities, however these capabilities are so limited they are almost worthless. Idera SharePoint audit builds on top of the base capabilities and extends it significantly.

There are a large number of improvements, but the main ones are as follows:

1. Adds Auditing capabilities to WSS3 and SharePoint foundation. SharePoint's limited auditing facilities are normally only available on MOSS 2007 and SharePoint Server 2010.
2. The Audit data and reports generated by SharePoint's standard functionality are extremely difficult to interpret as data is stored and displayed in a cryptic manner. Idera SharePoint audit interprets SharePoint's audit data and makes it easy to report.
3. SharePoint's audit events are not very complete. In addition to making the standard events easier to interpret, Idera SharePoint audit adds the following (optional) events:
  - a. Tracking views of list items.
  - b. Tracking inserts of items.
  - c. Tracking changes to individual columns (shows old and new values)
  - d. Tracking authentication events such as log-in and log-out.
4. Auditing can be enabled automatically on all new and existing collections using a unique hierarchical administration model.
5. SharePoint audit logs can quickly grow out of control. It is not uncommon for environments that use SharePoint's standard auditing facilities to grow beyond 100 million rows of audit data in a relatively short amount of time. This amount of data cannot be reported by SharePoint as any report just times out. By excluding useless audit events and automatically truncating old data, Idera SharePoint audit logs continue to be usable, even after collecting many years' worth of data.
6. SharePoint's standard log querying facilities are extremely basic and limited. Idera SharePoint audit adds friendly but powerful log querying and reporting screens.
7. Idera SharePoint audit provides an Audit Monitoring facility to report on the state of auditing across all Site Collections in all Web Applications.

## 2 Deployment

Idera SharePoint audit consists of two separate components. A Windows Service, which must be installed on one of the SharePoint servers in your farm, and a WSP file that contains all SharePoint User interface related logic.

The WSP installer will only need to be executed on a single machine, after which it will automatically be distributed to all SharePoint servers in the farm.

### 2.1 Upgrading from Muhimbi SharePoint Audit 2.0

If you choose, you can upgrade from Muhimbi SharePoint Audit 2.0 to Idera SharePoint audit 2.5. If you have an earlier version of Muhimbi SharePoint Audit, you must upgrade to version 2.0 of Muhimbi SharePoint Audit before you can upgrade to Idera SharePoint audit.

When you upgrade, you uninstall your Muhimbi SharePoint Audit deployment using the existing version of the `Uninstall.cmd` file.

You then install Idera SharePoint audit. When you perform the upgrade, your existing audit data is retained. You do not lose any existing audit content when you upgrade to the new version. When you perform the upgrade, you must reconfigure any Muhimbi SharePoint Audit settings. Idera SharePoint audit does not use your existing settings.

After the upgrade process is complete, you must restart the computer that hosts SharePoint audit. Until you restart the computer, SharePoint audit does not collect events.

## 2.2 Installation

*Before deploying the solution, make sure your account has the privileges to deploy SharePoint 'wsp' files. If your systems are configured to use UAC then please make sure all scripts / installers are executed using elevated 'real administrator' privileges.*

*If you are experiencing any problems when accessing the solution from SharePoint then please check out chapter 4.5 Common issues & Errors.*

*Please copy the installation files to a local hard disk before starting the installation process as installation from a UNC path is not supported.*

### 2.2.1 Installing

### 2.2.2 the Windows Service

*The Windows Service that comes with the Idera SharePoint audit should only be installed on a single server in your SharePoint farm. Please do not install it on more than one machine.*

Please carry out the following steps to install the service:

1. Copy the installation archive, as downloaded from the Idera web site, to a local drive and unpack it. Note that installation from a UNC path is not supported.
2. If an older version of the Service is already installed, you must follow the steps in section 2.3 to remove it before you install Idera SharePoint audit 2.5.
3. The service will need to run under a user account with the following privileges. When the software is installed for evaluation purposes then it is recommended to use the developer's or administrator's local account providing it is configured as follows:
  - a. Local Administrator.
  - b. Log on as a Service right.
  - c. Database roles: *db\_ddladmin*, *db\_securityadmin* and *Idera\_Audit\_Admin*. The *Idera\_Audit\_Admin* role is not available until the database has been created in Central Administration. For full details about how to configure the various accounts involved, see *Appendix – Service and Database Accounts*.

You could also consider using your SharePoint Service account for this.

4. Install the Audit Service by launching '*Idera SharePoint Audit\Audit Service Installer\setup.exe*'.
5. Follow the instructions and enter the account defined in step #3 when prompted. For domain accounts please include the domain name. For local accounts use the '.\' prefix, e.g. '.\Administrator')

## 2.2.3 Installing / upgrading the SharePoint Front End

If a copy of the solution is already installed on your SharePoint farm then please un-install it first. For details see 2.3 *Uninstallation*.

To install the software, open the 'Idera SharePoint Audit\SharePoint Installer' directory and run 'install.cmd'<sup>1</sup>

Progress of the installation as well as the outcome of the installation process can be followed via the *Central Administration > Operations > Solution Management* screen (In SharePoint 2010 this screen is located in *Central Administration > System Settings > Manage Farm Solutions*).

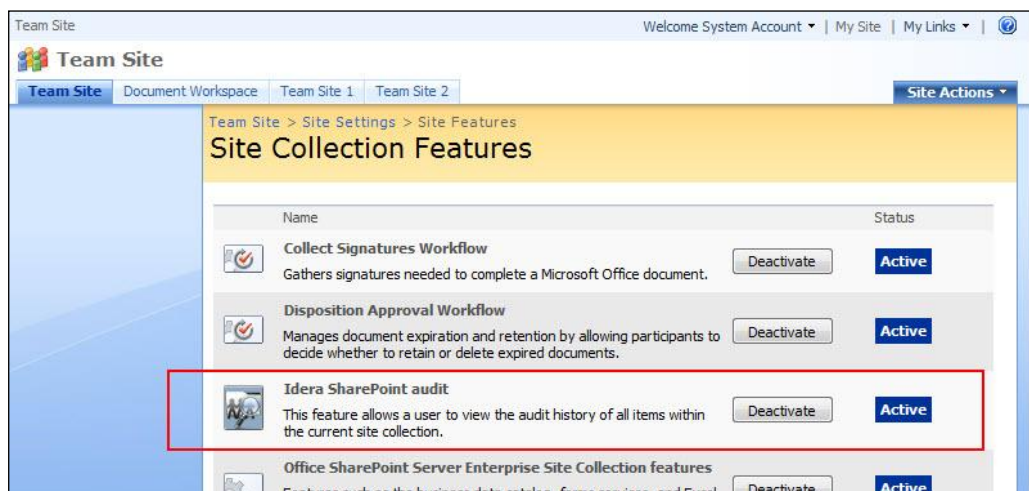
Once the installation has completed successfully the new SharePoint Features are automatically activated. *However, auditing is not automatically enabled to ensure that any existing audit settings are not modified. Proceed to section 3.1 Initial Configuration to setup the database and activate the Audit Log Crawler.*

## 2.2.4 Feature Activation / Deactivation

All audit related SharePoint Features are activated automatically. Under normal circumstances there is no need to manually deactivate any; however you may choose to disable the Audit Viewer from individual site collections. Note that this does not impact the actual auditing, just the Viewer

The Site collection Feature can be disabled as follows:

1. Navigate to the root of the relevant Site Collection.
2. Open the *Site Actions* menu.
3. Click *Site Settings*.
4. In the *Site Collection Administration* section, click *Site Collection Features*.



5. Click the 'Deactivate' button next to the 'Idera SharePoint audit' Feature.

<sup>1</sup> The process is automated and the administrator does not need to interact with stsadm directly. However, if you are an experienced SharePoint administrator then please feel free to make manual modifications to the batch files. Installation using the command line makes use of the standard stsadm command line utility located at: %CommonProgramFiles%\Microsoft Shared\Web Server Extensions\12\BIN (or ..14\BIN in SP2010)

## 2.2.5 Installing the License

When you install Idera SharePoint audit, it includes an evaluation license that lets you report on up to 500 log entries for up to 14 days. In order to run a fully licensed copy of the software without any trial messages and other restrictions, you must enter a license code.

You use the SharePoint Central Admin page to add licenses.

On SharePoint 2007 farms, in the Central Administration page, click *Operations*, then in the Idera SharePoint audit area, click *Licensing*.

On SharePoint 2010 farms, in the Central Administration page, click *General Application Settings*, then in the Idera SharePoint audit area, click *Licensing*.

In the Idera Licensing – Overview page, click *Add License* to add a license code.

## 2.3 Uninstallation

The solution can be un-installed automatically, using a command line batch script, or manually via Central Administration.

*Note that removal of the solution does not change or disable any of the audit settings that may have been specified. Please make any necessary changes to the audit settings, e.g. disable auditing, before removing the solution.*

### 2.3.1 Un-installing the Audit service

After you install Idera SharePoint audit 2.5 or newer, you can uninstall the Audit Service using the standard Windows *Programs and Features* or *Add / Remove Programs* control panel.

### 2.3.2 Un-installing the SharePoint Front End via the command line

To un-install the application, run 'uninstal.cmd'. This retracts the solution and deletes it from the Solution Store.

