SOPHOS

Cybersecurity made simple.

Sophos Enterprise Console

auditing guide

product version: 5.5

Contents

1 About this guide

This guide tells you how to monitor changes in Sophos Enterprise Console configuration and other user or system actions.

2 About Sophos Auditing

Sophos Auditing enables you to monitor changes in Sophos Enterprise Console configuration and other user or system actions. You can use this information for regulatory compliance and troubleshooting or, in the case of malicious activity, during a forensic analysis.

By default, auditing is disabled. After you enable auditing in Sophos Enterprise Console, an audit entry is written to the SQL Server database SophosSecurity whenever certain configuration settings are changed or certain actions are performed.

The audit entry includes the following information:

- Action performed
- User who performed the action
- User's computer
- User's sub-estate
- Date and time of the action

Both successful and failed attempts at actions are audited, so the audit entries can show who performed actions on the system and who started actions that did not complete successfully.

You can use third-party programs, such as Microsoft Excel, Microsoft Access, Microsoft SQL Server Reporting Services, or Crystal Reports, to access and analyze data stored in the auditing database.

Important
Sophos Auditing makes data available to third-party applications. By using this feature you assume the responsibility of the security of the data made available, which includes ensuring the data can only be accessed by authorized users. For security considerations, see Built-in database protection (page 4).

For more information about what actions are audited, see What actions are audited? (page 19).

3 Key steps in using Sophos Auditing

The key steps in using Sophos Auditing are:

- Ensure the database is secure
- Enable auditing
- Grant access to the audit data
- Create an audit report

4 Ensure the database is secure

4.1 Built-in database protection

Sophos Enterprise Console and the SophosSecurity database provide several built-in types of protection for the audit data:

- Access control
- Tamper protection

Access control

Access control is implemented at the following levels:

- Front-end graphical user interface (GUI) level

  Only users who have the **Auditing** right in Sophos Enterprise Console and are members of the Sophos Console Administrators group can enable or disable auditing.

- Database level

  By default, only users who are members of the Sophos DB Admins group can access the database interfaces. In addition, the stored procedures from the database interfaces require a valid user session token to be presented. The token is generated by the system when a user opens the GUI or changes the sub-estate.

Tamper protection

The database is designed to prevent changes to the audit event data. There is no need to update any data in the auditing database, apart from certain configuration settings. There are triggers which would roll back any attempts to update or delete data from the tables.

The data can only be deleted by purging the database. Data that is more than two years old is purged automatically every 24 hours as part of the standard embedded scheduled purge task on the Sophos Enterprise Console server. You can also use the PurgeDB tool to purge the data (see http://www.sophos.com/en-us/support/knowledgebase/109884.aspx).

4.2 Enhance database security

Audit the database

In addition to the protection built into the Sophos Enterprise Console databases, we recommend setting additional protection at the SQL Server instance level (if not already in place) to audit user activities and changes on your SQL Server.

For example, if you are using an Enterprise edition of SQL Server 2008, you can use the SQL Server Audit feature. Earlier versions of SQL Server support login auditing, trigger-based auditing, and event auditing by using a built-in trace facility.

For more information about features that you can use for auditing activities and changes on your SQL Server system, see the documentation for your version of SQL Server. For example:

- SQL Server Audit (Database Engine)
- Auditing (Database Engine), SQL Server 2008 R2
- Auditing in SQL Server 2008
- Auditing (Database Engine), SQL Server 2008

Encrypt connections to the database

We strongly recommend that you encrypt connections between any clients and the Sophos Enterprise Console databases. For more information, see the SQL Server documentation:

- Enable Encrypted Connections to the Database Engine (SQL Server Configuration Manager)
- Encrypting Connections to SQL Server 2008 R2
- How to enable SSL encryption for an instance of SQL Server by using Microsoft Management Console

Control access to the database backups

Ensure proper, restrictive access control to any database backups or copies. This will ensure that unauthorized users cannot access the files, tamper with them, or accidentally delete them.

Note
The links in this section lead to information maintained by third parties and are provided for your convenience. Although we try to review the accuracy of the links periodically, the links may change without our knowledge.

Database connection check

When running the Sophos Enterprise Console 5.5.1 installer, database connection checks are made (prior to installation or upgrade) to establish whether a connection can be made to the database using TLS 1.2.

To ensure that TLS 1.2 is used when connecting to the database, use the **CheckDBConnection.exe** tool to provide output on the connection checks and make manual changes.

For more information, see knowledgebase article 127521.

5 Enable Sophos Auditing

By default, auditing is disabled. To enable auditing:

1. In Sophos Enterprise Console, on the **Tools** menu, click **Manage Auditing**.
2. In the **Manage Auditing** dialog box, select the **Enable auditing** check box.

> **Note**
> If the option is grayed out, this means that you don't have permission to manage auditing. You must be a member of the Sophos Console Administrators group and have the **Auditing** right in Enterprise Console to enable or disable auditing. For more information about user rights and role-based administration, see the Sophos Enterprise Console Help.

6 Grant access to the audit data

By default, only system administrators can access the audit data. Other users who need to access the data to create audit reports will need to be explicitly granted "Select" permission on the schema **Reports** in the database SophosSecurity. This can be done using the sqlcmd utility or in the SQL Server Management Studio.

