SharePoint audit™

Getting Started with Idera SharePoint audit

idera

Legal notice

Idera, Inc., DTx, IntelliCompress, Point admin toolset, Pointbackup, Pointcheck, PowerShellPlus, SharePoint enterprise manager, SharePoint security manager, 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 Idera, 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. © 2012 Idera, 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, IDERA, 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. Idera, Inc., may make improvements in or changes to the software described in this document at any time.

© 2003-2012 Idera, 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 Idera, 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

Welcome to Idera SharePoint audit

Idera SharePoint audit enhances the native auditing capabilities in SharePoint with expanded audit coverage, reporting, automatic audits, and simplified administration.

SharePoint audit lets you analyze the native SharePoint audit events. In addition, SharePoint audit enhances the native SharePoint audit data with the following data types:

- Logon events
- Inserts
- Field value changes
- Views
- Updates
- Deletes

SharePoint audit helps you to save time and also ensures consistent audits across the farm. You can enforce consistent audit policies on all of the servers and sites that make up your farm. When new sites or site collections are added, existing policies are applied to them automatically. SharePoint audit also monitors the state of auditing on your site collections. You can use a report to determine where auditing is enabled and disabled, and what types of actions are not audited on any given site.

SharePoint audit gives you the tools to meet the regulatory and compliance data needs for your SharePoint farm. You can use this data to help you meet the challenges of Sarbanes-Oxley (SOX), HIPAA, GLBA, Title 21 CFR Part 11, FERC, NERC, and others.

What is Idera SharePoint audit?

Idera SharePoint audit give the SharePoint administrator powerful tools to help audit activity across the SharePoint farm.

SharePoint audit helps you to do the following:

- Simplify Audit Administration
- Support your Compliance Needs
- Expand Audit Coverage
- Create Audit Reports

How does Idera SharePoint audit help me?

Idera SharePoint audit helps you in the following ways:

Lightweight and easy to deploy	With minimal server requirements, Idera SharePoint audit is light-weight, fast, efficient and easy to install.
Flexible setup	Unique, hierarchical administration model allows you to specify globally and tune locally with flexible auditing level overrides at the web application or site collection level.
Control what you log	Idera SharePoint audit's fine grained control over the type of events and data logged means that your audit logs won't grow out of control.
Safeguard performance speed	Idera SharePoint audit data is held in a separate database, protecting your SharePoint content database from any impact.
Automatic auditing	New site collections are automatically added to the set of monitored sites.
Monitor auditing level	Generate an overview of the auditing status across site collections across your SharePoint farm using the audit monitor.
Track important data	Track the important events and get the data you need for SOX, HIPAA GLBA, Title 21 CFR Part 11, FERC, NERC or others. Idera SharePoint audit can help you capture authentications, views, modifications or deletes. You can also see new and old field values.
Add to SharePoint auditing	Idera SharePoint audit enriches the native SharePoint audit data with logon events, inserts, and field value changes.

Audit all versions of SharePoint	Add auditing functionality to Windows SharePoint Services (WSS) 3.0 & SharePoint Foundation 2010.
Out-of-the-box and custom reporting	SharePoint audit provides out-of-the-box and custom reporting on information like content viewing, modification and deletion.
View and filter audit log data	SharePoint audit enables administrators and compliance professionals to view and audit SharePoint log data at any level. View logs from any list item's context menu.
Query audit data	SharePoint audit enables you to query audit data at the farm, site collection or list level and export logs to Excel as pivot tables for further manipulation.

Finding answers

This documentation set includes a comprehensive online Help system as well as additional resources that support you as you install and use the product. You can also search Idera Solutions, available at the Idera customer service portal (www.idera.com/support).

Using this Documentation

This documentation set includes a comprehensive online Help system as well as additional resources that support you as you install and use the product. You can also search Idera Solutions, available at the Idera customer service portal (www.idera.com/support).

Contacting Idera

Please contact us with your questions and comments. We look forward to hearing from you. For support around the world, please contact us or your local partner. For a complete list of our partners, please see our Web site (www.idera.com).

Sales	713.523.4433 1.877.GO.IDERA (464.3372) (only in the United States and Canada)
Sales Email	sales@idera.com
Support	713.533.5144 1.877.GO.IDERA (464.3372) (only in the United States and Canada) www.idera.com/support
Web site	www.idera.com

Using the Help

This Help system can be accessed through the Help link on any Idera SharePoint audit page in the SharePoint Central Administration page.

TIP:	The online Help requires Internet Explorer version 7.0 or later.

Understanding the document conventions

Idera documentation uses consistent conventions to help you identify items throughout the printed online library.

Convention	Specifying
Bold	Window items
Italics	Book and CD titles Variable names New terms
`Fixed Font`	File and directory names Commands and code examples Text typed by you
Straight brackets, as in [value]	Optional command parameters
Curly braces, as in {value}	Required command parameters
Logical OR, as in value 1 | value 2	Exclusively command parameters where only one of the options can be specified

About Idera

At Idera, we deliver a new generation of tools for managing, administering, and securing your Microsoft Windows Servers, including SQL Server, SharePoint, PowerShell and Microsoft Dynamics. We employ numerous industry experts worldwide who are devoted to bringing proven solutions to you, the administrator. Idera provides solutions that help you ensure server performance and availability and reduce administrative overhead and expense. Our award-winning products install in minutes, configure in hours and deploy worldwide in days. Idera is a Microsoft Gold Certified Partner headquartered in Houston, Texas, with offices in London, UK, Melbourne, Australia, and Sao Paulo, Brazil.

Idera products

Our tools are engineered to scale - from managing a single server to enterprise deployments with thousands of servers. Idera products combine ease of use with a design that installs in minutes, configure in hours, and deploy worldwide in days. To learn more about Idera products, visit our Web site (http://www.idera.com/products).

3.0 Release Notes

Idera SharePoint audit extends the built-in SharePoint auditing capabilities, providing complete SharePoint auditing for security and compliance management.

Updated: 9/20/2012 3:25 PM

New features

Idera SharePoint audit helps ensure compliance with the corporate security policies and the government regulations. In addition, it does the following:

- Enhances SharePoint audit data with logon events and inserts.
- Tracks views, updates, deletes and changes to the field or column level.
- Simplifies auditing administration across your SharePoint farm.
- Lets you use out-of-the-box reports to easily identify security events.

3.0 features

- Alerting: Now SharePoint audit lets you set up alerts on any audited event type and receive email notification to one or more email addresses. Find out right away when monitored actions happen, and most importantly when to take corrective action.
- Audit Log Management: Select and exclude user or service accounts that should not be tracked in the Idera SharePoint audit log.
- Miscellaneous bug fixes and enhancements.

Tips

The following tips for Idera SharePoint audit can help you to install and use SharePoint audit. ***If you need further assistance with any item***, please contact Support (www.idera.com/support).

- **New license is not validated for 2 minutes**

  When you add a license to SharePoint audit, the new license can take up to 2 minutes to be validated in the license page. When SharePoint audit validates the license, you must reload the license dialog for the validated license to appear. You can click Reload in your browser or navigate to another page, then return to the license page.

- **Any column change appears as a Schema Change**

  Any change to the SharePoint columns appears in SharePoint audit as a Schema Change.

- **Renamed libraries and list events do not appear in SharePoint audit**

  If you rename a library or list, the rename event does not appear in SharePoint audit. SharePoint itself does not record these changes. In consequence, SharePoint audit is unable to report them.

Learning about SharePoint audit events and filters

Idera SharePoint audit extends the native SharePoint auditing capabilities, providing complete SharePoint auditing for security and compliance management. When you use SharePoint audit, you can select the event types to audit. You can also control how SharePoint audit filters the events that appear in reports.

For more information, see the following:

- *Learning about auditing SharePoint events* on page 13
- *Learning about filtering audit events* on page 14

Learning about auditing SharePoint events

In addition to its own audit types and events, the SharePoint Audit Suite supports all audit types provided by SharePoint. The administrator can select any combination of the following Audit Types to log.