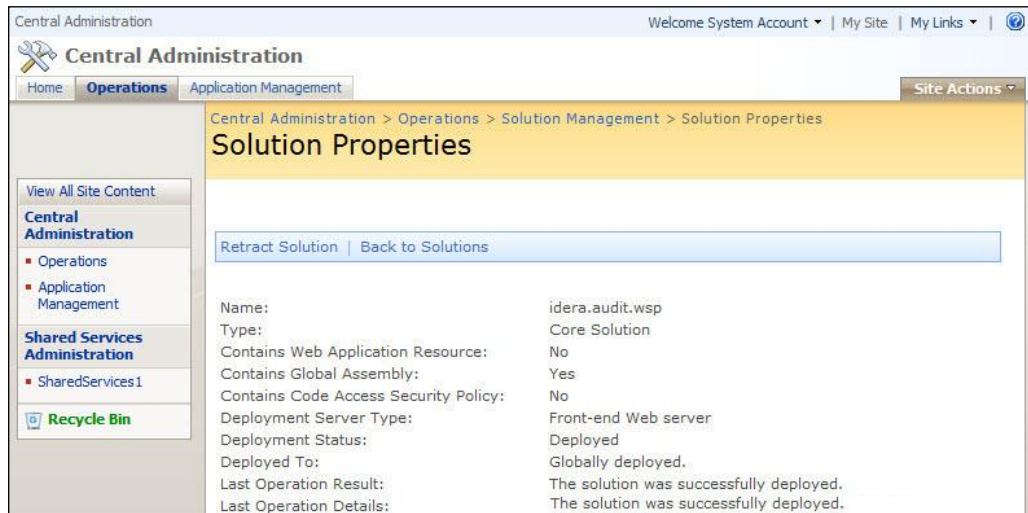
For more fine grained control either use Central Administration (see 2.3.3) to un-install the solution or manually modify the 'uninstall.cmd' script.

Progress of the un-installation as well as the outcome of the process can be followed in the Central Administration page. On the SharePoint 2007 Central Administration page, click *Operations > Solution Management*. On the SharePoint 2010 Central Administration page, click *System Settings > Manage Farm Solutions*.

### 2.3.3 Un-installing the SharePoint Front End via Central Administration

To un-install the solution using the Central Administration web based interface please follow the steps outlined below:

1. In SharePoint 2007, open Central Administration and click *Operations > Solution Management*.  
In SharePoint 2010 open Central Administration and click *System Settings > Manage Farm Solutions*).
2. Click `idera.audit.wsp` to retract the Solution.



3. Click the '*Retract Solution*' button.
4. Accept the default settings and click OK.
5. Depending on the size of the web farm this may take a few minutes. Refresh the '*Solution Management*' page until the status is set to 'Not Deployed'
6. Click on the solution name again, 'idera.audit.wsp'.
7. Click the '*Remove Solution*' button to completely remove it from the farm.

You can use the steps in Chapter 2 *Deployment* to reinstall the solution.

## 3 General Usage

Idera SharePoint audit is very easy to use. It consists of four areas: *Initial Configuration*, *Administering Audit Settings*, *Monitoring the Audit System* and *Viewing the Audit logs*.

### 3.1 Initial Configuration

The very first time the software is installed the Auditing Database must be created and the log crawlers need to be configured.

#### 3.1.1 Creating the database

The Idera SharePoint audit service periodically 'crawls' the SharePoint Audit log, enriches the data to make it useful, and write the details to a custom database.

Before the service can do this, you must create the database. On the SharePoint 2007 Central Administration page, click *Operations*, then in the Idera SharePoint audit area, click *Configure Audit Database*. On the SharePoint 2010 Central Administration page, click *General Application Settings*, then in the Idera SharePoint audit area, click *Configure Audit Database*.

Central Administration v2.5.0.14

Welcome System Account | My Site | My Links

Central Administration

Home Operations Application Management Site Actions

Central Administration > Operations > Audit Database Configuration

**Audit Database Configuration**

Use this page to create a new auditing database or to connect to an existing one.

**Database Name and Authentication**

Use of the default database server and database name is recommended for most cases. Refer to the administrator's guide for advanced scenarios where specifying database information is required.

Use of Windows authentication is strongly recommended. To use SQL authentication, specify the credentials which will be used to connect to the database.

Database Server: KIBON\SQL2K10

Database Name: Idera\_SharePoint\_Audit

Database authentication:

- Windows authentication (recommended)
- SQL authentication

Account:

Password:

OK Cancel

The various fields are self-describing. A default database name is suggested, but you can enter any name. If an existing database name is specified then the tables needed by Idera SharePoint audit are added to that database. If the database does not yet exist then a new database is created.

When using an existing database, make sure that – no matter how unlikely – tables using the following names don't already exist.

- Idera\_CrawlStatus

- Idera\_EnrichedAuditData
- Idera\_Versions
- Idera\_Web

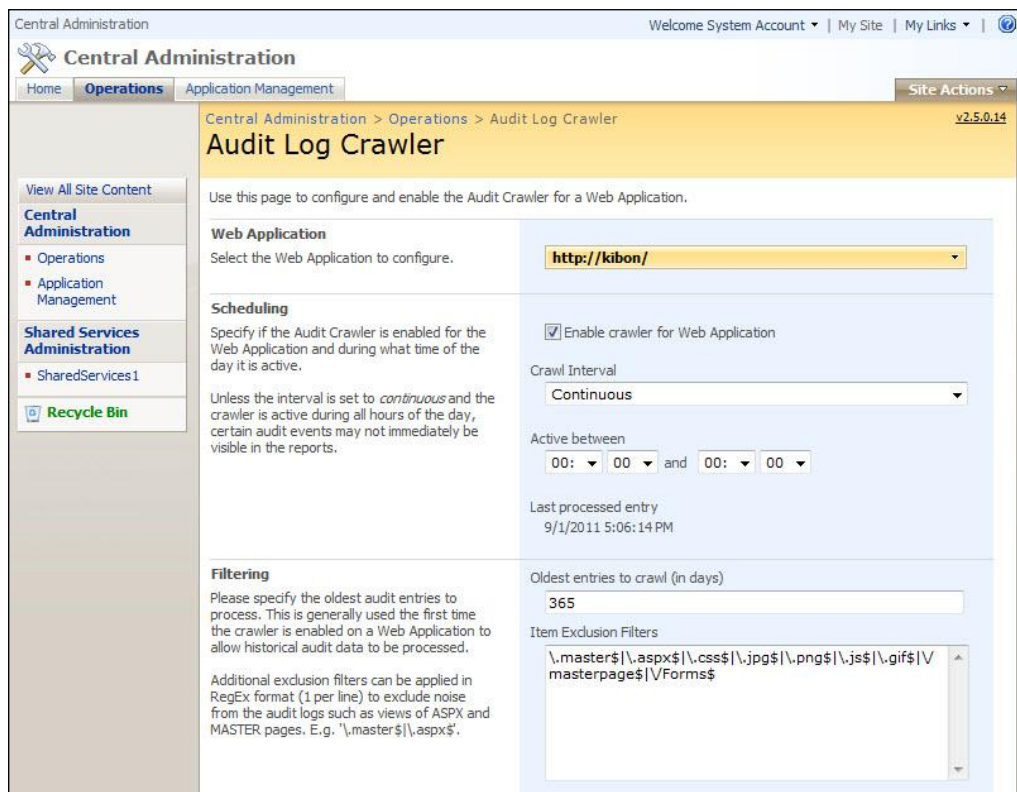
In addition, all stored procedures added by the solution start with the “Idera\_” prefix.

You should add the database to the daily backup cycle. *Do not add the tables to an existing SharePoint Content or Configuration database. Changes to the SharePoint databases can result in your SharePoint databases being unsupported by Microsoft.*

### 3.1.2 Configuring the audit log crawlers

Once the database schema has been created the next step is to configure the Farm Level (and optional Web Application and Site Collection) Audit Settings (See 3.2). The reason for doing this before enabling the Log Crawler is that the Log Crawler needs to know<sup>2</sup> if Authentication events (Log-in / Log-out) need to be generated when importing historical data. *So proceed to section 3.2 and continue with the next paragraph when finished.*

Once Audit Settings have been configured at least one ‘Crawler’ must be enabled. Log crawlers are configured at the Web Application Level and can be enabled or disabled on demand.



The settings are largely self-describing. Details are as follows:

<sup>2</sup> The Log Crawler is responsible for determining the Log-in and Log-out events based on historical Audit Log entries.

1. **Web Application:** Specify the web application for which to configure the crawler.
2. **Enable Crawler:** Only enable the crawler for a web application if you intend to track audit data for it or truncate the audit logs periodically.
3. **Scheduling:** In some heavy duty SharePoint deployments you may want to schedule the crawler to be only active during off-peak hours. The default option of *active between 00:00 and 00:00* means *always active*.
4. **Oldest entries to crawl:** The first time that you install Idera SharePoint audit and it crawls SharePoint's audit logs, there may be a lot existing data in your SharePoint audit logs (100 million records is not uncommon). By default the first crawl imports entries from the last 30 days, but this can be increased to a larger number. As a result the initial crawl may take a while to complete.
5. **Item Exclusion Filters:** SharePoint's standard audit facilities tend to track a lot of data that is of little interest, e.g. requests for simple ASPX pages, master pages or even images and css files. The exclusion filter allows multiple lines of Regular Expressions to be defined for audit items to exclude. The most common unimportant file extensions are configured by default<sup>3</sup>. Feel free to add or remove to the list as this will make it much easier to generate sensible audit reports for your infrastructure.

**Authentication**

SharePoint does not audit login and logout events. Idera SharePoint audit generates these events if Authentication auditing is enabled.

Login events are raised when a user first accesses a Site Collection.

Logout events are raised when a user's last access to a Site Collection is longer than the session timeout specified in this section.

Logout session timeout (in minutes)  
30

**Log Truncating**

Reduce database size and increase performance by automatically deleting old Log Entries for the SharePoint Audit Log as well as Idera's Audit log.

Specify 0 days for the SharePoint Audit Log to remove entries directly after they have been transferred to the Idera Audit Log.