6.1 Grant access to the audit data using the sqlcmd utility

To grant access to the audit data:

1. Copy the following script snippet to a document, for example, a Notepad file.

```
USE SophosSecurity;

DECLARE @stmt NVARCHAR(max);

DECLARE @Account VARCHAR(512)

/* Replace <Domain>\<User> with the actual account name for which to
 grant access to the audit data. */

SET @Account = N'<Domain>\<User>'

IF NOT EXISTS( SELECT * FROM sys.server_principals WHERE name =
 @Account )
BEGIN
      SET @stmt = N'CREATE LOGIN [' + @Account + N'] FROM WINDOWS';
      EXEC sp_executesql @stmt;
END;

IF NOT EXISTS( SELECT * FROM sys.database_principals WHERE name =
 @Account )
BEGIN
      SET @stmt = N'CREATE USER [' + @Account + N'] FOR LOGIN [' +
 @Account + N']';
      EXEC sp_executesql @stmt;
END;

SET @stmt = N'GRANT SELECT ON SCHEMA :: [Reports] TO [' + @Account +
 N']';
EXEC sp_executesql @stmt;
GO
```

2. Replace the <Domain> and <User> placeholders in the statement "SET @Account = N'<Domain>\<User>'" with the domain and username of the user to whom you want to grant access.

If your computers are in a workgroup, replace <Domain> with the name of the computer where the database is installed. If the user will be accessing the data from a different workgroup computer, the user account must exist on both computers, with the same username and password.

3. Open the command prompt.
4. Connect to the SQL Server instance. Type:

```
sqlcmd -E -S <Server>\<SQL Server instance>
```

The default SQL Server instance is SOPHOS.

5. Copy the script snippet from the file and paste it into the command prompt.
6. Press Enter to run the script.
After the script runs, the user is granted "Select" permission on the **Reports** schema of the SophosSecurity database and can access the audit data.
7. Repeat for each user who needs access.

6.2 Grant access to the audit data using SQL Server Management Studio

Before you can grant "Select" permission on the schema **Reports** in the database SophosSecurity to a user in SQL Server Management Studio, ensure that the user has a SQL Server login and is a SophosSecurity database user.

- If the user already has a SQL Server login, add it as a SophosSecurity database user. In Object Explorer, expand the server, expand the **Databases** folder, expand **SophosSecurity**, and then expand **Security**. Right-click **Users** and click **New User**. In the **Database User** dialog box, enter the user name and select the login name. Click **OK**.

  For more information about creating database users, see http://msdn.microsoft.com/en-us/library/aa337545.aspx#SSMSProcedure.

- If the user doesn't have a SQL Server login, add a new SQL Server login and make it a SophosSecurity database user. In Object Explorer, expand the server, expand **Security**. Right-click **Logins** and click **New Login**. In the **Login** dialog box, on the **General** page, enter the account or group name. Go to the **User Mapping** page and select **SophosSecurity**. Click **OK**.

  For more information about creating SQL Server logins, see http://msdn.microsoft.com/en-us/library/aa337562.aspx#SSMSProcedure.

To grant access to the audit data to a user, in SQL Server Management Studio:

1. In Object Explorer, expand the server, expand the **Databases** folder, expand **SophosSecurity**, expand **Security**, and then expand **Schemas**.
2. Right-click **Reports** and click **Properties**.
3. In the **Schema Properties - Reports** dialog box, on the **Permissions** page, click **Search**. In the **Select Users or Roles** dialog box, add a user or users.
4. For each user, in the **Permissions for <user>** section, on the **Explicit** tab, select **Select** under **Grant**, and then click **OK**.

7 Create an audit report in Microsoft Excel

This example shows you how to import audit data from the SQL Server database and analyze the data in Microsoft Excel 2010.

The following sections describe how to create an audit report in Microsoft Excel by following these key steps:

- Set up a connection to the auditing database (create a new data source).
- Create a query in Microsoft Query.
- Return data to Excel.
- Create a report in Excel (a table or a PivotTable report).

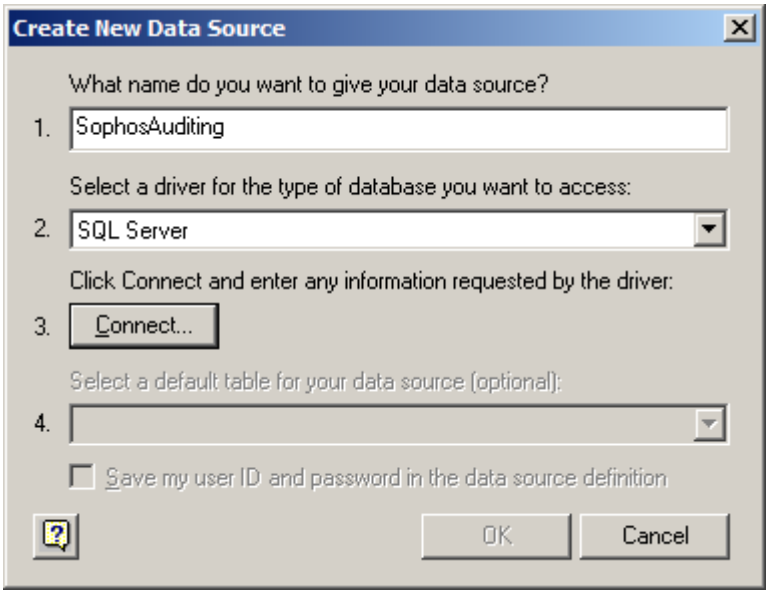
Note
We recommend using numeric IDs instead of string values if you want to bind any external logic to exported audit data. For example, instead of using values from the **TargetType** field, use the values from the **TargetTypeId** field. This will help to avoid potential compatibility issues should any string values change in a future release of Enterprise Console. For a table of numeric IDs, see Appendix: Numeric IDs of the data field values (page 27).