Most Used

Element	Notes
View	Viewing of a specified object by a user.
Insert	New items are added to a list or a library.
Update	Update of an object.
Field change	Track changes to fields, including the value before and after the change.
Check-in	Check in of an object.
Check-out	Check out of an object.
Delete	Deletion of an object.
Delete child objects	Deletion of any of the selected object's child objects, for example when a folder is deleted.
Move or rename	An object is moved or renamed.
Undelete	Deletion of an object is reversed, for example when an object is restored from the recycle bin.

Security related

Element	Notes
Security change	A change in the security configuration of an object, or a change in the object audit settings.
Authentication	Synthetic events generated by SharePoint audit based on user access of a Site Collection.

Miscellaneous

Element	Notes
Workflow	Use of an object in a workflow task.
Profile change	A change to a profile that is associated with an object.
Schema change	A change to the schema of an object, such as adding a column to a list.
Search	A search for a selected object.

Learning about filtering audit events

The Idera SharePoint audit log viewer lets you filter audit entries. You can use any of the following event types as filter criteria:

Most Used

Element	Notes
View	Viewing of a specified object by a user.
Insert	New items are added to a list or a library.
Update	Update of an object.
Field change	Track changes to fields, including the value before and after the change.
Check-in	Check in of an object.
Check-out	Check out of an object.
Delete	Deletion of an object.
Delete child objects (`Child-Delete`)	Deletion of any of the selected object's child objects, for example when a folder is deleted.
Move or rename	An object is moved or renamed.
Child move or rename	One of the selected object's child objects are moved or renamed, for example when a folder is renamed.
Undelete	Deletion of an object is reversed, for example when an object is restored from the recycle bin.
Copy	Copying of an object.

Audit related

Element	Notes
Changes to audit settings (`AuditMaskChange`)	Any change to the event types audited for the object.
Deletion of audited events (`EventsDeleted`)	Any deletion of audited events from the SharePoint database, for example an automated log truncation.

Security related

Element	Notes
Authentication	Synthetic events generated by SharePoint audit based on user access of a Site Collection.
Create user group	Creation of a user group for a SharePoint Site Collection
Delete user group	Deletion of a group for a SharePoint Site Collection
Add user to group	Addition of a new member to a group that is associated with a specific Site Collection.
Delete user from group.	Removal of a member from a group that is associated with a specific Site Collection.
Apply inheritance	Activating inheritance of security settings from the parent of an object.
Break inheritance	Disabling inheritance of security settings from the parent of an object.
Change permissions	Any change to the permissions that a user or group has to an object.
Changing of permissions levels	Any change to a role definition associated with an object.
Removal of permissions levels	Removal of a role definition associated with an object.
Creation of permissions levels	Creation of a new role definition associated with an object.
Break permission level inheritance	Disabling inheritance of role definitions from the parent of an object.

Miscellaneous

Element	Notes
Workflow	Use of an object in a workflow task.
Profile change	A change to a profile that is associated with an

Element	Notes
	object, such as adding a content type.
Schema change	A change to the schema of an object, such as adding a column to a list.
Search	A search for a selected object.
Custom	A custom action or event.

Learning about the components and architecture

Idera SharePoint audit includes the following components:

- Idera SharePoint audit Windows Audit Service
- Idera SharePoint audit SharePoint Solution Package (WSP)
- Idera SharePoint audit database

When you install SharePoint audit, you select a single SharePoint server in your farm to host the Audit Service. The Audit Service installer installs and configures the service automatically.

The Audit Service analyzes the contents of your existing SharePoint log files. It copies the contents of the log files to an internal SharePoint audit database and enriches the log files with audit data that it generates.

In addition, the installer adds the WSP to a single server in the SharePoint farm. SharePoint then automatically distributes the solution package to every SharePoint server in the farm. The Solution Package appears in your SharePoint farm as a Site Collection Feature. If needed, you can deactivate the feature in your SharePoint Site Collections.

After you install SharePoint audit, you specify a Microsoft SQL Server host for the SharePoint audit database. You also specify the name of the database. SharePoint audit uses the database to store the audit data that it processes. After the SharePoint audit installer creates the database, you must ensure that the Application Pool Account for each Web Application in the farm has access to the database. You can use the Microsoft SQL Server Management Studio or a similar tool to configure this access.

Learning about the requirements

You can install Idera SharePoint audit on any computer that meets or exceeds the hardware, software, and permission requirements.

Consider the following requirements when you install SharePoint audit in a typical environment.

- *Hardware requirements* on page 19
- *Software requirements* on page 19
- *Permission requirements* on page 20

Hardware requirements

Idera SharePoint audit requires the following hardware on any computer that hosts a component.

Hardware Type	Requirement
CPU	2 GHz. One or more multi-core CPUs per server.
Memory	1.5 GB per SharePoint server
Hard Drive Space	5 MB disk space for the components. Additional space for the audit logs.

Software requirements

Idera SharePoint audit components have the following general software requirements, as well as specific requirements outlined in the following sections. ***If a service pack is not specified***, a service pack is not required for that version of the software.

General Software Requirements

The SharePoint audit administrator should use one of the following browser versions:

- Internet Explorer 7
- Internet Explorer 8
- Internet Explorer 9

Users of SharePoint Audit can use any web browser supported by SharePoint, including modern versions of Internet Explorer, Google Chrome, Mozilla Firefox, Safari, and Opera.

You must have access to one or more Microsoft SharePoint farms with one of the following installed:

- Microsoft Office SharePoint Server (MOSS) 2007 SP1 with the July, 2008 Infrastructure upgrade
- Microsoft Windows SharePoint Services (WSS) 3.0 SP1 with the July, 2008 Infrastructure upgrade
- Microsoft SharePoint Foundation 2010
- Microsoft SharePoint Server 2010

The servers that make up your SharePoint farm can use either the 32-bit or the 64-bit version or Microsoft Windows. The servers must use one of the following operating systems:

- Microsoft Windows Server 2003
- Microsoft Windows Sever 2003 R2
- Microsoft Windows Server 2008
- Microsoft Windows Server 2008 R2

The SQL Servers that your farm includes must use one of the following versions of Microsoft SQL Server:

- Microsoft SQL Server 2005 Enterprise Edition, Standard Edition, or Express Edition
- Microsoft SQL Server 2008 Enterprise Edition, Standard Edition, or Express Edition
- Microsoft SQL Server 2012

Permission requirements

Idera SharePoint audit requires specific permissions and rights to successfully operate.

SharePoint audit stores audit data in a database that it creates. Since the information in this database is very sensitive, you must manually grant certain user accounts access to the database so that SharePoint audit can report on and display the content in the database.

In addition, the Audit Service must be able to access your SharePoint Site Collections and the native SharePoint audit data.

When you install SharePoint audit, you supply the credentials for the Service Account that the Audit Service uses. The account that you supply must have the following permissions assigned on the server that hosts the Audit Service:

- A member of the Local Administrators group.
- A member of the Farm Administrators group.
- Has `Full Control` permissions assigned for every Web Application that you want to audit. The SharePoint audit installer creates a Web Application Policy for all existing Web Applications that assigns this permission.
- Has the `Log On As Service` right assigned.
- Has the following database roles assigned:
    - `dbcreator`
    - `db_ddladmin`
    - `db_securityadmin`

In addition, if you specify Windows Authentication when you configure the SharePoint audit database, you must assign the new `Idera_Audit_Admin` database role to the account.

After the SharePoint audit installer creates the database, you must ensure that the Application Pool Account for each Web Application in the farm has access to the database. You can use the Microsoft SQL Server Management Studio or a similar tool to configure this access.

If you specify SQL Authentication when you configure the SharePoint audit database, you do not need to assign the new `Idera_Audit_Admin` database role to the account.

If SharePoint audit uses the same account as the Central Administration Application Pool, no database privilege changes are required.

You must also grant access to any SharePoint Site Collections that you want SharePoint audit to crawl or analyze. On both SharePoint 2007 and SharePoint 2010, you can use the Policy for Web Application page to create a SharePoint policy to grant this access. The Policy for Web Application page URL is `http://<CentralAdministration Site>/_admin/policy.aspx`.