Delete entries from the SharePoint Audit Log:  
 Older than  days  
 Never

Delete entries from the Idera Audit Log:  
 Older than  days  
 Never

**Recrawl Log**

Enable this option to clear the Idera Audit log for this web application and recrawl the SharePoint Audit log, e.g. after changing the Authentication or Filtering options.

Please note that this may take a while depending on the size of the audit log and the value of the *Oldest entries to crawl*.

Any SharePoint audit data deleted as part of the *Log Truncating functionality* will not be recrawled.

Recrawl audit log for this web application.

OK Cancel

6. **Session Timeout:** Idera SharePoint audit allows data to be tracked related to users logging in and out. By default the system assumes that

<sup>3</sup> Note that by excluding *.aspx* and *image* based file extensions Wiki and Picture library audit events may not appear when viewing the audit logs. Amend the existing filter to suit your particular situation.

after 30 minutes of inactivity the user has logged out. This value can be increased or decreased based on your requirements.

7. **SharePoint Audit log truncating:** In high activity environments, or when audit logging is not managed properly, it is not uncommon for the SharePoint Audit table to grow beyond 100 million rows. Fortunately Idera SharePoint audit allows these audit logs to be truncated automatically. When enabled, it keeps 30 days of data by default, but you can set it as high or as low as desired. A value of 0 will remove the data from the SharePoint Audit log directly after it has been processed by the Idera SharePoint audit. However, entries that have been truncated from the SharePoint audit logs cannot be re-crawled. When experimenting with, or evaluating the system you may want to keep this setting disabled.
8. **Idera SharePoint audit log truncating:** When SharePoint's audit entries are processed and enriched by the Idera SharePoint audit service, all data is written to a custom Idera SharePoint audit database table. When audit data is viewed or reported using any of the Idera SharePoint audit screens then data is read from this table. Even though, depending on the filters, this table may contain less data compared to the SharePoint Audit tables, you may want to consider truncating it as well to make it manageable to backup and improve performance. It is recommended to set this value to a sensible amount, when enabled it defaults to keeping data for 1 year.

Please note that it may take up to 30 seconds for any changes to become active.

With the database configured and the crawler enabled you are now ready to query the audit logs.

### 3.1.3 Changing the Audit Service's Config file.

The settings for the Idera SharePoint audit service can be changed by editing the *Idera.SharePoint.Audit.Service.exe.config* file located in the directory where you installed the Audit Service.

Note that the Service must be restarted after making changes to the configuration file. Use the *Windows Services* MMC or the command line to do this:

```
Net stop "Idera SharePoint Audit Service"  
Net start "Idera SharePoint Audit Service"
```

The Idera SharePoint audit service uses the industry standard *log4net* framework to write logging and trace data to a log file. Out-of-the-box, information is logged to the *IderaAudit.log* file stored in the directory the Audit service has been installed in. A new file is created for each day and the default logging level is set to 'INFO'.

Warnings and Errors are also written to the Windows Event Log.

You may want to consider changing the following settings:

- **Log file location:** change the path of the log file name in the *appender* element to a location of your preference.
- **Log Level:** By default only 'INFO' and critical information such as warnings and errors are logged. To get a better view of what the service is

doing, e.g. during a troubleshooting session, you may want to consider switching the <root> log level to 'DEBUG' mode.

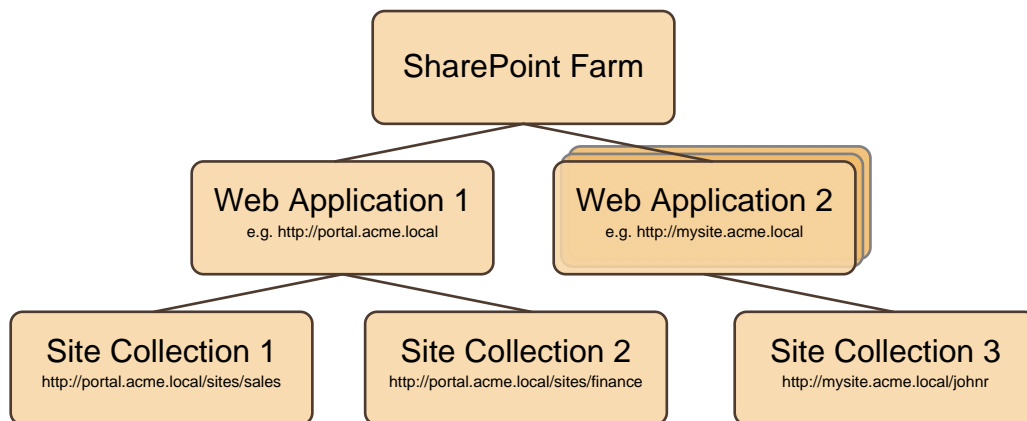
- **Verbose Logging:** For troubleshooting purposes *Verbose Logging* can be enabled by setting the *verboseLogging* config value to *true* AND setting the *Log Level* to *Debug*. This will log an extremely detailed level of information to the log file. Do not leave this option enabled when it is not needed as it will quickly fill up your disk space with rapidly growing log files.

More information can be found at <http://logging.apache.org/log4net/index.html>.

## 3.2 Administering audit settings

Idera SharePoint audit uses a unique hierarchical model to specify Audit Settings at the Farm, Web Application or Site Collection level. Administrators can specify settings at one level and define if any of the underlying levels are allowed to override these settings.

The hierarchical model matches SharePoint's.



Before we review the system in more detail, consider some examples of the flexibility this model allows:

1. **Only allow settings to be specified for the entire farm at the Farm level.** This can be achieved by configuring the desired settings at the Farm level and disabling 'Enable overriding of audit settings'.
2. **Specify different audit settings for Web Application 2 (for example, MySites).** This can be achieved as follows:
  - a. Specify the most common settings at the Farm level and enable 'Enable overriding of audit settings'.
  - b. At the Web Application level, select *Web Application 2* and disable *Inherit all settings from the Web Farm*.
  - c. Change the settings to whatever is applicable for this Web Application.Note that *Web Application 1* is still inheriting its settings from the Farm Level.
3. **Enable extra comprehensive auditing on the 'Finance' site collection.** To keep the level of Audit data manageable you may take the decision to only audit 'Views' at the Farm level and enable more comprehensive

auditing on sensitive site collections such as the *Finance* site. This can be achieved as follows:

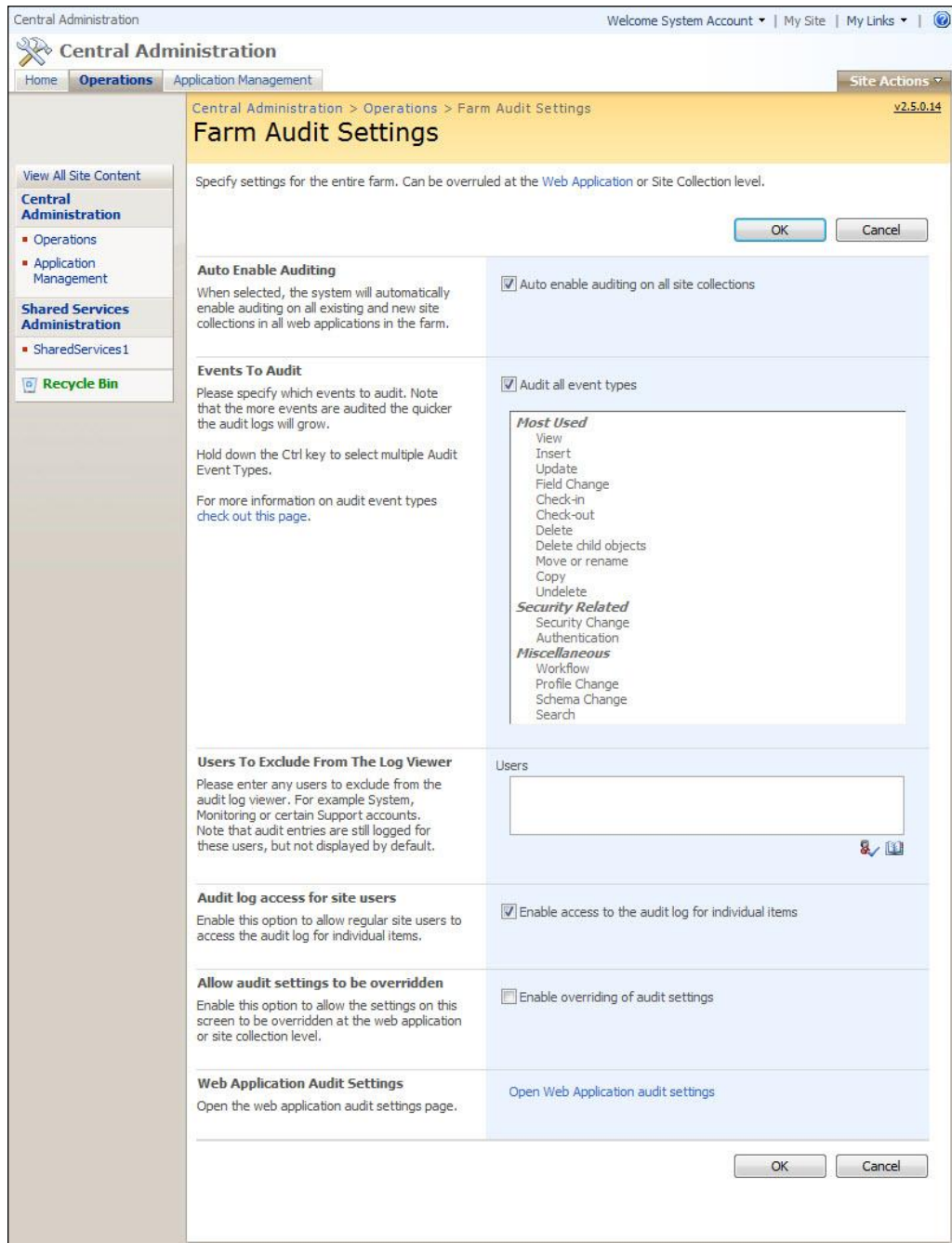
- a. Specify the 'View' audit event at the Farm level and enable '*Enable overriding of audit settings*'.
- b. On the *Finance* site, disable *Inherit all settings from the Web Application* and select the *Audit all event types* option.