For more information about importing SQL Server data and creating reports in Excel, see Microsoft documentation.

7.1 Set up a connection to the database

First, you need to connect to the database.

1. Open Excel. On the **Data** tab, in the **Get External Data** group, click **From Other Sources**, and then click **From Microsoft Query**.
   The **Choose Data Source** dialog box appears.
2. On the **Databases** tab, leave **<New Database Source>** selected and click OK.
3. In the **Create New Data Source** dialog box, type the name you want to give your data source. In this example, we call it **SophosAuditing**.
4. In the **Select a driver for the type of the database you want to access** box, select **SQL Server**.

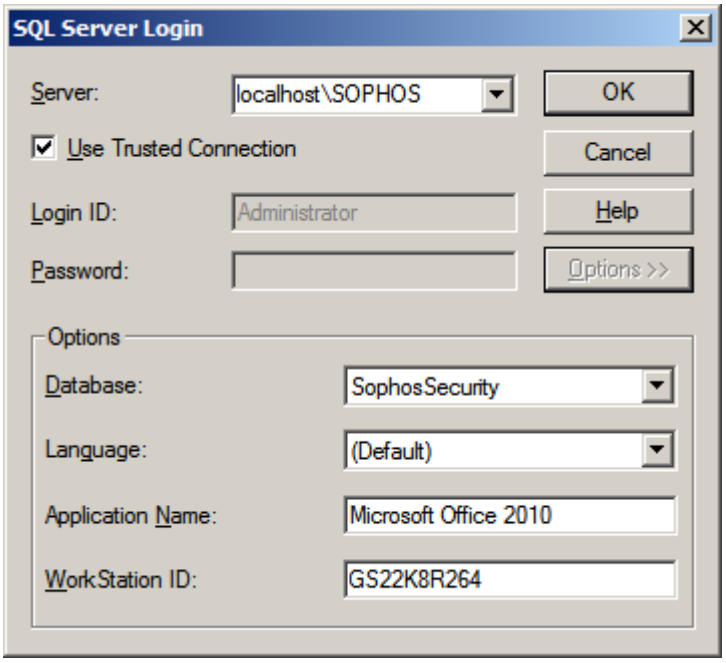


Click **Connect**.

5. In the **SQL Server Login** dialog box, in the **Server** box, enter the name of the SQL Server that you want to connect to.

   In this example, we are connecting to the SOPHOS database instance on the same computer (localhost).

6. Click **Options** to expand the **Options** panel. In the **Database** box, select **SophosSecurity**.



Click **OK**.

7. In the **Create New Data Source** dialog box, under **Select a default table for your data source (optional)**, select **vAuditEventsAll**.
8. Click **OK**.

7.2 Create a query

This example shows how to query the data source you just created for the information about changes to the Data Control policies over the past three months.

1. In the **Choose Data Source** dialog box, clear the **Use the Query Wizard to create/edit queries** check box.
2. Select the data source you created in the previous steps (in this example, **SophosAuditing**) and click **OK**.
   The **Microsoft Query** dialog box displays **Query from SophosAuditing** with the default table, **vAuditEventsAll**, which you selected when you created the data source.
3. Do one of the following:
   - Create a query in the design view.
     a) In the **Microsoft Query** dialog box, on the **Criteria** menu, click **Add Criteria**.
     b) In the **Add Criteria** dialog box, next to **Field**, select **Timestamp**. Ensure that the **Operator** field is blank. In the **Value** field, type:

        ```
        >=DATEADD(mm,-3,GETUTCDATE())
        ```

        Use the list separator specified in Region and Language settings in Control Panel. For example, if your list separator is a semicolon, use semicolons instead of commas in the statement above. You may receive the error message "Extra ')'" if you use an incorrect list separator.

        Click **Add**. The criterion is added to **Query from SophosAuditing**.
     c) In the **Add Criteria** dialog box, next to **Field**, select **TargetType**. In the **Operator** field, select **equals**. In the **Value** field, select or type **Policy**.

        Click **Add**. The criterion is added to **Query from SophosAuditing**.
     d) In the **Add Criteria** dialog box, next to **Field**, select **TargetSubType**. In the **Operator** field, select **equals**. In the **Value** field, select or type **Data control**.

        Click **Add**. The criterion is added to **Query from SophosAuditing**.