Tip:	Members of the Farm Administrators group do not necessarily have access to all Site Collections. The SharePoint audit installer creates a Web Application Policy that assigns the required permission on all existing Web Applications. If you create a new Web Application, you should define a SharePoint Policy for the new Web Application that grants the Audit Service account Full Control in every Site Collection in the Web Application.

Installing and upgrading

You can install and deploy Idera SharePoint audit in any network environment. You must have at least one Microsoft SharePoint farm deployed to use SharePoint audit.

- Learn about the components and architecture.
  See *Learning about the components and architecture* on page 17.
- Review the hardware requirements, software requirements, and permission requirements.
  See *Hardware requirements* on page 19, *Software requirements* on page 19, *Permission requirements* on page 20
- Install the SharePoint audit service and SharePoint Solution package (WSP).
  See *Installing SharePoint audit* on page 23.

You can also upgrade an existing SharePoint audit installation.

See *Upgrading SharePoint audit* on page 24.

Installing SharePoint audit

Idera SharePoint audit includes two separate components. The SharePoint audit installer installs both components for you automatically.

You run the installer on any server in your SharePoint farm. The installer installs the Audit Service and Solution Package (WSP). SharePoint automatically distributes the Solution Package to the servers in the farm.

When you install, you specify a user account that SharePoint audit uses to access the farm. The account that you specify must meet certain permission requirements.

See *Permission requirements* on page 20 for additional information.

Tip:	When you install SharePoint audit, you should disable Windows User Account Control (UAC) during the installation.

After you install the SharePoint audit components, you add the SharePoint audit license and configure SharePoint audit.

For information about adding a license, see *Adding the SharePoint audit licenses* on page 27.

For information about configuring SharePoint audit, see *Configuring your deployment* on page 27.

How do I install Idera SharePoint audit?

You use the SharePoint audit Installer to install.

To install SharePoint audit

1. Log on to the computer where you want to install SharePoint audit. You must use an administrator account to log on.
2. Close all open applications.
3. In the SharePoint audit installer directory, run `Setup.exe`.
4. In the Welcome to the InstallShield Wizard for Idera SharePoint audit page, click **Next**.
5. In the License Agreement page, click **I accept the terms in the license agreement**, then click **Next**.

6. In the Destination Folder page, select the directory where the installer should store the SharePoint audit files. then click **Next**.
7. In the Setup Type page, choose the type of installation. Do one of the following, then click **Next**:
    - Click **Complete** to install the Audit Service and Solution Package on the server.
    - Click **Custom** to select the components to install on the server.
8. ***If you chose to perform a Custom installation***, in the Custom Setup page, select the components to install, then click **Next**.
9. In the Idera SharePoint audit Service Account page, specify the User Name and Password that the service should use, then click **Next**. The installer grants the `Logon as Service` right to the account that you specify. In addition, the installer creates a `Full Control` Web Application policy for the account on every Web Application in the farm. When you enter the User Name, you should enter it in the format *<Domain Name>\<User Name>*. You can also click **Browse** to the user name.
10. In the Ready to Install the Program page, click **Install**.
11. In the InstallShield Wizard Completed page, click **Finish**.

Upgrading SharePoint audit

If your SharePoint farm has version 2.5 of Idera SharePoint audit installed, you can upgrade to version 3.0 of SharePoint audit.

When you upgrade, SharePoint audit saves your existing audit content, settings, and licenses.

To upgrade, you use the installer to replace the existing SharePoint audit components.

For information about installing the components, see *Installing SharePoint audit* on page 23.

After you install the components, you must upgrade the Audit Database. When you use the Audit Database Configuration page to review the database settings, SharePoint audit upgrades the database automatically. When the installation is complete, open the Audit Database Configuration page and review the settings, then click **OK** to save the settings.

For information about using the Audit Database Configuration page, see *Configuring the SharePoint audit database* on page 28.

Uninstalling SharePoint audit

If necessary, you can uninstall the Idera SharePoint audit components. When you uninstall the components, you use the Windows Programs and Features control panel to remove the SharePoint audit Solution Package (WSP) and the Audit Service. If you choose, you can also remove the SharePoint audit database from your SQL Server host.

How do I uninstall SharePoint audit ?

You use the Windows Programs and Features Control Panel uninstall SharePoint audit.

To uninstall the SharePoint audit

1. Log on to the computer where you want to remove SharePoint audit. You must use an administrator account to log on when you want to remove SharePoint audit.
2. In the Windows Control Panel, open the Programs and Features Control Panel.

3. In the Programs and Features Control Panel, click **Idera SharePoint audit**, then click **Uninstall**.
4. In the Programs and Features dialog box, click **Yes** to uninstall the Audit Service.

How do I remove the SharePoint audit database?

You can use the Microsoft SQL Server Management Studio to delete the Idera SharePoint audit database from your SQL Server.

Configuring your deployment

After you install Idera SharePoint audit, you must add a license and configure it for use. When you configure it, you first create the database that SharePoint audit uses to store audit information. You then configure the permissions for the database.

After you set up the database, you can configure the audit settings for the Farm. You can optionally also configure Web Application and Site Collection audit settings.

Finally, you can configure the Audit Log Crawlers for the Farm. You can also create Audit Log Crawlers for the Web Applications and Site Collections that make up your farm.

You can also monitor the SharePoint audit status.

You can find out more information in the following topics;

- *Adding the SharePoint audit licenses* on page 27
- *Configuring the SharePoint audit database* on page 28
- *Learning about the Audit Settings* on page 30
- *Configuring the Audit Log Crawlers* on page 34
- *Monitoring the audit status* on page 35

Adding the SharePoint audit licenses

Idera SharePoint audit is a licensed product. You must have a valid license installed to use it. When you install a trial copy of SharePoint audit, it includes a license valid for 14 days. To continue using SharePoint audit, you must purchase a license code from Idera. After you purchase the license, you must add it to your SharePoint audit deployment.

You can contact Idera Sales to purchase a SharePoint audit license.

When you purchase a license, you must have the Farm ID available. The Farm ID appears in the Idera Licensing - Overview page.

How do I add the SharePoint audit license?

You use the SharePoint audit License page in the SharePoint Central Administration page to add the license code.

To add a SharePoint audit license

1. Open the SharePoint Central Admin Page.
2. Do one of the following:
   - ***If you are using SharePoint 2007***, click **Operations**, then in the Idera Share-Point audit area, click **Licenses**.
   - ***If you are using SharePoint 2010***, click **General Application Settings**, then in the Idera SharePoint audit area, click **Licenses**.
3. In the Idera Share Point audit Licenses page, click **Add License**.
4. In the Idera Share Point audit Licenses - Edit License page, type or paste the SharePoint audit license code in the License field. If you choose to, you can enter comments in the Custom Remarks field.
5. In the Idera Share Point audit Licenses - Edit License page, click **Save**.

Idera SharePoint audit Licenses - Edit License page

The Idera Licensing - Edit License page lets you add license codes for your Idera SharePoint audit deployment. You use the Idera Licensing - Overview page to review your licenses and to add additional licenses.

For information about licenses, see *Adding the SharePoint audit licenses* on page 27.

How do I add the SharePoint audit license?

You use the Idera Licensing - Overview page in the SharePoint Central Administration page to add the license code.

To install a SharePoint audit license

1. Open the SharePoint Central Admin Page.
2. Do one of the following:
   - ***If you are using SharePoint 2007***, click **Operations**, then in the Idera SharePoint audit area, click **Licensing**.
   - ***If you are using SharePoint 2010***, click **General Application Settings**, then in the Idera SharePoint audit area, click **Licensing**.
3. In the Idera Licensing - Overview page, click **Add License**.
4. In the Idera Licensing - Edit License page, type or paste the SharePoint audit license code in the License field. If you choose to, you can enter comments in the Custom Remarks field.
5. In the Idera Licensing - Edit License page, click **Save**.

Configuring the SharePoint audit database

Idera SharePoint audit stores enriched audit data and other information in a Microsoft SQL Server database. You use the Audit Database Configuration page to specify the settings that SharePoint audit uses for the database.