### 3.2.1 Farm Level settings

At the top of the hierarchical model sits the SharePoint Farm. The audit settings for this level can be accessed from the Central Administration page. On the SharePoint 2007 Central Administration page, click *Operations*, then in the Idera SharePoint audit area, click *Farm level audit settings*. On the SharePoint 2010 Central Administration page, click *General Application Settings*, then in the Idera SharePoint audit area, click *Farm level audit settings*.

The farm level settings can only be modified by Farm Administrators. The following settings can be configured:

1. **Auto Enable Auditing:** When selected, the system will automatically enable auditing on all existing and new site collections in all web applications that have been configured to inherit the settings from the Farm level.
2. **Events To Audit:** Use this section to specify which events to audit. Please note that the more event types are being audited, the faster the logs will grow. It is therefore strongly advised to just keep with the basic event types such as View, Update and Delete and enable more comprehensive auditing on those site collections that require it.
3. **Users To Exclude From The Log Viewer:** Any users to exclude from the results displayed in the audit log viewer can be entered in this area. For example *System*, *Search Crawl*, *Monitoring* or certain *Support* accounts. Note that audit entries are still logged for these users and can be viewed by explicitly entering these names in the Audit log viewer.
4. **Allow site users to access audit log for individual items:** Under normal circumstances the Audit logs can only be viewed by Site Collection Administrators. However, you may want to allow all users to view the Audit log on individual items.



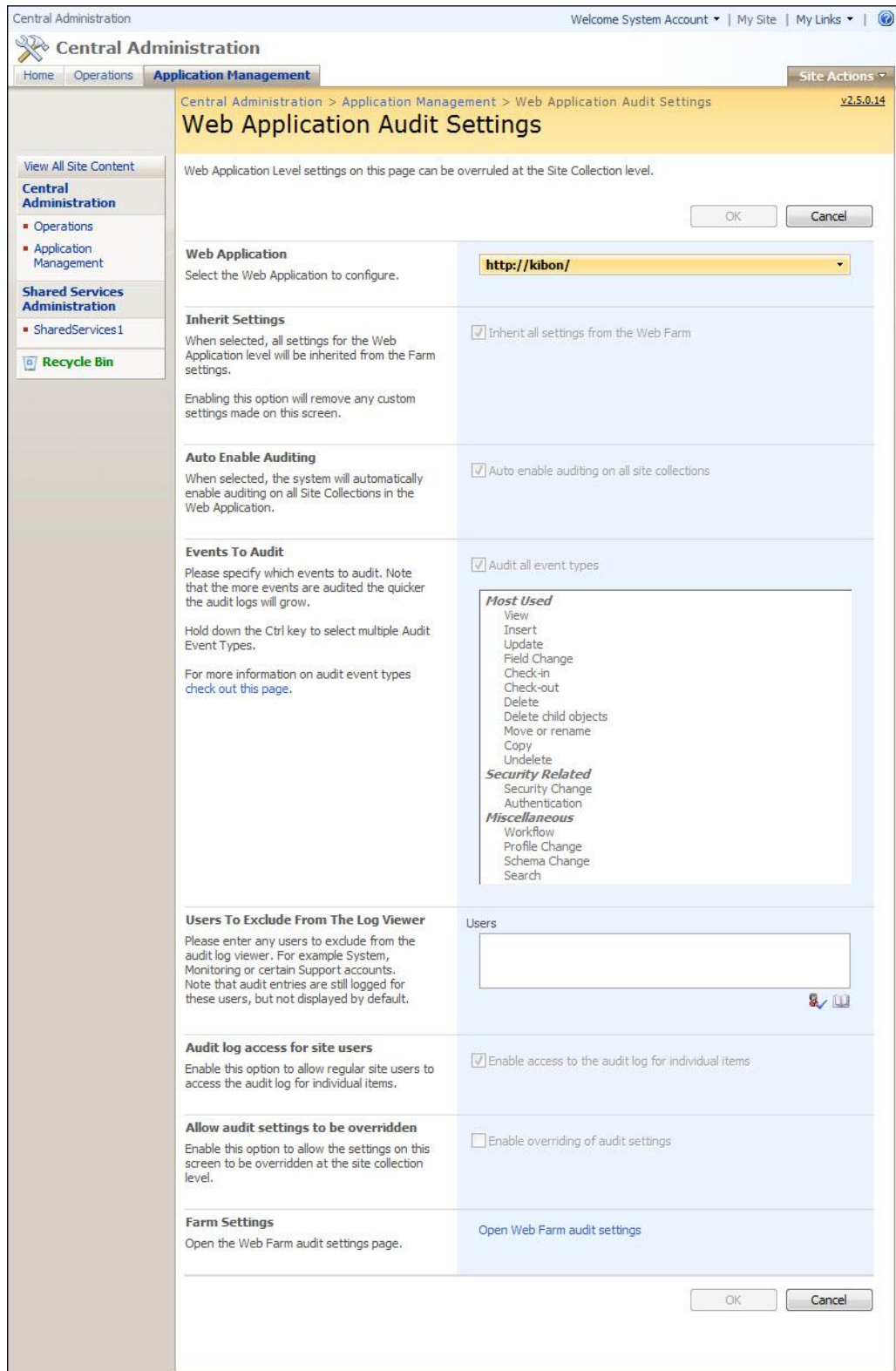
5. **Allow audit settings to be overridden:** By default all Web Applications and Site Collections inherit their settings from the Farm level. Enable this option to allow the settings to be overridden at the Web Application level.

**Caution: Changing the Farm level settings will impact any Web Application and Site collection that inherits settings from the farm.**

## 3.2.2 Web Application Level settings

Each Farm contains one or more Web Applications. If you enable override of settings at the Farm level, you can access the settings for the Web Application on the Central Administration page. On the SharePoint 2007 Central Administration page, click *Operations*, then in the Idera SharePoint audit area, click *Web Application audit settings*. On the SharePoint 2010 Central Administration page, click *General Application Settings*, then in the Idera SharePoint audit area, click *Web Application audit settings*.

The Web Application level settings can only be modified by Farm Administrators.



Most settings are similar to the Farm Level Settings outlined in section 3.2.1 and won't be repeated here. The settings specific to this screen are as follows:

1. **Web Application:** Select the Web Application for which to specify the settings.

2. **Inherit settings:** When selected, all settings for the Web Application level will be inherited from the Farm settings.

**Caution: Changing the Web Application level settings will impact any Site collection that inherits settings from the Web Application.**

### 3.2.3 Site collection Level settings

Each Web Application contains one or more Site collections. If you enable setting override at the Web Application level, settings for the Site Collection can be accessed on the Site Actions menu. Click *Site Actions* > *Site Settings*, then in the Idera SharePoint audit area, click *Site collection audit settings*.

The Site collection level settings can be accessed by Farm Administrators as well as Site Collection Administrators<sup>4</sup>. The settings are similar to the Farm Level Settings outlined in section 3.2.1 and won't be repeated here.

Team Site > Site Settings > Site Collection Audit Settings v2.5.0.14

**Site Collection Audit Settings**

Specify audit settings for the entire Site Collection.

OK Cancel

**Inherit Settings**  
When selected, all settings for the Site Collection level will be inherited from the Web Application settings.  
Enabling this option will remove any custom settings made on this screen.

Inherit all settings from the Web Application

**Events To Audit**  
Please specify which events to audit. Note that the more events are audited the quicker the audit logs will grow.  
Hold down the Ctrl key to select multiple Audit Event Types.  
For more information on audit event types check out this page.

Audit all event types

**Most Used**  
View  
Insert  
Update  
Field Change  
Check-in  
Check-out  
Delete  
Delete child objects  
Move or rename  
Copy  
Undelete  
**Security Related**  
Security Change  
Authentication  
**Miscellaneous**  
Workflow

**Users To Exclude From The Log Viewer**  
Please enter any users to exclude from the audit log viewer. For example System, Monitoring or certain Support accounts. Note that audit entries are still logged for these users, but not displayed by default.

Users

**Audit log access for site users**  
Enable this option to allow regular site users to access the audit log for individual items.

Enable access to the audit log for individual items

OK Cancel

<sup>4</sup> Note that Site Collection Administrators are specified in Central Administration > Application Management > SharePoint Site Management > Site collection administrators.

### 3.3 Monitoring the audit system

To get an overview on what kind of auditing is enabled on each site collection, open the Audit Monitor from the Central Administration page. On the SharePoint 2007 Central Administration page, click *Operations*, then in the Idera SharePoint audit area, click *Audit Monitoring*. On the SharePoint 2010 Central Administration page, click *General Application Settings*, then in the Idera SharePoint audit area, click *Audit Monitoring*.

Site Name ↑	Web Application	Site Collection	Description
⚠ Central Administration	http://kbon:7134	/	Warning: The following audit types are disabled: CheckOut, CheckIn, View, Delete, Update, ProfileChange, ChildDelete, SchemaChange, SecurityChange, Undelete, Workflow, Copy, Move, Search, All
🟢 My Site	http://kbon	/mysites	OK: All Enabled
🟢 Shared Services Administration: SharedServices1	http://kbon	/ssp/admin	OK: All Enabled
🟢 Team Site	http://kbon	/	OK: All Enabled
🟢 Team Site	http://kbon:8080	/	OK: All Enabled
🟢 Team Site	http://kbon:9090	/	OK: All Enabled

The Audit Monitor has the ability to return the status in XML format to allow system management software such as *Microsoft's Operations Manager*, *SiteScope*, *OpenView* or *Tivoli* to automatically monitor the state of auditing in a SharePoint farm.