        In the **Add Criteria** dialog box, click **Close**.
     e) In the **Microsoft Query** dialog box, add fields from **vAuditEventsAll** to the query by double-clicking on them. Alternatively, you can add a field to the query by dragging it from the table to the display area.
   - Create a query in the SQL view.

a) In **Microsoft Query**, click the **SQL** button and type your SQL statement, for example:

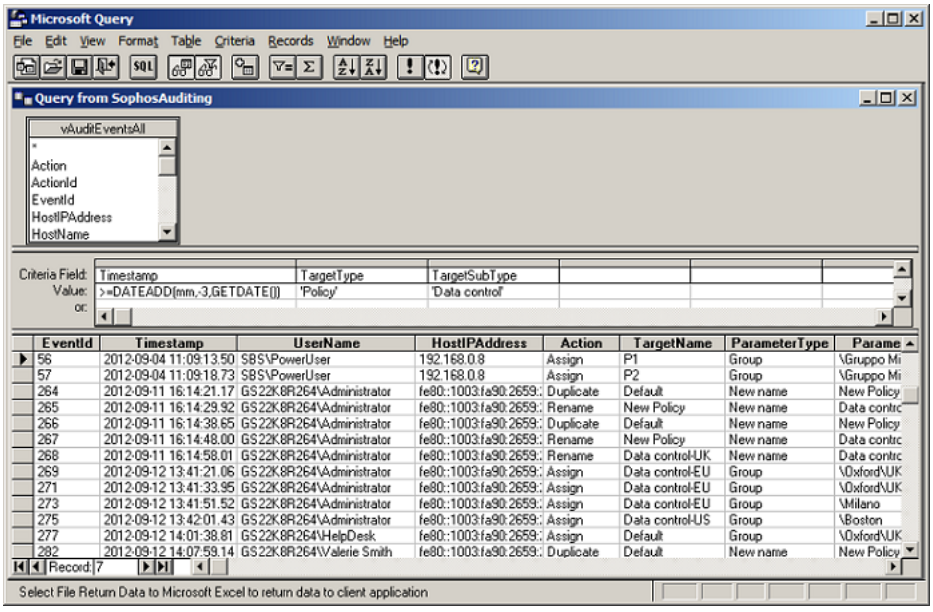
```
SELECT EventId, Timestamp, UserName, HostIPAddress, Action,
 TargetName, ParameterType, ParameterValue, Result

FROM SophosSecurity.Reports.vAuditEventsAll

WHERE (Timestamp>=DATEADD(mm,-3,GETUTCDATE()))
AND (TargetType='Policy')
AND (TargetSubType='Data control')

ORDER BY EventId ASC
```

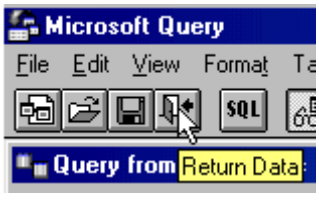
Click **OK**.



4. To save the query, on the **File** menu, click **Save**.

7.3 Return data to Excel

To return to Excel, in the **Microsoft Query** dialog box, click the **Return Data** button.



Alternatively, on the **File** menu, click **Return Data to Microsoft Excel**.

Back in Excel, the **Import Data** dialog box appears, where you can choose which type of report to create.

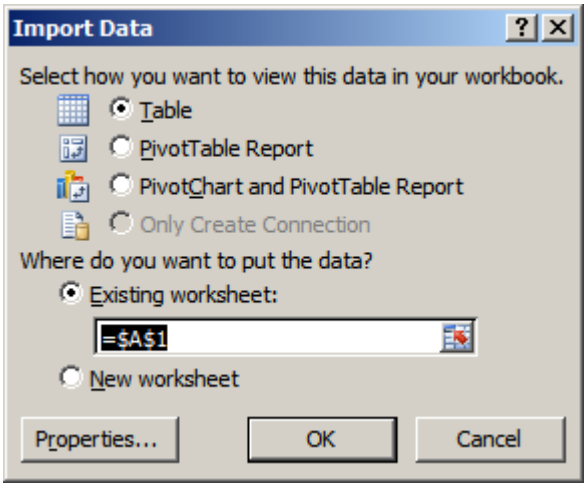
The following examples show how to:

- Create a table (page 13)
- Create a PivotTable report (page 14)

7.4 Create a table

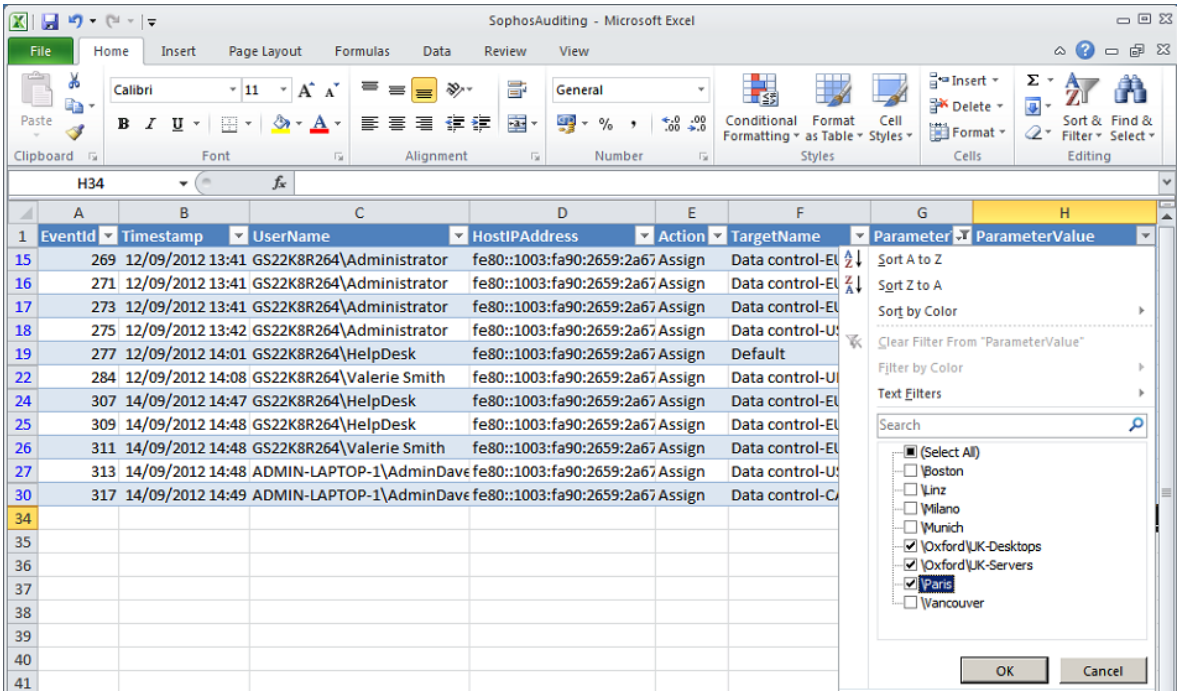
1. If you chose to import the audit data into an Excel table, in the **Import Data** dialog box, leave **Table** selected.