When you create the database, you specify the following:

- Database Server name
- Database name
- Authentication method

You can use any Microsoft SQL Server that meets the requirements. The server that hosts the database can also host other databases. The server does not need to be a part of the SharePoint farm.

You can use either Windows Authentication or SQL authentication for the database. Normally, you should use Windows Authentication. If you do use SQL authentication, you must specify the user name and password that SharePoint audit uses to connect to the server.

After you create the database, you should use the SQL Server Management Studio tool to assign the new `Idera_Audit_Admin` database role to the SharePoint audit service account.

For more information about permissions, see *Permission requirements* on page 20.

If necessary, you can use the Audit Database Configuration page to change the database settings. If you change the database server or the database name, none of your existing audit data appears in SharePoint audit, only new audit data appears.

Tip:	You should generally not make changes to the settings for an existing SharePoint audit database.

Normally, you create a database for SharePoint audit to use. If you choose, you can reuse an existing database. You should not reuse one of your existing SharePoint databases. If you reuse an existing database, the database cannot contain tables with the following names:

- `Idera_CrawlStatus`
- `Idera_EnrichedAuditData`
- `Idera_Versions`
- `Idera_Web`
- `Idera_Alerts`
- `Idera_AlertDefinitions`
- `Idera_AlertDefinitionScopeObjects`
- `Idera_AlertDefinitionAccounts`
- `Idera_AlertDefinitionRecipients`

In addition, SharePoint audit adds several stored procedures to an existing database. All of the added stored procedures have the `Idera_` prefix.

Tip:	Make sure that you add the SharePoint audit database to your SQL Server backup routine.

How do I configure the Audit Database?

You use the Audit Database Configuration page in the SharePoint Central Administration page to configure the Audit Database.

To configure the Audit Database

1. Open the SharePoint Central Admin Page.
2. Do one of the following:
   - ***If you are using SharePoint 2007***, click **Operations**, then in the Idera SharePoint audit area, click **Configure audit database**.
   - ***If you are using SharePoint 2010***, click **General Application Settings**, then in the Idera SharePoint audit area, click **Configure audit database**.
3. In the Configure SharePoint audit Database page, do the following:
   - Specify the name of the SQL Server in the Database Server field.
   - Specify the name of the database to use for SharePoint audit in the Database Name field. You can use the default name if you choose.
   - Select the type of authentication to use. ***If you use SQL Authentication***, you must specify an account name and password to use for the database.
4. In the Configure SharePoint audit Database page, click **OK**.

Learning about the Audit Settings

SharePoint objects are arranged in a hierarchy. Your Farm is made up of one or more Web Applications, which in turn include one or more Site Collections. SharePoint settings can reflect this hierarchy. Options that the administrator sets at the Farm or Web Application level can automatically take effect at lower levels of the hierarchy. On the other hand, the administrator can choose to allow settings made at a lower level to override options set at the Farm or Web Applications levels.

Audit settings in Idera SharePoint audit mimic this approach. The SharePoint audit administrator can configure options at the Farm, Web Application, and Site Collection levels of the SharePoint hierarchy. When you set options, you can choose to enforce the settings at lower levels in the hierarchy. You can also choose to let lower-level settings override higher-level settings. The administrator can also choose to inherit no settings from a higher-level object.

When you change the Farm Audit Settings, the changes can affect every Web Application and Site Collection in the farm. When you change Web Application Audit Settings, the changes can only affect that specific Web Application and its associated Site Collections. When you change the settings for a Site Collection, only the specific site is affected.

Structuring the settings in this way lets you meet the following needs:

Specify all settings at the Farm level.	You can prevent all lower levels from making changes to the SharePoint audit settings. This lets you centralize all audit settings in one place, making it easy to verify and update settings.
Specify unique settings for a single Web Application or Site Collection.	You can configure Common SharePoint audit settings at the Farm Level. You can disable inheritance for the SharePoint object that should have unique settings, then configure its settings directly.
Specify common settings at the Farm level and override settings for specified objects.	You can specify the Audit settings that all of the SharePoint objects should share at the Farm level. You can then override specific settings for a lower level object.

Tip: SharePoint audit stores audit settings at the Farm, Web Application, Site Collection, and Site levels in the SharePoint Object model. If a SharePoint Information Management Policy or a third-party product makes changes to the Audit Settings, audit data may not be collected properly.

What Audit Settings are available for the Farm, Web Applications, and Site Collections?

The Audit Settings that are available vary. Many settings are shared between levels, but not all.

Audit Setting	Farm	Web App	Site Collection
Inherit settings		✓	✓

Audit Setting	Farm	Web App	Site Collection
Enable auto auditing	✓	✓	
Events to audit	✓	✓	✓
Users to exclude	✓	✓	✓
Audit log access for site users	✓	✓	✓
Allow audit settings to be overridden	✓	✓	

Tip:	When specify users to exclude, SharePoint audit omits those user names when it crawls the SharePoint Audit Log. The users do not appear in the Audit Log in Share-Point audit. The users also do not cause SharePoint audit to generate alerts.

What do the settings configure?

You use the Farm Audit Settings, the Web Application Audit Settings, and the Site Collection Audit Settings to control the data that appears in the SharePoint audit log. You can make changes to the following settings:

Inherit Set-tings	When **Inherit all settings** is selected, all Audit Settings are inherited. A Web Application inherits settings from the Farm. A Site Collection inherits settings from the Web Application. If this option is selected on both a Site Collection and its parent Web Application, the Site Collection inherits its settings from the Web Application, which inherits them from the Farm. Indirectly, the Site Collection inherits its settings from the Farm.
Audit new Site Col-lections	When **Automatically audit all new site collections** is selected, SharePoint audit audits all Site Collections. When SharePoint audit detects a new Site Collection, it automatically enables auditing on the Site Collection.
Events to audit	You can select the events that SharePoint audit analyzes. You can select **Audit all event types** to include everything. You can also select specific events to include. You can click an event to include it. You can also control-click to select additional events. SharePoint audit log files grow in proportion to the number of event types that you audit. The more event types that you audit, the faster the log files grow. Consider limiting the number of event types that you audit to minimize the rate at which the log files grow.
Users to exclude	If you choose, SharePoint audit can exclude users when it crawls the Audit Log. SharePoint audit does not collect audit information for these users. You can use this ability to hide the System and Monitoring accounts,

	as well as certain support accounts.
Audit log access for site users	Normally, only Site Collection Administrators can review audit logs. You can select the **Enable access to the audit log for individual items** option to allow users to review the audit logs for individual items in the SharePoint farm.
Allow audit settings to be overridden	You can select the **Enable override of audit settings** option to allow lower-level SharePoint objects to override the SharePoint audit settings. When you select this option, you can use SharePoint audit to customize the settings for the Web Applications or Site Collections that make up the object.

Tip:	SharePoint audit stores audit settings in the SharePoint object model. If you make changes to the native SharePoint audit settings in the Site Settings for the top-level Site in a Site Collection, those changes override the settings made in SharePoint audit. To ensure that SharePoint audit collects the desired data, you should only make audit setting changes through SharePoint audit.

What event types can be audited?

For information about the event types, see *Learning about auditing SharePoint events* on page 13.

How do I make changes to the Audit Settings?

You can make changes to the settings for the Farm as a whole, and for each Web Application and each Site Collection that makes up the Farm.

For information about configuring the Farm Audit Settings, see*Configuring the Farm Audit Settings* on page 32.

For information about configuring the Web Application Audit Settings, see *Configuring the Web Application Audit Settings* on page 33.

For information about configuring the Site Collection Audit Settings, see *Configuring the Site Collection Audit Settings* on page 33.

Configuring the Farm Audit Settings

In Idera SharePoint audit, you can configure the audit settings for the entire Farm. If you choose, you can require the Web Applications and Site Collections that make up the Farm to use the same Audit Settings.

For information about the settings, see *Learning about the Audit Settings* on page 30.

For information about the Web Application Audit Settings, see *Configuring the Web Application Audit Settings* on page 33.

For information about the Site Collection Audit Settings, see *Configuring the Site Collection Audit Settings* on page 33.