To request the status in XML format, add the following parameters to the Audit Monitor's URL:

1. WebApp: The URL, including port number, of the Web Application to return the audit status for. If this parameter is not specified then the status of all Web Applications will be returned.
2. Status: The Status to filter for, choose from:
  - a. All: Return all Statuses.
  - b. AllEnabled: Return all site collections with all Audit options enabled.
  - c. PartialEnabled: Return all site collections with some auditing enabled
  - d. NoneEnabled: Return all site collections that have no auditing enabled.

The following request will return the status for all site collections in the portal.idera.local (on port 82) web application:

`http://<YourCAServer>/_layouts/Idera.SharePointAudit.Farm/AuditMonitor.aspx?WebApp=http://portal.idera.local:82&status=All`

This returns the following XML, which can subsequently be processed by the system management software.

```
<?xml version="1.0" encoding="utf-8" ?>
<AuditMonitorEntries>
  <AuditMonitor>
    <Status>Ok</Status>
    <SiteName>Root</SiteName>
    <WebApplication>http://portal.idera.local:82</WebApplication>
    <SiteCollection>/</SiteCollection>
    <Description>OK: All Enabled</Description>
  </AuditMonitor>
  <AuditMonitor>
    <Status>Ok</Status>
    <SiteName>Test</SiteName>
    <WebApplication>http://portal.idera.local:82</WebApplication>
    <SiteCollection>/sites/test</SiteCollection>
    <Description>OK: All Enabled</Description>
  </AuditMonitor>
</AuditMonitorEntries>
```

## 3.4 Viewing audit logs

One of the key features of Idera SharePoint audit is the ability to query the contents of the audit log using a user friendly interface.

The Log viewer is context sensitive and can be accessed from the *Central Administration* website, any *Site Collection's Site Settings* screen, a *List* or *Document Library's Action menu* or a *list item's context menu*.

### 3.4.1 Web Application Level

The *highest level* log viewer can be opened from the Central Administration page. On the SharePoint 2007 Central Administration page, click *Operations*, then in the Idera SharePoint audit area, click *View Web application audit logs*. On the SharePoint 2010 Central Administration page, click *General Application Settings*, then in the Idera SharePoint audit area, click *View Web application audit logs*. The functionality is described in detail below.

Central Administration > Application Management > Audit Log Viewer v2.5.0.14

## Audit Log Viewer

Query the audit log. Unfiltered queries may take some time to complete.

**Site Collection**  
Specify the Site Collection to view the audit entries for.

**Filter Results**  
Optionally specify criteria to filter the list of audit entries for.  
Note that when no filter is specified, requesting the list of Audit Entries may take a long time.  
The *Grouping* option comes into effect when exporting the data to Excel.

**Audit Events**  
Optionally specify which Audit Event Types to return.  
Hold down the Ctrl key to select multiple Audit Event Types.  
For more information on audit event types check out this page.

Sub Sites: This site and all sub sites

List and Libraries: All Lists and Libraries

User: [Text Box]

Item Types: All Item Types

Start Date: 8/6/2011 00:00

End Date: [Text Box] 00:00

Page Size: 100 Entries per page

Sorting / Grouping: Date

Show all event types

**Most Used**


- View
- Insert
- Update
- Field Change
- Check-in
- Check-out
- Delete
- Delete child objects
- Move or rename
- Child move or rename
- Copy
- Undelete
- Audit related**
- Changes to audit settings







1. **Site Collection:** Select any Web Application / Site Collection combination to view the logs for.
2. **Filter Results:** Specify a combination of filters to narrow the results down to. The following filters are available:
  - a. Sub sites: By default all sites and sub sites in a site collection are queried. Use this dropdown menu to narrow down the results to a specific site.
  - b. List and Libraries: Providing a specific site is selected, a specific list can be selected to narrow the results down to.
  - c. User: Specify any number of users to narrow the results down to. Note that entering the name of an 'excluded user' (See below) will return the entries for this user.
  - d. Item Types: Specify which item types to return. E.g. Document, List Item, List etc.

- e. **Start and End Date:** Specify a date range to narrow the results down to. Note that by default the start date is set to 1 month ago in order to limit the number of audit entries returned by the system.
- f. **Sorting / Grouping:** Specify how to sort and group the results. Note that *grouping* is only visualised when exporting data to Excel
3. **Audit Events:** Specify which Event Types to return. Select a single, multiple or all event types.
4. **Users to Exclude:** When configured, any users that are excluded by default from the search results are displayed in this area. For details on how to configure this see section 3.2.1 *Farm Level settings*.
5. **View Results:** Click this button to display the search results in the web browser as displayed below.

Central Administration > Application Management > Audit Log Viewer v2.5.0.14

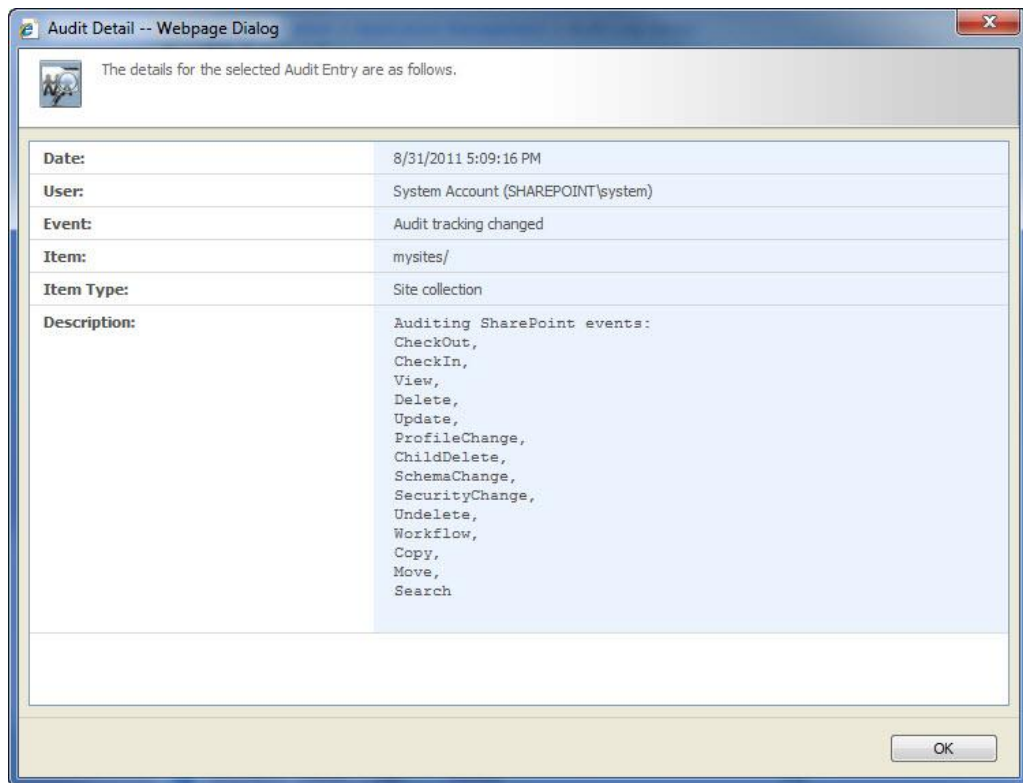
## Audit Log Viewer

 Export Audit entries to Excel

	Date ↓	User	Event	Item	Item Type	Description
	9/6/2011 3:22:44 PM	System Account	View	mysites/	Web	"Displayed by Idera A Monitor"
	9/6/2011 3:22:43 PM	System Account	Login	mysites/	Site collection	
	8/31/2011 5:19:31 PM	System Account	Logout	mysites/	Site collection	
	8/31/2011 5:19:30 PM	System Account	View	mysites/	Web	"Displayed by Idera A Monitor"
	8/31/2011 5:09:16 PM	System Account	Audit tracking changed	mysites/	Web	Auditing Idera events: Authentication, FieldChange, Insert
	8/31/2011 5:09:16 PM	System Account	Audit tracking changed	mysites/	Site collection	Auditing SharePoint events: CheckOut, CheckIn, View, Delet Update, ProfileChang ChildDelete, SchemaChange, SecurityChange, Undelete, Workflow, Copy, Move, Search

6. **Export Audit entries to Excel:** Once the search results are displayed in the browser, click this button to export the results to Excel.