   To place the data in the existing worksheet starting at cell A1, leave **Existing worksheet** selected:



   Click **OK**.

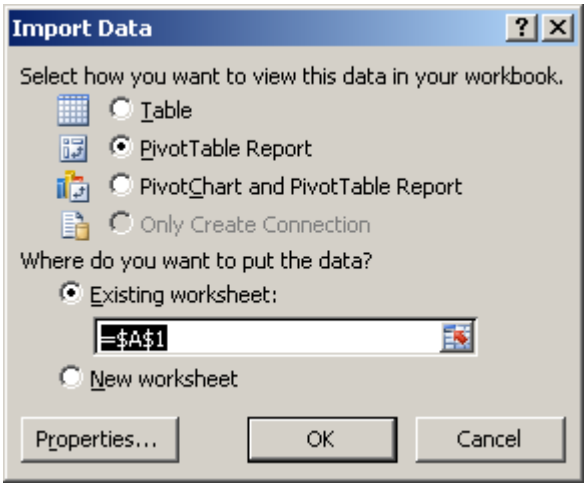
   The audit data is imported into an Excel table.
2. Save your Excel workbook.
3. You can use the search filter to analyze your data.



7.5 Create a PivotTable report

1. If you chose to import the audit data into an Excel table, in the **Import Data** dialog box, select **PivotTable Report**.

   To place the data in the existing worksheet starting at cell A1, leave **Existing worksheet** selected:



   Click **OK**.

   The resulting, empty PivotTable appears in the worksheet.
2. In the **PivotTable Field List** that appears on the right, select the fields you want to view.

   Tip
   You can filter data before you add fields. In the **PivotTable Field List**, in the **Choose fields to add to report** box, rest the pointer on a field name, and then click the filter drop-down arrow next to the field name. On the **Filter** menu, select the filter options that you want.

3. Depending on how you want your PivotTable to be displayed, drag the fields between the areas in the **PivotTable Field List**. For example, you may decide to display the names of the users and the policies that they touched as row labels and actions that the users performed on policies as column labels.
4. To be able to filter the PivotTable, under **PivotTable Tools**, **Options**, click **Insert Slicer**.
5. In the **Insert Slicers** dialog box, select the slicers you want to use and click **OK**.

   You can re-arrange the slicers on the worksheet by selecting a slicer and dragging and dropping it at a desired position. You can also customize your slicers, for example, by giving them different colors. To do this, select a slicer. Under **Slicer Tools**, **Options**, select one of the **Slicer Styles**.
6. Save your workbook.

8 More examples of creating an audit report

This section tells you how to create a new query from an existing data source in Microsoft Excel and gives you more examples of the queries you can use to create audit reports.

The section also tells you how to create a report containing detailed policy changes in an XML format.

8.1 Create a query from an existing data source

To create another audit report from the data source you created in Set up a connection to the database (page 9):

1. In Excel, go to the **Data** tab, click **From Other Sources**, and then click **From Microsoft Query**.
2. In the **Choose Data Source** dialog box, clear the **Use the Query Wizard to create/edit queries** check box. Select the data source you created previously (for example, SophosAuditing) and click **OK**.
3. In **Microsoft Query**, click the **SQL** button and enter a SQL statement for your report.

The following section contains some examples you can use.

8.2 More examples of queries

Example 1: Which policies a certain person changed over the past 60 days

```
SELECT EventId, Timestamp, TargetSubType, Action, TargetName,
 ParameterType, ParameterValue, Result

FROM SophosSecurity.Reports.vAuditEventsAll

WHERE (Timestamp>=DATEADD(dd,-60,GETUTCDATE()))
AND (TargetType='Policy')
AND (UserName='GS22K8R264\Administrator')

ORDER BY Timestamp DESC
```

Note
In a statement, instead of listing the fields you want to include in the report, you can type "SELECT *" to select all fields in the database view.