How do I configure the Farm Audit Settings?

You use the Farm Audit Settings page to configure the Audit Settings for the SharePoint farm.

To configure the Farm Audit Settings

1. Open the SharePoint Central Admin Page.
2. Do one of the following:
   - ***If you are using SharePoint 2007***, click **Operations**, then in the Idera SharePoint audit area, click **Farm audit settings**.
   - ***If you are using SharePoint 2010***, click **General Application Settings**, then in the Idera SharePoint audit area, click **Farm audit settings**.
3. In the Farm Audit Settings page, configure the Audit Settings options.
4. In the Farm Audit Settings page, click **OK**.

Configuring the Web Application Audit Settings

In Idera SharePoint audit, you can configure the audit settings for the entire Farm. If you choose, you can require the Web Applications and Site Collections that make up the Farm to use the same Audit Settings.

If the Farm Audit Settings allow it, you can configure the Audit Settings for each Web Application in the Farm.

For information about the settings, see *Learning about the Audit Settings* on page 30.

For information about the Farm Audit Settings, see *Configuring the Farm Audit Settings* on page 32.

For information about the Site Collection Audit Settings, see *Configuring the Site Collection Audit Settings* on page 33.

How do I configure the Web Application Audit Settings?

You use the Web Application Audit Settings page to configure the Audit Settings for each Web Application.

To configure the Web Application Audit Settings

1. Open the SharePoint Central Admin Page.
2. Do one of the following:
   - ***If you are using SharePoint 2007***, click **Application Management**, then in the Idera SharePoint audit area, click **Web application audit settings**.
   - ***If you are using SharePoint 2010***, click **General Application Settings**, then in the Idera SharePoint audit area, click **Web application audit settings**.
3. In the Web Application Audit Settings page, in the Web Application area, select the Web Application whose settings you want to change from the drop-down list.
4. In the Web Application Audit Settings page, configure the Audit Settings options.
5. In the Web Application Audit Settings page, click **OK**.

Configuring the Site Collection Audit Settings

In Idera SharePoint audit, you can configure the audit settings for the entire Farm. If you choose, you can require the Web Applications and Site Collections that make up the Farm to use the same

Audit Settings.

If the Farm Audit Settings and Web Application Audit Settings allow it, you can configure the Audit Settings for each Site Collection in the Farm.

For information about the settings, see *Learning about the Audit Settings* on page 30.

For information about the Farm Audit Settings, see *Configuring the Farm Audit Settings* on page 32.

For information about the Web Application Audit Settings, see *Configuring the Web Application Audit Settings* on page 33.

How do I configure the Site Collection Audit Settings?

You use the Site Collection Audit Settings page to configure the Audit Settings for each Site Collection.

To configure the Site Collection Audit Settings

1. Open the Site Collection page.
2. In the Site Collection page, click **Site Actions > Site Settings**, then in the Idera SharePoint audit area, click **Site collection audit settings**.
3. In the Site Collection Audit Settings page, configure the Audit Settings options.
4. In the Site Collection Audit Settings page, click **OK**.

Configuring the Audit Log Crawlers

Idera SharePoint audit uses Audit Log Crawler jobs that you configure to analyze and enrich the SharePoint audit log data. When the Audit Log Crawler job runs, it analyzes the SharePoint log files based on the criteria that you specify in the Audit Settings. You create a single Audit Log Crawler for every Web Application that you want to include in the audit.

For information about configuring the Audit Settings, see *Learning about the Audit Settings* on page 30.

When you create the Audit Log Crawler, you specify the following:

Web Application	The Web Application to crawl.
Schedule	How often the crawler should crawl the log. The job can crawl the logs continuously or at an interval that you specify. In addition, you can control when the Log Crawler runs.
Filtering	You can control how much of the log that the Log Crawler analyzes. You specify the maximum age in days of the entries that the Log Crawler analyzes. The first time that the Log Crawler runs, it processes all entries that more recent than the age that you specify. You can also enter filters to exclude items from the Log Crawler. A filter is a Regular Expression that specifies the filenames to exclude. You can add one new filter per line.

Authentication	Since SharePoint does not audit login or logout events, SharePoint audit synthesizes the events. SharePoint audit generates a login event the first time that a user accesses a Site Collection. SharePoint audit generates a logoff event when the most recent access to a Site Collection by a user exceeds an interval that you specify.
Log Truncation	You can specify how SharePoint audit deletes old entries from the SharePoint Audit log and the Idera Audit Log. You remove old entries from the logs to reduce the size of the SharePoint audit database and to increase performance. By default, SharePoint audit does not remove entries. You can specify the age in days of the oldest entry that SharePoint audit leaves in the logs. If you specify 0 days, SharePoint audit immediately transfers the entries to the Idera SharePoint audit log and deletes them from the SharePoint log.
Recrawl the log	If you choose, you can force the Audit Log Crawler to clear its records and recrawl the Audit Log. If you change the Authentication or Filtering options, you should recrawl the log.

How do I configure the Audit Log Crawler settings?

You use the Audit Log Crawler page to configure the Audit Log Crawler settings. You must configure the Audit Log Crawler settings separately for every Web Application that you want to audit.

Tip:	When you make a change to the Audit Log Crawler settings, it may take up to 30 seconds for the changes to take effect in the Audit Log Crawler.

To configure the Audit Log Crawler settings

1. Open the SharePoint Central Admin Page.
2. Do one of the following:
   - ***If you are using SharePoint 2007***, click **Operations**, then in the Idera SharePoint audit area, click **Configure audit log crawler**.
   - ***If you are using SharePoint 2010***, click **General Application Settings**, then in the Idera SharePoint audit area, click **Configure audit log crawler**.
3. In the Audit Log Crawler page, in the Web Application area, select the Web Application whose settings you want to change from the drop-down list.
4. In the Audit Log Crawler page, configure the Audit Log Crawler settings.
5. In the Audit Log Crawler page, click **OK**.

Monitoring the audit status

You can use the Audit Monitor page to review the status of Idera SharePoint audit. The Audit Monitor page shows you the current audit status. When you review status, you can filter by Web Application or status code. You can also choose how many Site Collections to display on each page of the Audit Monitor.

If you choose, you can also directly view the XML for the audit status. You can import the XML into third-party System Management software including Microsoft System Center Operations Manager, Hewlett-Packard Site Scope, Hewlett-Packard OpenView, IBM Tivoli, or similar software.

How do I monitor the audit status?

You use the Audit Monitor page to review the audit status.

To view the audit status

1. Open the SharePoint Central Admin Page.
2. Do one of the following:
   - ***If you are using SharePoint 2007***, click **Operations**, then in the Idera SharePoint audit area, click **Audit monitoring**.
   - ***If you are using SharePoint 2010***, click **General Application Settings**, then in the Idera SharePoint audit area, click **Audit monitoring**.
3. In the Audit Monitor page, in the Filter Results area, select the Web Application that you want to monitor from the drop-down list. Select the status codes to include and the number of site collections to display on each page from the drop-down lists.
4. Click **View Results**.

How do I view the XML results for the audit status?

You use a custom URL for the Audit Monitor page to view the XML results. When you create the URL, you append parameters to the Audit Monitor page URL.

When you use this custom URL, the results appear as an XML file. You can save the XML file and import it into a third-party Systems Management tool.

The following parameters control the XML content that appears:

`WebApp`	You can specify the Web Applications to include in the results. If you do not specify a Web Application, the result XML includes all Web Applications in the Farm. When you specify a Web Application, you must include the full URL for the Web Application, including the port number. The format for the parameter is `?WebApp=http://<Web Application URL>:<Web Application Port>`
`Status`	You specify the Status codes to include in the results. The format for the parameter is `?status=<Status Code>`

The Status Code controls which Site Collections appear in the results. You can specify any of the following status codes:

`All`	Include all Site Collections.
`AllEnabled`	Include Site Collections where all Audit options are enabled.
`PartialEnabled`	Include Site Collections where some Audit options are enabled.

`NoneEnabled`	Include Site Collections where no Audit options are enabled.