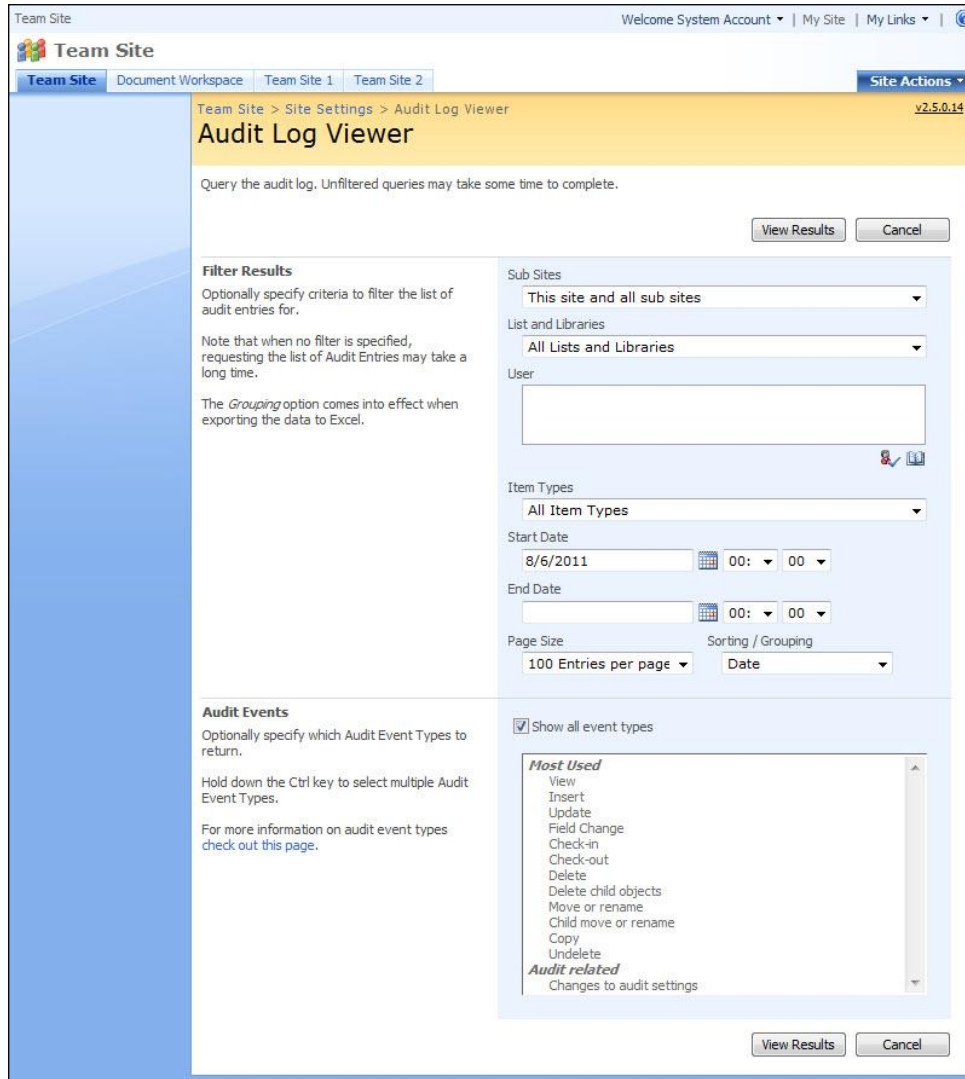
Click the blue button at the beginning of each line to display more details.



*Warning, querying large audit logs without specifying any search filters may take longer than expected. In order to keep the system responsive only the last 5000 entries that match the search criteria are returned. The trial version is limited to 500 entries.*

## 3.4.2 Site collection Level

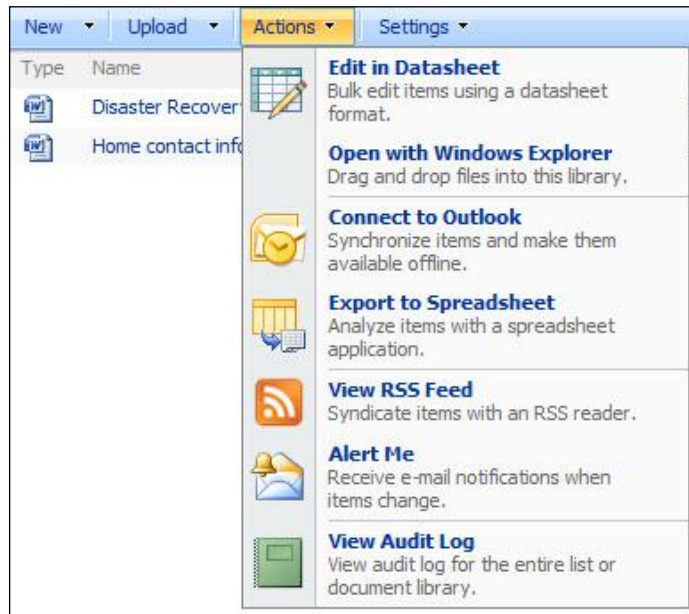
Site Collection Administrators can view the audit logs in the Site Settings page. To view the logs, click *Site Actions > Site Settings*, then in the Idera SharePoint audit area, click *View audit logs for this site*.



Its functionality is identical to the Web Application Audit Log Viewer described in 3.4.1 with the exception that it is not possible to switch between Site Collections.

## 3.4.3 List Level

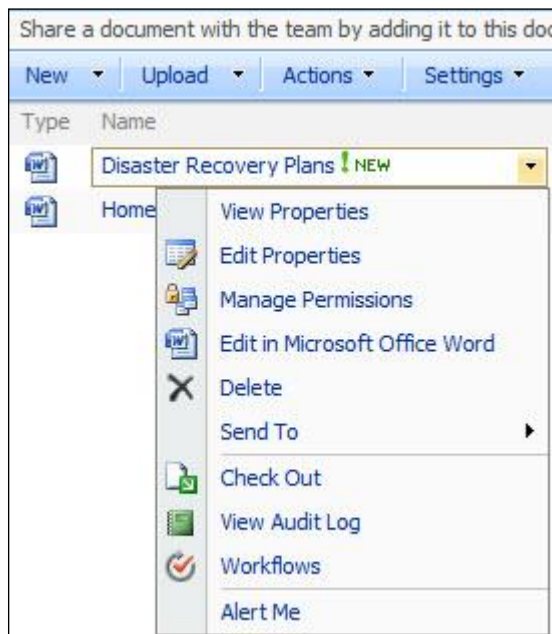
Site Collection Administrators and list owners can query the Audit Log for a list or library directly from the Actions menu as displayed below.



The log viewer is identical to the Web Application Audit Log Viewer described in 3.4.1 with the exception that it is not possible to switch to other Site Collections or lists.

### 3.4.4 Folder and Item level

Site Collection Administrators, list owners and - if configured - regular site users can query the Audit Log for an individual document or list item using the 'View Audit Log' option in the item's context menu.



The log viewer automatically displays all relevant audit entries without needing to manually specify any search criteria.

## 3.5 Running Reports

### 3.5.1 Exporting Audit data to Excel

Idera SharePoint audit allows audit data to be exported to Excel spreadsheets for further processing using Excel's built-in *pivot* and *filtering* functionality.

To generate an Excel report, view the audit data as described in section 3.4 and then click the *Export Audit entries to Excel* link. The results can be grouped by different columns using the *Sorting / Grouping* option on the Audit Log Query screen.

The following grouping options are available:

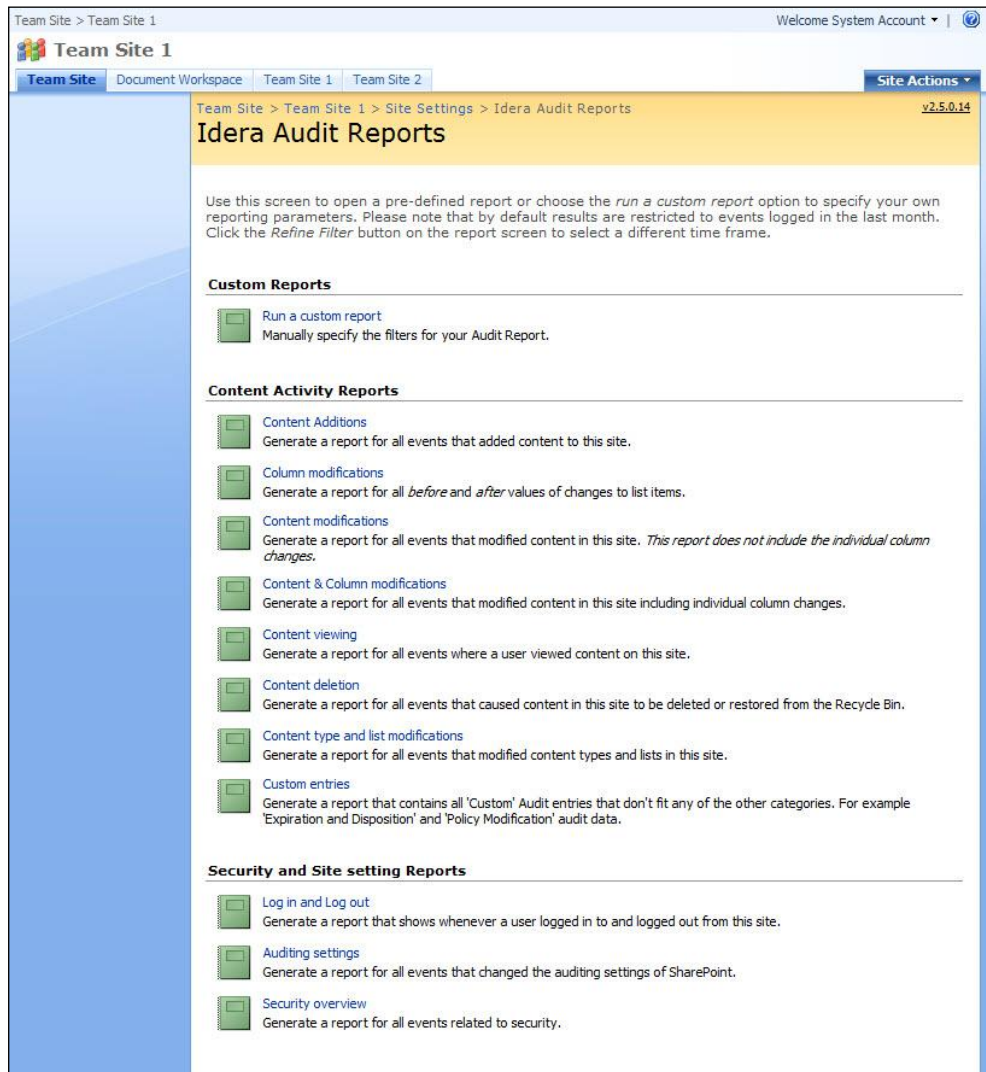
- by site
- by site / user
- by site / date
- by user
- by user / site
- by user / date
- by date
- by date / user
- by date / site