Example 2: Which policies were applied to a certain group in the past six months

```
SELECT *

FROM SophosSecurity.Reports.vAuditEventsAll

WHERE (Timestamp>=DATEADD(mm,-6,GETUTCDATE()))
AND (TargetType='Policy')
AND (Action='Assign')
AND (ParameterType='Group')
AND (ParameterValue='\Oxford\UK-Servers')

ORDER BY EventId DESC
```

Note
If the group for which you are creating a report is a subgroup of another group, you will need to either type the full path to the group or use the "ends with" statement (provided the name of the group is unique). For example, to create a report for the group \Oxford\UK-Servers, you can type either of the following:

- `ParameterValue='\Oxford\UK-Servers'`
- `ParameterValue Like '%UK-Servers'`

Example 3: What group changes were made by a certain person over the past three months

The following statement will result in a report showing what groups were created, deleted, moved or renamed and what computers were assigned to groups by the user in the past three months.

```
SELECT *

FROM SophosSecurity.Reports.vAuditEventsAll

WHERE (Timestamp>=DATEADD(mm,-3,GETUTCDATE()))
AND (UserName='GS22K8R264\Administrator')
AND ((TargetType='Group') OR ((TargetType='Computer') AND
 (Action='Assign')))
```

Example 4: What changes were made to a certain group over the past three months

```
SELECT *

FROM SophosSecurity.Reports.vAuditEventsAll

WHERE (Timestamp>=DATEADD(mm,-3,GETUTCDATE()))
AND (ParameterValue='\Oxford\UK-Desktops')
```

8.3 Return data to Excel

After you have created a query for your audit report, return data to Excel (**File** > **Return Data to Microsoft Excel**) and create a report as described in Create a table (page 13) or Create a PivotTable report (page 14).

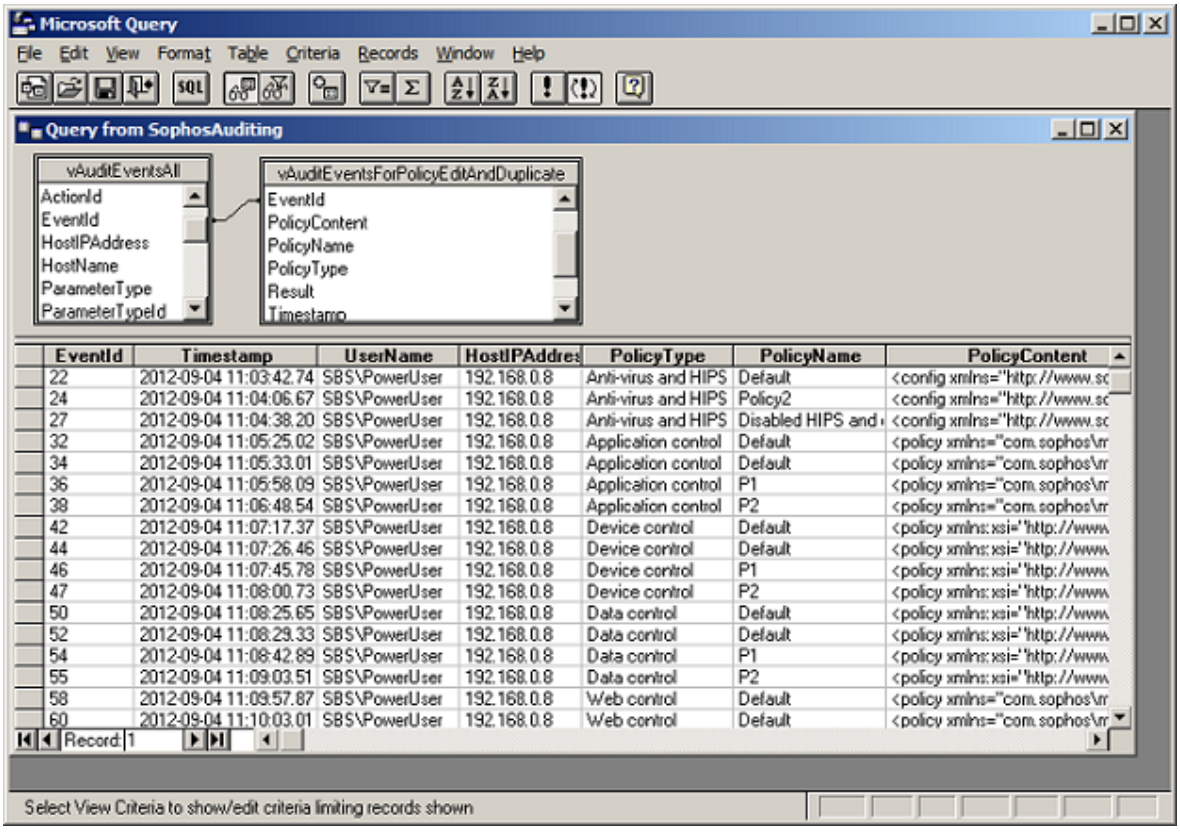
8.4 Create a report containing policy changes in an XML format

When a user edits a policy, the resulting policy settings are saved in an XML format and can be accessed via the **Reports.vAuditEventsForPolicyEditAndDuplicate** database view.

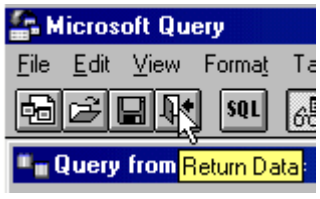
You can create a report containing this additional data by linking the two tables, **Reports.vAuditEventsAll** and **Reports.vAuditEventsForPolicyEditAndDuplicate**.

1. Create a new query from an existing data source, as described in Create a query from an existing data source (page 15).
2. In **Microsoft Query**, click **Table** and then click **Add Tables**. In the **Add Tables** dialog box, select **vAuditEventsForPolicyEditAndDuplicate** and click **Add**. Once done, click **Close**.
3. Link the tables to each other by linking the fields that are common to both tables. Click on the common field, **EventID**, in the first table and drag the mouse over to the **EventID** field in the second table.
4. Add fields to the query by double-clicking on them. Alternatively, you can add a field to the query by dragging it from the table to the display area.