The section of the URL that includes the parameters begins with a question mark (`?`).

When you specify both the Web Application and Status Code, the parameters can be in any order. You connect the parameters with the ampersand (`&`).

The custom URL should be in the following format:

```
http://<SharePoint Central Administration URL>/_admin/Idera.SharePointAudit.Farm/AuditMonitor.aspx?WebApp=http://<Web Application URL>:<Web Application Port>&status=<Status Code>
```

Or:

```
http://<SharePoint Central Administration URL>/_admin/Idera.SharePointAudit.Farm/AuditMonitor.aspx?status=<Status Code>&WebApp=http://<Web Application URL>:<Web Application Port>
```

Or, to specify only the Web Application:

```
http://<SharePoint Central Administration URL>/_admin/Idera.SharePointAudit.Farm/AuditMonitor.aspx?WebApp=http://<Web Application URL>:<Web Application Port>
```

Or, to specify only the Status Code:

```
http://<SharePoint Central Administration URL>/_admin/Idera.SharePointAudit.Farm/AuditMonitor.aspx?status=<Status Code>
```

To view the audit status as an XML file

1. Open the SharePoint Central Admin Page.
2. Do one of the following:
   - ***If you are using SharePoint 2007***, click **Operations**, then in the Idera SharePoint audit area, click **Audit monitoring**.
   - ***If you are using SharePoint 2010***, click **General Application Settings**, then in the Idera SharePoint audit area, click **Audit monitoring**.
3. Create the custom extension to the URL and paste it in the address bar of your Web Browser, then press Enter. The XML results appear in the Web Browser. You can save the result XML file for use in another program.

Viewing and reporting on audits

You can use Idera SharePoint audit to review the contents of audit logs and to create reports. When you view or report on the contents of the audit logs, you can export the results to a Microsoft Excel-format file for use in another program.

Viewing audit logs

Audited events appear in the audit logs in Idera SharePoint audit. You can review the Audit Logs for a single Web Application, a single Site Collection, a List, or a Folder or Item in SharePoint. You can apply similar filters to the logs at any level.

Tip:	The audit log can include the selected SharePoint object and all of the objects that it contains. If you review the audit log for multiple levels, the same audited event can appear in multiple audit logs. That is, the same event can appear in the Web Application audit log, the site collection audit log, the list audit log, and so on. When you view the audit log at a particular level in the SharePoint object hierarchy, you filter the log based on your selection.

When you view the audit log, you can filter the results. Not all filter criteria appear for every audit log level. The filter criteria that are available depend on the audit log level. You can also limit the number of results that appear on each page and control the sort order and grouping of the results. The following criteria are available:

Criteria	Web Application	Site Collection	List	Folder or Item
Sub Sites	✓	✓		
List and Libraries	✓	✓		
User	✓	✓	✓	✓
Item Type	✓	✓	✓	✓
Start Date	✓	✓	✓	✓
End Date	✓	✓	✓	✓
Page Size	✓	✓	✓	✓
Sorting/Grouping	✓	✓	✓	✓
Audit Events	✓	✓	✓	✓

You can filter based on the following criteria:

Sub Sites	**You can choose to include a specific site or you can include the site and all sub sites.**

Lists and Libraries	You can choose to include a specific list or library or you can include all lists and libraries.
User Name	You can specify a single user name to include in the results. All other users are omitted.
Item types	You can choose to include a specific item type or you can include all item types.
Start Date	You can specify the date and time for the oldest audit log entries to view. If you do not specify a start date, there is no limit to the age of the log entries that appear. The default start date is 1 month in the past.
End Data	You can specify the date and time for the newest audit log entries to view. If you do not specify an end date, log entries can appear up to the current date and time.
Page Size	You can limit the number of log entries that appear on a single page.
Sorting / Grouping	You can control how log entries appear in the audit log.
Audit Events	You can limit the entries that appear in the audit log based on the event type. You can include all audit log entries or a subset. You can click a single event type to include it, or control-click or shift-click to select additional event types. For information about the Audit Event Types, see *Learning about auditing SharePoint events* on page 13.

Tip: To limit the time it takes SharePoint audit to display results of queries of large log files, only the first 5000 results that match the criteria that you specify appear when you view the log file.

In the Audit Settings, you can specify that SharePoint audit omits certain users from the audit logs. The Audit Log Viewer page notes any user names that are omitted.

For information about the audit settings, see *Learning about the Audit Settings* on page 30.

For information about the Web Application Audit Settings, see *Configuring the Farm Audit Settings* on page 32.

For information about the Web Application Audit Settings, see *Configuring the Web Application Audit Settings* on page 33.

For information about the Site Collection Audit Settings, see *Configuring the Site Collection Audit Settings* on page 33.

When you view an Audit Log, you can click the blue **i** button for more information about the log entry. You can also export the log to a Microsoft Excel format file.

How do I view the Audit Log for a Web Application?

You use the SharePoint Central Administration page to view the Audit Log for a Web Application. Farm Administrators can view the Audit Log for a Web Application.

To view the Audit Log for a Web Application

1. Open the SharePoint Central Admin Page.
2. Do one of the following:
   - ***If you are using SharePoint 2007***, click **Application Management**, then in the Idera SharePoint audit area, click **View Web application audit logs**.
   - ***If you are using SharePoint 2010***, click **General Application Settings**, then in the Idera SharePoint audit area, click **View Web application audit logs**.
3. In the Audit Log Viewer page, in the Site Collection area, click the drop-down list, then click **Change Site Collection**.
4. In the Select Site Collection dialog box, in the Web Application drop-down list, click **Change Web Application**.
5. In the Select Web Application dialog box, click the Web Application whose audit logs you want to review.
6. In the Select Site Collection dialog box, in the URL area, click the Site Collection whose audit logs you want to review, then click **OK**.
7. In the Audit Log Viewer page, in the Filter Results and Audit Events areas, configure the Audit Log filter settings, then click **View Results**.

How do I view the Audit Log for a Site Collection?

You use the Site Actions menu to view the Audit Log for a Site Collection. Farm Administrators and Site Collection Administrators can review the audit logs for Site Collections.

To view the Audit Log for a Site Collection

1. Open the Site Collection or Site whose audit logs you want to view.
2. In the Site Collection or Site, click **Site Actions > Site Settings**.
3. In the Site Settings page, in the Idera SharePoint audit area, click **View audit logs for this site**.
4. In the Audit Log Viewer page, in the Filter Results and Audit Events areas, configure the Audit Log filter settings, then click **View Results**.

How do I view the Audit Log for a List?

You use the View Audit Log action in the List Tools to view the Audit Log for a List. Farm Administrators, Site Collection Administrators, and List Owners can review the Audit Logs for a List.

To view the Audit Log for a List

1. Open the List whose audit logs you want to view.
2. Do one of the following:
    - ***If you are using SharePoint 2007***, click **Actions > View Audit Log**.
    - ***If you are using SharePoint 2010***, in the SharePoint ribbon, in the List Tools area, click **List**, then click **View Audit Log**.
3. In the Audit Log Viewer page, in the Filter Results and Audit Events areas, configure the Audit Log filter settings, then click **View Results**.

How do I view the Audit Log for a Library?

You use the View Audit Log action in the Library Tools to view the Audit Log for a Library. Farm Administrators, Site Collection Administrators, and Library Owners can review the Audit Logs for a Library.

To view the Audit Log for a Library

1. Open the Library whose audit logs you want to view.
2. Do one of the following:
    - ***If you are using SharePoint 2007***, click **Actions > View Audit Log**.
    - ***If you are using SharePoint 2010***, in the SharePoint ribbon, in the Library Tools area, click **Library**, then click **View Audit Log**.
3. In the Audit Log Viewer page, in the Filter Results and Audit Events areas, configure the Audit Log filter settings, then click **View Results**.

How do I view the Audit Log for a folder or an item?

You use the View Audit Log item in the action menu to view the Audit Log for a folder or an item. Farm Administrators, Site Collection Administrators, and List Owners can review the Audit Logs for a Folder or Item. The SharePoint audit administrator can configure SharePoint audit to allow Folder or Item owners to view Audit Logs for a folder or for an item.