SharePoint Audit Log Extract					
Exported by:		System Account			
Exported on:		9/7/2011 9:40:27 AM			
Site collection:		http://kibon/mysites			
Row Labels	User	Event	Item	Item Type	Description
<b>06 Sep 2011</b>					
15:41:27	System Account	View	mysites/	Web	Site collection audit log viewed
15:22:44	System Account	View	mysites/	Web	"Displayed by Idera Audit Monitor"
15:22:43	System Account	Login	mysites/	Site collection	
<b>31 Aug 2011</b>					
17:19:31	System Account	Logout	mysites/	Site collection	
17:19:30	System Account	View	mysites/	Web	"Displayed by Idera Audit Monitor"
17:09:16	System Account	Audit tracking changed	mysites/	Web	Auditing Idera events: Authentication, FieldChange, Insert System Account (SHAREPOINT\system)
				Site collection	Auditing SharePoint events: CheckOut, Checkin, View, Delete, Update, ProfileChange, ChildDelete, SchemaChange, SecurityChange, Undelete, Workflow, Copy, Move, Search
17:09:15	System Account	Login	mysites/	Site collection	
<b>29 Aug 2011</b>					
13:06:03	System Account	Logout	mysites/	Site collection	
13:06:02	System Account	View	mysites/	Web	"Displayed by Idera Audit Monitor"
12:58:46	System Account	Update	mysites/_catalogs/wp	List	TopAnswer.webpart
			mysites/_catalogs/wp/TopAnswer.webpart	Document	
			mysites/_catalogs/wp/SummaryResults.webpart	Document	
			mysites/_catalogs/wp/TopAnswer.webpart	Document	
		Insert	mysites/_catalogs/wp/TopAnswer.webpart	Document	Title changed from "" to "Top Federated Results"
		Field Change	mysites/_catalogs/wp/TopAnswer.webpart	Document	Group changed from "" to "Search"

Sample Report, Grouped by Date / User

## 3.5.2 Running predefined reports

Although the audit log filtering screen described in section 3.4 is very powerful, there is an easier option available for the casual user who just needs to run simple reports from time to time, the *Idera Audit Reports* screen. Site Collection Administrators can run the predefined reports. Click *Site Actions > Site Settings*, then click *Run Audit Reports*.



The following predefined reports are available:

- **Run a custom report:** Manually specify the filters for your Audit Report.
- **Content Additions:** Shows all events that added content to the site.
- **Column modifications:** Generate a report for all *before* and *after* values of changes to list items.
- **Content modifications:** Generate a report for all events that modified content in the site. This report does not include the individual column changes.
- **Content & Column modifications:** Generate a report for all events that modified content in the site including individual column changes.

- **Content viewing:** Shows all events where a user viewed content.
- **Content deletion:** Generate a report for all events that caused content in the site to be deleted or restored from the Recycle Bin.
- **Content type and list modifications:** Generate a report for all events that modified content types and lists in the site.
- **Custom entries:** Generate a report that contains all 'Custom' Audit entries that don't fit any of the other categories. For example '*Expiration and Disposition*' and '*Policy Modification*' audit data.
- **Log in and Log out:** Generate a report that shows whenever a user logged in to and logged out from the site.
- **Auditing settings:** Generate a report for all events that changed the auditing settings of SharePoint.
- **Security settings:** Generate a report for all events that changed the security configuration of SharePoint.

Note that all reports include entries for the last 30 days only. To see more data click the *Refine Filter* button.

### 3.5.3 Creating custom reports

The *Predefined Reports* screen described in 3.5.2 passes the parameters needed for the report using the *query string*. This makes it very simple to create your own custom reports and store them as URLs in a standard SharePoint list of hyperlinks.

For example:

- **Content & Column modifications:**

```
http://<path_to_your_site_collection>/_layouts/Idera.SharePointAudit.Site/AuditLogViewer.aspx?RequestFrom=sitecollection&action=Results&eventTypes=Update;Delete;ChildDelete;CheckOut;CheckIn;Undelete;Copy;Move;ChildMove;FieldChange&sortOrder=Date:Desc&subsiteFilter=All&listsFilter=All&userFilter=siteItemType=All&startDateFilter=30&endDateFilter=&pageSize=100
```

- **Login & Logout events:**

```
http://<path_to_your_site_collection>/_layouts/Idera.SharePointAudit.Site/AuditLogViewer.aspx?RequestFrom=sitecollection&action=Results&eventTypes=Authentication&sortOrder=Date:Desc-User:Asc&subsiteFilter=All&listsFilter=All&userFilter=&itemType=All&startDateFilter=30&endDateFilter=&pageSize=100
```

The parameters match those defined in the Query section of the *Audit Log Viewer* describer in 3.4, and are largely self describing. Listed below are the parameter names and the values accepted by each parameter.

- **eventTypes:** The *audit event types* to include in the results. Use *All* to include all audit entries or one or more of the types defined below in a ‘;’ delimited list.
  - **Most Used:** View, Insert, Update, FieldChange , CheckIn, CheckOut, Delete, ChildDelete , Move, ChildMove, Copy, Undelete
  - **Audit Related:** AuditMaskChange, EventsDeleted
  - **Security Related:** Authentication, SecGroupCreate, SecGroupDelete, SecGroupMemberAdd, SecGroupMemberDel,

SecRoleBindInherit, SecRoleBindBreakInherit,  
SecRoleBindUpdate, SecRoleDefModify, SecRoleDefDelete,  
SecRoleDefCreate, SecRoleDefBreakInherit

- **Miscellaneous:** Workflow, ProfileChange, SchemaChange, Search, Custom
- **sortOrder:** The order by which to sort and group the results. The following options are supported, note that the *Desc* and *Asc* values can be modified:
  - *Date:Desc*
  - *Date:Desc-User:Asc*
  - *Date:Desc-Site:Asc*
  - *User:Asc*
  - *User:Asc-Site:Asc*
  - *User:Asc-Date:Desc*
  - *Site:Asc*
  - *Site:Asc-User:Asc*
  - *Site:Asc-Date:Desc*
- **subSiteFilter:** Either *All* or the unique ID of a specific subsite to filter for.
- **listFilter:** Either *All* or the unique ID of a specific list to filter for.
- **userFilter:** A ',' separated list of user accounts to include in the results.
- **itemType:** Either *All* or the name of the item type to filter for: *Document*, *Folder*, *List*, *ListItem*, *Site* or *Web*.
- **startDateFilter:** The number of days, relative to the current date, to use as the start date. E.g. '30' means 30 days ago.
- **endDateFilter:** The number of days, relative to the current date, to use as the end date. E.g. '30' means 30 days ago.
- **pageSize:** The number of audit entries to display on each page.
- **source:** The URL to return to when the *Cancel* button is clicked.

## 4 Troubleshooting & Other common tasks

If you still have questions after reading this chapter then please check out the links in chapter 1 *Introduction*.

### 4.1 Windows Event Log

Unless you have decided to disable certain logging levels in *Central Administration > Operations > Logging and Reporting > Diagnostic logging*, (*Monitoring > Configure Diagnostic Logging* in SP 2010) the following entries may be written to the event log:

1. **Warnings:** If you are running an evaluation copy of the software, or your license has expired then this is reported as a warning message in the Application Event Log.
2. **Errors:** Although the software attempts to catch any error and present the user with a friendly message, the actual errors are still written to the event log.

On SharePoint 2007 farms, all event entries that Idera SharePoint audit write use the *Windows SharePoint Services 3* event source. On SharePoint 2010, farms, all event entries use the *SharePoint Foundation* event source. You can filter the events by the Event ID, which is always 41735.

### 4.2 SharePoint Trace Log

Unless you have decided to disable certain logging levels in the Central Administration page, these entries may be included in the SharePoint trace log.

To configure logging, on the SharePoint 2007 Central Administration page, click *Operations*, then in the Logging and Reporting area, click *Diagnostic logging*. On the SharePoint 2010 Central Administration page, click *Monitoring*, then in the Reporting area, click *Configure diagnostic logging*. All Warnings and errors that are written to the Windows Event Log are also written to the SharePoint Trace log.

1. An entry is written whenever the software is installed, uninstalled, activated or deactivated.

Note that the location of the log files is defined in the *Diagnostic Logging* screen in Central Administration.

### 4.3 SharePoint audit log

Providing SharePoint Auditing is enabled, the following audit entries are written to the log by Idera SharePoint audit:

1. A 'View' event against the item being viewed (List, Document, site etc) every time the audit log is viewed.
2. A 'View' event against the site collection every time it's Audit Status is queried via the Audit Monitor.

## 4.4 Audit Service trace log

The Audit Service maintains a detailed trace log named *IderaSharePointaudit.log* in the directory the service has been installed in. For details about changing settings for this trace log see section 3.1.3.

## 4.5 Common issues & Errors

### 4.5.1 Your account is not allowed to deploy SharePoint Solutions

Before attempting to deploy the solution, please make sure your account is a Farm Administrator and your account has *db\_owner* rights on the Admin content database. This is a common requirement for being able to deploy SharePoint Solutions and is not specific to Idera SharePoint audit.

### 4.5.2 Authentication information is not being logged or not correctly

Idera SharePoint audit adds the ability to track login and logout events. As SharePoint provides no support for these events, the Idera SharePoint audit service determines this information based on users' activity found in SharePoint's own audit logs.

This generally works very well, but there are a few things that need to be taken into account.