> **Tip**
> You can use the **Joins** dialog in Microsoft Query (**Table** > **Joins**) to create a query joining the two tables.



5. To save the query, on the **File** menu, click **Save**.
6. To return to Excel, click the **Return Data** button.



Alternatively, on the **File** menu, click **Return Data to Microsoft Excel**.

Back in Excel, the **Import Data** dialog box appears. Create a table (Create a table (page 13)). The **PolicyContent** column will contain the policy configuration changes in XML format.

Tip

If you use Microsoft SQL Server Management Studio, you can query the **Reports.vAuditEventsForPolicyEditAndDuplicate** view directly. Then, when you follow a link in the **PolicyContent** column in the query results, the policy content will be displayed in an XML editor in a format more readable than that in an Excel table.

9 What actions are audited?

Categories of audited actions include:

- Computer actions
- Computer group management
- Policy management
- Role management
- Sophos Update Manager management
- System events

9.1 Computer actions

The following computer actions are audited:

- Acknowledge/resolve alerts and errors
- Protect a computer
- Update a computer
- Delete a computer
- Perform a full system scan on a computer

9.2 Computer group management

The actions logged for group management are:

- Create a group
- Delete a group
- Move a group
- Rename a group
- Assign a computer to a group

9.3 Policy management

The actions logged for policy management are:

- Create a policy (page 20)
- Rename a policy
- Duplicate a policy (page 20)
- Edit a policy
- Assign a policy to a computer

- Reset a policy to factory defaults
- Delete a policy (page 20)

9.3.1 Create a policy

When you create a new policy, the default policy is duplicated into a new policy named "New Policy". You can rename the new policy immediately after it has been created. For example, if you create a new Anti-Virus and HIPS policy and rename it to "Servers", the following audit entries will be created:

Table 1: Create a new policy and give it a new name

Action	Target Type	Target SubType	Target Name	Parameter Type	Parameter Value	Result
Duplicate	Policy	Anti-virus and HIPS	Default	New name	New Policy	Success
Rename	Policy	Anti-virus and HIPS	New Policy	New name	Servers	Success

9.3.2 Duplicate a policy

When you duplicate a policy, a "Duplicate a policy" event is created, for example:

Table 2: Duplicate a policy

Action	Target Type	Target SubType	Target Name	Parameter Type	Parameter Value	Result
Duplicate	Policy	Web Control	TestPolicy1	New name	Copy of TestPolicy1	Success

9.3.3 Delete a policy

When you delete a policy, any groups that use the deleted policy will revert to using the default policy. In this case, no separate audit event is created that shows that the default policy has been reapplied.

9.4 Role management

The actions logged for role management are:

- Create a role
- Delete a role
- Rename a role
- Duplicate a role

- Add a user to a role
- Remove a user from a role
- Add a right to a role
- Remove a right from a role

9.5 Sophos Update Manager management

The actions logged for Sophos Update Manager management are:

- Update an update manager
- Make an update manager comply with configuration
- Acknowledge alert
- Delete an update manager
- Configure an update manager

9.5.1 How changes in Update Manager configuration are recorded

In Enterprise Console, the **Configure update manager** dialog box contains a number of tabs and configuration options that are essentially the update manager's configuration policies. When you edit the update manager's configuration, actions are logged against the following policies:

- Update Manager - subscription - specifies software subscriptions that the update manager keeps up to date.
- Update Manager - upstream - specifies the update source for the update manager.
- Update Manager - downstream - specifies shares where the update manager downloads the software.
- Update Manager - schedule - specifies how often the update manager checks for threat detection data and software updates.
- Update Manager - general - specifies logging options for the update manager.
- Software subscription - specifies configuration of a software subscription, for example, "Recommended".

Sometimes changes in one update manager policy cause changes in other update manager policies (such as parameter ID value changes). In such cases, you will see several records in SophosSecurity database for one change you made. For example, if you create a schedule on the **Schedule** tab of the **Configure update manager** dialog box and click OK, the following audit entries will be created:

Table 3: Create an Update Manager's update schedule

EventId	Action	Target Type	Target SubType	Target Name	Parameter Type	Parameter Value	Result
22	Edit	Policy	Update Manager - schedule	New name	None		Success

EventId	Action	Target Type	Target SubType	Target Name	Parameter Type	Parameter Value	Result
21	Edit	Policy	Update Manager - upstream	New Policy	None		Success
20	Edit	Policy	Update Manager - subscription		None		Success

In this case, only the first action, logged for the **Update Manager - schedule** policy, results in a real configuration change. The rest of the policy changes logged for this event are internal parameter ID changes. To check what the changes are, you can use the **Reports.vAuditEventsForPolicyEditAndDuplicate** view of the SophosSecurity database, as described in Create a report containing policy changes in an XML format (page 17).

9.6 System events

The following system events are audited:

- Enable auditing
- Disable auditing

10 Sophos Auditing data fields

The following database views, or data sources, are available for Sophos Auditing:

- Reports.vAuditEventsAll
- Reports.vAuditEventsForPolicyEditAndDuplicate

The data fields available for each of these data sources are listed below. All date-time columns are returned in UTC in the format "yyyy-mm-dd hh:mi:ss" (24 hours). The fields common to both views are highlighted in bold

Reports.vAuditEventsAll

The **Reports.vAuditEventsAll** database view contains the full list of audit events and most of the audit information.