To view the Audit Log for a folder or an item

1. Open the list or library that contains the folder or item whose audit logs you want to view.
2. In the list or the library, click the action menu for the folder or the item, then click **View Audit Log**.
3. In the Audit Log Viewer page, in the Filter Results and Audit Events areas, configure the Audit Log filter settings, then click **View Results**.

Reporting on audit logs

Idera SharePoint audit Audit Log Viewer lets you review the audit logs at the Web Application, Site Collection, List, Library, Folder, and Item levels. When you view the audit logs, you can specify the exact content that you want to review and later export the content to a Microsoft Excel-format file for use in another program.

For information about viewing Audit Logs, see *Viewing audit logs* on page 39.

In addition, SharePoint audit includes pre-defined reports for the Site Collection level. A report is a pre-defined group of Audit Log Viewer settings. When you run the report, SharePoint audit filters the

audit log for the Site Collection that you choose and displays the results. You can then export the contents of the report to a Microsoft Excel-format file for use in another program.

SharePoint audit includes the following pre-defined reports:

Content Additions	Includes all events that add content to the specified site.
Column Modifications	Includes the value of the list items before and after the change.
Content Modifications	Includes all events that modified content in the site. The report does not include individual column changes.
Content and Column Modifications	Includes all events that modified content in the site, including any column changes.
Content Viewing	Includes all events where a user viewed content on the site.
Content Deletion	Includes all events where a user deleted content on the site or restored content from the Site Recycle Bin.
Content Type and List Modifications	Includes all events that modified the content types or lists on the site.
Custom Entries	Includes all Custom Audit entries that do not match any other categories.
Log in and Log out	Includes the synthetic Login and Logout entries generated by SharePoint audit.
Auditing Settings	Includes all events that change the SharePoint auditing settings.
Security Overview	Includes all events related to security.

How do I generate a custom report for a Site Collection?

You use the Audit Log Viewer tool to generate a custom report for a site collection. You can click **Run a custom report** in the Idera Audit Reports page to open the Audit Log Viewer.

For information about the Audit Log Viewer, see *Viewing audit logs* on page 39.

How do I generate a predefined report for a Site Collection?

You use the Site Actions menu to generate a predefined report for a Site Collection. Farm Administrators and Site Collection Administrators can generate a predefined report for Site Collections.

To generate a predefined report for a Site Collection

1. Open the Site Collection or Site that you want to generate a report for.
2. In the Site Collection or Site, click **Site Actions > Site Settings**.
3. In the Site Settings page, in the Idera SharePoint audit area, click **Run Audit Reports**.
4. In the Idera Audit Reports page, click the name of the report that you want to generate.

5. In the Audit Log Viewer page, in the Filter Results and Audit Events areas, review the Audit Log filter settings, then click **View Results**.

Using alerts

You can configure Idera SharePoint audit to generate alerts based on criteria that you specify. When SharePoint audit generates an alert, it can send an email to one or more addresses that you specify. The alert email includes the contents of the alert event along with an optional footer that you define.

When you use alerts, you must configure the alert settings, then define one or more alert triggers. You can also review the alert logs that SharePoint audit creates when it generates an alert.

Configuring the Alert Settings

You can configure Idera SharePoint audit to generate an Alert email when a condition that you specify is met. Before you can use Alerts, you should configure the Idera SharePoint audit Alert Settings.

When you configure the Alert Settings, you specify the following:

Email server	You can use the email server that your SharePoint farm uses. You can also specify a custom email server. If you use a custom email server, you must enter the host name or IP address and the port for the SMTP server to use. You should also supply a From address and a reply-to address. You also specify the character set to use for the email. Finally, you can choose to use SSL to connect to the SMTP server.
Email footer	You can define an email footer that SharePoint audit includes with every alert email. You can use the formatting toolbar to customize the appearance of the footer.
Global alert recipients	You can enter one or more email addresses that are global recipients of alerts. Global recipients are the default recipients for all alerts. You can exclude global recipients from particular alert definitions if you supply an alternate recipient. Alert recipients are grouped into internal and external recipients. Internal recipients are those listed in the Active Directory for the farm. You can use the SharePoint Check Names and Select People tools to verify that you have the correct addresses. External recipients are those that are not in the Active Directory list for your farm. You type their names in the External recipients field in the format `<name>@<domain>`. When you add global recipients, you can specify that global recipients only receive alerts if no alert-specific recipient is set.
Alert	You can configure SharePoint audit to remove alerts that are older than

groom-ing	you specify from the Alert log.

For information about viewing and creating alert definitions, see *Managing the alert definitions* on page 46.

For information about viewing the alert log, see *Viewing the alert log* on page 51.

How do I configure the Alert settings?

You use the Alert Settings page in the SharePoint Central Administration page to configure the Alert settings.

To configure Alert Settings

1. Open the SharePoint Central Admin Page.
2. Do one of the following:
   - ***If you are using SharePoint 2007***, click **Operations**, then in the Idera SharePoint audit area, click **Alert Settings**.
   - ***If you are using SharePoint 2010***, click **General Application Settings**, then in the Idera SharePoint audit area, click **Alert Settings**.
3. In the Alert Settings page, configure the alert settings, then click **Save** .
4. In the Audit Log Crawler page, configure the Audit Log Crawler settings.
5. In the Web Application Audit Settings page, click **OK**.

Managing the alert definitions

The Idera SharePoint audit Alert Definition Manager page lets you create, review, edit, and delete alert definitions. You use the SharePoint Central Administration page to view the Alert Definitions page.

The Alert Definition Manager page lets you make the following changes to alerts:

Create	You can define alerts that SharePoint audit emails to users that you specify when events that you specify occur in the SharePoint farm.
Enable	You can enable one or more temporarily-disabled alerts.
Dis-able	You can temporarily disable one or more alerts. When you disable an alert, the event no longer triggers alerts but SharePoint audit does not remove the alert definition.
Delete	You can remove one or more alert definitions from SharePoint audit.
Edit	You can make changes to an existing Alert definition.

When you create or edit an alert, you must specify the following criteria:

Alert definition name	Every alert that you define must have a unique name.
Event type	You specify the type of event that triggers the alert.

Scope	You can choose to have SharePoint audit trigger the alert when the event occurs anywhere in the farm. You can also specify a subset of the farm that triggers the alert. When you specify a subset, you can choose the Web Application, Site Collection, Site, and List or Library to include in the scope.
Event user	You can specify one or more users that trigger the alert.
Alert recipients	You can specify one or more email addresses that receive the alerts. In addition to the recipients that you specify, any global recipients receive the alert. Global Recipients are configured in the Alert Settings page. For more information about Global Recipients, see *Configuring the Alert Settings* on page 45. Alert recipients are grouped into internal and external recipients. Internal recipients are those listed in the Active Directory for the farm. You can use the SharePoint Check Names and Select People tools to verify that you have the correct addresses. External recipients are those that are not in the Active Directory list for your farm. You type their names in the External recipients field in the format `<name>@<domain>`.

How do I create an alert?

You use the Alert Definition Manager page to create a new SharePoint audit alert.

To create an alert

1. Open the SharePoint Central Admin Page.
2. Do one of the following:
   - ***If you are using SharePoint 2007***, click **Application Management**, then in the Idera SharePoint audit area, click **Alert definition manager**.
   - ***If you are using SharePoint 2010***, click **General Application Settings**, then in the Idera SharePoint audit area, click **Alert definition manager**.
3. In the Alert Definition Manager page, click **Create**.
4. In the Alert Definition Editor page, specify the Alert definition name, then select the event to alert on from the Event type drop-down list.
5. In the Scope area, do one of the following:
   - Click **Entire farm** to trigger the alert when the event is detected anywhere in the farm.
   - Click **Select scope** and then use the **Web application**, **Site collection**, **Site**, and **List or Library** drop-down lists to select a SharePoint object that triggers the alert, then click **Add Scope Object**. You can add multiple scope objects.
6. In the Event user area, specify one or more users that trigger the alert. You can use the SharePoint Check Names and Select People tools to help select the names.