1. The *Authentication* audit event needs to be enabled.
2. As this information is determined based on other auditing activity, the *View* audit event should be enabled at a minimum. If there is no audit data found then the system cannot work out if a user has logged in or out.
3. You may want to consider tracking additional audit event types such as *View*, *Update*, *Delete*, *Move*, *Insert*, *Check-In*, *Check-Out* and *Copy* to improve the precision of the Authentication events. For example, if someone is editing an MS-Word file for a long time then *View* events are not recorded, but *Update* events are.

### 4.5.3 Errors on newly added servers

The software may not work on any new servers that have been added to the SharePoint farm after the initial deployment of SharePoint Audit.

This is a known issue with SharePoint. For details see section 4.5.5.

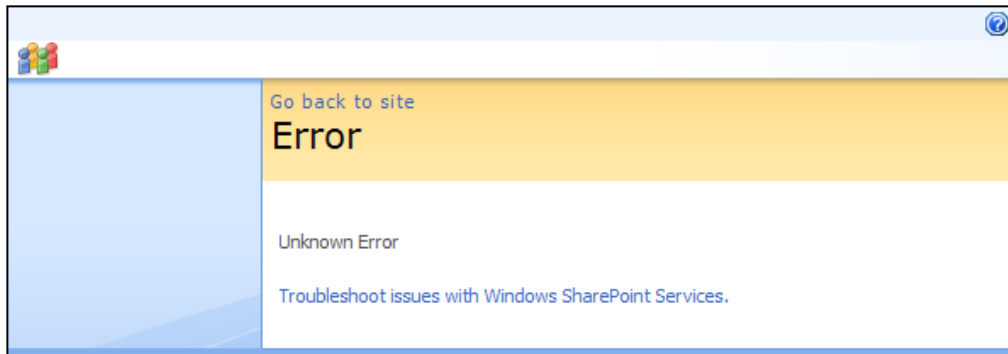
### 4.5.4 An evaluation message is displayed in the User Interface

If an *evaluation* message appears on each screen, something may be wrong with your license. This may be caused by:

1. No license is present at all. Contact Idera for information about purchasing a license at [www.idera.com](http://www.idera.com)
2. Your support license has expired and you have installed a copy of the software that was released after the support license expiration date.
3. Your license has expired.

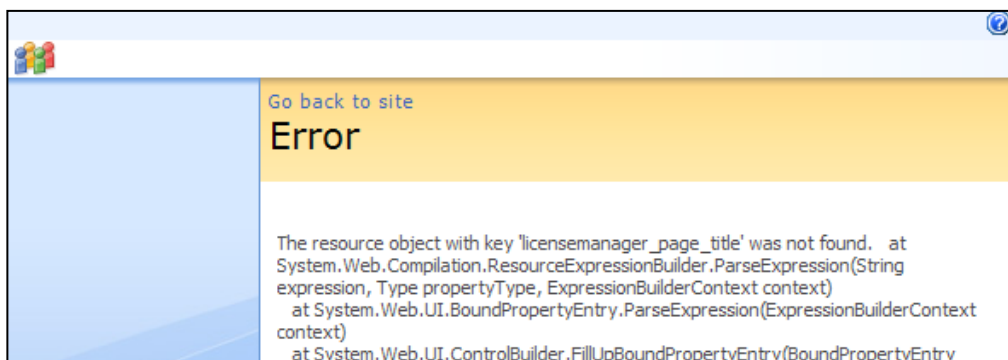
## 4.5.5 'Unknown Error' or 'resource object not found'

If the error message 'Unknown Error' or the equivalent in your local language appears, then there may have been a problem with the distribution of your language specific resource files.



This error is not logged to the event log as this is a SharePoint error, which is triggered before our software is started. To get more detail about the error, temporarily change the *CallStack* attribute in the *SafeMode* element in the web.config to *True*.

If a message similar to the following is displayed after refreshing the page then you need to force SharePoint to redistribute the resource files.



This can be done by issuing the following command<sup>5</sup> on each server exhibiting the problem:

```
stsadm -o copyappbincontent
```

In some cases running the command mentioned previously does not resolve the problem. As a last resort copy the resource files manually on all Web Front End Servers from one of the following:

Platform	Source	Destination
SharePoint 2007	C:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\12\CONFIG\Resources\IdersAuditSharedResources.*	C:\inetpub\wwwroot\wss\VirtualDirectories\<webapplication>\App_GlobalResources
SharePoint 2010	C:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\14\CONFIG\Resources\IdersAuditSharedResources.*	C:\inetpub\wwwroot\wss\VirtualDirectories\<webapplication>\App_GlobalResources

<sup>5</sup> STSADM is located at %CommonProgramFiles%\Microsoft Shared\Web Server Extensions\12\BIN on SharePoint 2007 servers and at %CommonProgramFiles%\Microsoft Shared\Web Server Extensions 14\BIN on SharePoint 2010 servers.

It is not clear why a small number of SharePoint deployments refuse to copy the resource files. We are investigating the matter further.

### 4.5.6 Viewing audit logs is slow

Although we have made every possible effort to make the audit viewer as fast and responsive as possible, if you are logging an unusual amount of Audit data then you may want to consider the following:

1. **Specify a more detailed search filter.** Narrowing the results down by date and list will improve the query time significantly.
2. **Only log the audit data you are interested in.** When you are not interested in each individual column change then there is no need to track, for example, *Field Changes*.
3. **Filter out unwanted audit entries.** The Idera SharePoint audit tool allows relatively minor audit events such as the viewing of ASPX files and Master pages to be filtered out. For details see 3.1.2 *Configuring the audit log crawlers*.
4. **Reduce the number of days to retain log data.** Idera SharePoint audit allows audit entries older than a specified number of days to be automatically purged. If you don't need more than 3 months of Audit data then there is no need to keep it around for 3 years. For details see 3.1.2 *Configuring the audit log crawlers*.

## Appendix – Service and Database Accounts

Idera SharePoint audit stores 'enriched' audit data in its own SQL Server database. Due to the nature of the data this database has been secured well and you may need to manually grant certain user accounts used in your environment the appropriate privileges. The *Audit Service* also 'crawls' all SharePoint Site Collections and may need to be granted additional rights in SharePoint as well.

This appendix describes which accounts are involved and what privileges they must be granted.

### Audit Service account

The Idera SharePoint audit service is responsible for recording audit activity in all site collections that belong to web applications for which an Audit Log Crawler has been configured (see 3.1.2). The results are written to a custom Idera SharePoint audit database (see 3.1.1). In order to be able to do this the account used by the Audit Service must be given the appropriate privileges to carry out these activities.

#### SharePoint Privileges

The Audit Service account must be given full access to all site collections that are part of web applications for which a crawler has been configured. This can be achieved by creating a *Policy* for the relevant Web Applications<sup>6</sup>.

Note that *Farm Administrators* do not necessarily have access to all Site Collections and neither do users defined in the *Local Administrators* group unless these groups already participate in a SharePoint Policy.

#### Database Privileges – Windows Authentication

This sub section applies to environments where the *Windows Authentication* option is chosen on the *Audit Database Configuration* screen.

If the account the Audit Service runs under is the same as the account used by your Central Administration Application Pool then no changes to any database privileges are required.

However, if the accounts are not the same then the *db\_ddladmin*, *db\_securityadmin* and *Idera\_audit\_admin* database roles should be assigned to the service account. Note that the *Idera\_audit\_admin* role is not available until the Idera SharePoint audit database has been created (see 3.1.1).

#### Database Privileges – SQL Authentication

If the *SQL Authentication* option is chosen on the Audit Database Configuration screen then the service account will not need to be granted any rights on the Idera SharePoint audit database.

---

<sup>6</sup> [http:// <your\\_ca\\_site>/\\_admin/policy.aspx](http://<your_ca_site>/_admin/policy.aspx)

## Security settings for Central Administration pages

The Idera SharePoint audit-specific screens in Central Administration access the database in the context of the Application Pool account used by your Central Administration Web Application. Depending on your choice of database authentication you may need to carry out some manual configuration steps.

### SharePoint Privileges

The Central Administration Application pool already has all required privileges. No additional changes should be needed.

### Database Privileges – Windows Authentication

If the *Windows Authentication* option is chosen on the Audit Database Configuration screen then the database will be created and accessed using the Central Administration's Application Pool account. This account will most likely have all the privileges needed as it already deals with creating new Content Databases.

When the Idera SharePoint audit database objects are added to an existing database schema then this account must be granted the *db\_ddladmin* and *db\_securityadmin* roles on that database.

### Database Privileges – SQL Authentication

If the *SQL Authentication* option is chosen on the Audit Database Configuration screen then the database will be created and accessed using the specified SQL account. This account will need to be given the *dbcreator* and *securityadmin* server roles.

When the Idera SharePoint audit database objects are added to an existing database schema then this account must be granted the *db\_ddladmin* and *db\_securityadmin* roles on that database.

## Security settings for Individual Site collections

The Idera SharePoint audit-specific screens on the individual site collections (e.g. the Log Viewer or Site Collection Audit Settings screens) run in the context of the Application Pool account that hosts the Site Collection. Depending on your configuration you may need to make some manual changes.

### SharePoint Privileges

No changes are needed as the account already has full access to the Site Collection.

### Database Privileges – Windows Authentication

If the *Windows Authentication* option is chosen on the Audit Database Configuration screen then the database will be accessed using the Site Collection's Web Application's Application Pool account. If this account is different from the Central Administration Application Pool account then please make sure that the former is granted the *Idera\_audit\_admin* role on the Idera SharePoint audit database.

### Database Privileges – SQL Authentication

If the *SQL Authentication* option is chosen on the Audit Database Configuration screen then no changes are needed as this account has already been given all required privileges.