Data field	Data type	Description
EventId	integer	A unique numeric ID of the event.
Timestamp	datetime	The time when the action logged in the event took place.
Action	nvarchar(128)	The action logged in the event, for example, Create, Edit, Rename, Assign, Delete.
TargetType	nvarchar(128)	The type of the object or configuration setting modified by the action, for example, Group, Computer, Policy, Role.
TargetSubType	nvarchar(128)	The subtype of the object or setting modified by the action, where applicable. For example, the name of the modified policy, such as Anti-virus and HIPS or Data control.
TargetName	nvarchar(4000)	The name of the object or setting modified by the action, for example, the user-defined name of the policy or group.
ParameterType	nvarchar(128)	The type of the new setting or object assigned to the target. For example, for Action="Rename" and TargetType="Policy", ParameterType="New name". For Action="Assign" and TargetType="Computer", ParameterType="Group".
ParameterValue	nvarchar(4000)	The value of the new setting or object, for example, the new user-defined name of the policy, or the new group the computer has been assigned to.

Data field	Data type	Description
Result	nvarchar(128)	The result of the action; has the value "Success" or "Failure".
UserName	nvarchar(256)	The name of the user who carried out the action.
HostName	nvarchar(256)	The name of the computer from which the user carried out the action.
HostIPAddress	nvarchar(48)	The IP address of the computer from which the user carried out the action. If network connections between the server and Enterprise Console are made over IPv6, then IPv6 addresses will be recorded. Otherwise, IPv4 addresses will be recorded.
ActionId	integer	A unique numeric ID of the action.
TargetTypeId	integer	A unique numeric ID of the target type.
TargetSubTypeId	integer	A unique numeric ID of the target subtype.
ParameterTypeId	integer	A unique numeric ID of the parameter type.
SubEstateId	integer	A unique numeric ID of the user's sub-estate.
ResultId	integer	A unique numeric ID of the result, 1 (success) or 0 (failure).
UserSid	nvarchar(128)	The user's security identifier .

Reports.vAuditEventsForPolicyEditAndDuplicate

The **Reports.vAuditEventsForPolicyEditAndDuplicate** database view contains information about policy changes.

Data field	Data type	Description
EventId	integer	A unique numeric ID of the event.
Timestamp	datetime	The time when the action logged in the event took place.
Action	nvarchar(128)	The action logged in the event.
Result	nvarchar(128)	The result of the action; has the value "Success" or "Failure".

Data field	Data type	Description
PolicyType	nvarchar(128)	The type of the policy changed by the action, for example, Anti-virus and HIPS or Web control.
PolicyName	nvarchar(4000)	The user-defined name of the policy.
PolicyContent	XML	The snippet of the policy configuration changes, in XML format.
UserName	nvarchar(256)	The name of the user who carried out the action.

11 Troubleshooting

When Sophos Auditing fails, an event is logged in the Windows Application Event Log with the source "Sophos Auditing". This usually happens when there is a database connectivity problem.

12 Appendix: Numeric IDs of the data field values

The following tables show unique numeric IDs of some of the Sophos Auditing data field values.

We recommend using these numeric IDs instead of string values if you want to bind any external logic to exported audit data. This will help to avoid potential compatibility issues should any string values change in a future release of Sophos Enterprise Console.

Data field	Data field value	Numeric ID
Action	Unknown	0
	Create	1
	Delete	2
	Duplicate	3
	Move	4
	Rename	5
	Add to	6
	Remove from	7
	Edit	8
	Log on	9
	Update	10
	Acknowledge	11
	Reset	12
	Assign	13
	Protect	14
	Scan	15
	Clean up	16
	Comply	17

Data field	Data field value	Numeric ID
TargetType	Unknown	0
	Group	1
	Role	2
	Policy	3
	Computer	4
	Sub-estate	5
	AD synchronization point	6
	Report	7
	Update manager	8
	Configuration	9
TargetSubType for TargetType=Policy	Legacy updating	1
	Anti-virus and HIPS	2
	Firewall	4
	Application control	7
	NAC	8
	Update Manager - upstream	9
	Update Manager - downstream	10
	Update Manager - general	11
	Update Manager - subscription	12
	Update Manager - schedule	13
	Data control	15
	Device control	16
	Software subscription	17
	Updating	18
	Tamper protection	19
	Web control	22
	Exploit prevention	30
TargetSubType for TargetType=Configuration	Unknown	0
	Dashboard	1
	Email alerts	2
	Purge	3
	Auditing	4

Data field	Data field value	Numeric ID
ParameterType	None	0
	New name	1
	New location	2
	Group	3
	User/Group	4
	Right	5
	Computer	6
	Alert	7
	Error	8
	Software update alert	9
	Configuration value	10
Result	Pending	0
	Success	1
	Failure	2

13 Technical support

You can find technical support for Sophos products in any of these ways:

- Visit the Sophos Community at community.sophos.com/ and search for other users who are experiencing the same problem.
- Visit the Sophos support knowledge base at www.sophos.com/en-us/support.aspx.
- Download the product documentation at www.sophos.com/en-us/support/documentation.aspx.
- Open a ticket with our support team at https://secure2.sophos.com/support/contact-support/support-query.aspx.

14 Legal notices