7. In the Alert recipients area, specify one or more email addresses that receive the alerts. In addition to the recipients that you specify, any global recipients receive the alert. The Complete list of alert definition recipients area lists all of the recipients, including global recipients.
8. Click **Save**.

How do I edit an alert?

You use the Alert Definition Manager page to make changes to an existing SharePoint audit alert.

To edit an alert

1. Open the SharePoint Central Admin Page.
2. Do one of the following:
   - ***If you are using SharePoint 2007***, click **Application Management**, then in the Idera SharePoint audit area, click **Alert definition manager**.
   - ***If you are using SharePoint 2010***, click **General Application Settings**, then in the Idera SharePoint audit area, click **Alert definition manager**.
3. In the Alert Definition Manager page, click the name of the alert that you want to edit.
4. In the Alert Definition Editor page, make any needed changes to the alert definition, then click **Save**.

How do I enable a disabled alert?

You use the Alert Definition Manager page to enable one or more disabled SharePoint audit alerts. You can only enable a disabled alert. A disabled alert has `Disabled` in the Status column in the Alert Definition Manager page.

To enable disabled alerts

1. Open the SharePoint Central Admin Page.
2. Do one of the following:
   - ***If you are using SharePoint 2007***, click **Application Management**, then in the Idera SharePoint audit area, click **Alert definition manager**.
   - ***If you are using SharePoint 2010***, click **General Application Settings**, then in the Idera SharePoint audit area, click **Alert definition manager**.
3. In the Alert Definition Manager page, select the checkbox for one or more disabled alerts, then click **Enable**.

How do I disable an alert?

You use the Alert Definition Manager page to disable one or more SharePoint audit alerts. You can only disable an enabled alert. An enabled alert has `Enabled` in the Status column in the Alert Definition Manager page. When you disable an alert, you temporarily suspend its operation. You can later enable the alert to resume alerting.

To disable enabled alerts

1. Open the SharePoint Central Admin Page.
2. Do one of the following:
   - ***If you are using SharePoint 2007***, click **Application Management**, then in the Idera SharePoint audit area, click **Alert definition manager**.
   - ***If you are using SharePoint 2010***, click **General Application Settings**, then in the Idera SharePoint audit area, click **Alert definition manager**.
3. In the Alert Definition Manager page, select the checkbox for one or more enabled alerts, then click **Disable**.

How do I delete an alert?

You use the Alert Definition Manager page to delete one or more SharePoint audit alerts. When you delete an alert, the alert definition is no longer available in SharePoint audit. You can recreate the alert, but the new alert is not connected to the old.

To delete one or more alerts

1. Open the SharePoint Central Admin Page.
2. Do one of the following:
   - ***If you are using SharePoint 2007***, click **Application Management**, then in the Idera SharePoint audit area, click **Alert definition manager**.
   - ***If you are using SharePoint 2010***, click **General Application Settings**, then in the Idera SharePoint audit area, click **Alert definition manager**.
3. In the Alert Definition Manager page, select the checkbox for one or more alerts, then click **Delete**.
4. In the dialog box, click **OK** to delete the alert.

Editing alert definitions

The Idera SharePoint audit Alert Definition Editor page lets you specify the settings for an alert definition. You use the Alert Definition Manager page to create or edit the alert, then use the Alert Definition Editor to specify the Alert settings.

For information about the Alert Definition Manager, see *Managing the alert definitions* on page 46.

When you create or edit an alert, you specify the following criteria:

Alert definition name	Every alert that you define must have a unique name.
Event type	You specify the type of event that triggers the alert.
Scope	You can choose to have SharePoint audit trigger the alert when the event occurs anywhere in the farm. You can also specify a subset of the farm that triggers the alert. When you specify a subset, you can choose the Web Application, Site Collection, Site, and List or Library to include in the scope.
Event user	You can optionally specify one or more users that trigger the

	alert.
Alert recipients	You can specify one or more email addresses that receive the alerts. In addition to the recipients that you specify, any global recipients receive the alert. Global Recipients are configured in the Alert Settings page. For more information about Global Recipients, see *Configuring the Alert Settings* on page 45. Alert recipients are grouped into internal and external recipients. Internal recipients are those listed in your the Active Directory listing for your farm. You can use the SharePoint Check Names and Select People tools to verify that you have the correct addresses. External recipients are those that are not in the Active Directory list for your farm. You type their names in the External recipients field in the format `<name>@<domain>`.

How do I create an alert?

You use the Alert Definition Manager page to create a new SharePoint audit alert.

To create an alert

1. Open the SharePoint Central Admin Page.
2. Do one of the following:
   - ***If you are using SharePoint 2007***, click **Application Management**, then in the Idera SharePoint audit area, click **Alert definition manager**.
   - ***If you are using SharePoint 2010***, click **General Application Settings**, then in the Idera SharePoint audit area, click **Alert definition manager**.
3. In the Alert Definition Manager page, click **Create**.
4. In the Alert Definition Editor page, specify the Alert definition name, then select the event to alert on from the Event type drop-down list.
5. In the Scope area, do one of the following:
   - Click **Entire farm** to trigger the alert when the event is detected anywhere in the farm.
   - Click **Select scope** and then use the **Web application**, **Site collection**, **Site**, and **List or Library** drop-down lists to select a SharePoint object that triggers the alert, then click **Add Scope Object**. You can add multiple scope objects.
6. In the Event user area, specify one or more users that trigger the alert. You can use the SharePoint Check Names and Select People tools to help select the names.
7. In the Alert recipients area, specify one or more email addresses that receive the alerts. In addition to the recipients that you specify, any global recipients receive the alert. The Complete list of alert definition recipients area lists all of the recipients, including global recipients.
8. Click **Save**.

How do I edit an alert?

You use the Alert Definition Manager page to make changes to an existing SharePoint audit alert.

To edit an alert

1. Open the SharePoint Central Admin Page.
2. Do one of the following:
    - ***If you are using SharePoint 2007***, click **Application Management**, then in the Idera SharePoint audit area, click **Alert definition manager**.
    - ***If you are using SharePoint 2010***, click **General Application Settings**, then in the Idera SharePoint audit area, click **Alert definition manager**.
3. In the Alert Definition Manager page, click the name of the alert that you want to edit.
4. In the Alert Definition Editor page, make any needed changes to the alert definition, then click **Save**.

Viewing the alert log

You use the Idera SharePoint audit Alert Log Viewer to view the Alert Log. When you view the Alert Log, you review the alerts that SharePoint audit generated. You can view all alerts created by one or more alert definitions that you select. You can also view all of the alerts that meet new criteria that you specify.

For information about the criteria that you can specify, see *Editing alert definitions* on page 49.

You can also filter the alerts that appear in the log based on the following criteria:

- Item type
- Event start date
- Event end date
- Alert start date
- Alert end date

You can control how many Alerts appear in each page when you view the alert log and specify how the alerts are sorted and grouped.

When you view the alert log, you can export the log contents to a Microsoft Excel-format file that you can use in Excel or another program.

How do I view the Alert Log?

You use the SharePoint Central Administration pages to view the SharePoint audit Alert Logs.

Viewing the Alert Logs

1. Open the SharePoint Central Admin Page.
2. Do one of the following:
    - ***If you are using SharePoint 2007***, click **Application Management**, then in the Idera SharePoint audit area, click **View alert logs**.
    - ***If you are using SharePoint 2010***, click **General Application Settings**, then in the Idera SharePoint audit area, click **View alert logs**.

3. In the Alert Log Viewer page, in the Alert Definition Criteria area, do one of the following:
    - ***If you want to view all alerts from one or more existing Alert Definitions***, click **Select alert definitions**, then select one or more existing definitions from the Alert Definitions field. You can click one definition, then Control-Click or Shift-Click to add additional definitions.
    - ***If you want to view all alerts that match alert criteria that you specify***, click **Select individual alert definition criteria**, then specify the criteria.
4. ***If you want to filter the results of the search***, you can specify the filter criteria in the Filter Results area.
5. Click **View Results**.

Index

A

C

D

E

L

W