ADVANCED SECURITY AUDIT POLICY

The nine basic audit policies under **Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Audit Policy** allow you to configure security audit policy settings for broad sets of behaviors, some of which generate many more audit events than others. An administrator has to review all events that are generated, whether they are of interest or not.

In Windows Server 2008 R2 and Windows 7, administrators can audit more specific aspects of client behavior on the computer or network, thus making it easier to identify the behaviors that are of greatest interest. For example, in **Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Audit Policy**, there is only one policy setting for logon events, **Audit logon events**. In **Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\System Audit Policies**, you can instead choose from eight different policy settings in the **Logon/Logoff** category. This provides you with more detailed control of what aspects of logon and logoff you can track.

A default domain policy is automatically generated when a new domain is created. In this section, we will edit the default domain policy and add an advanced security audit policy setting that audits when a user either successfully or unsuccessfully logs on to a computer in the CONTOSO domain.

To configure, apply, and validate an advanced domain logon audit policy setting, you must:

- Configure an advanced domain logon policy setting.
- Ensure that Advanced Audit Policy Configuration settings are not overwritten.
- Update Group Policy settings.
- Verify that the advanced logon security audit policy settings were applied correctly.

To configure an advanced domain logon audit policy setting

1. Log on to CONTOSO-SRV as a member of the local **Administrators** group.
2. Click **Start**, point to **Administrative Tools**, and then click **Group Policy Management**.
3. In the console tree, double-click **Forest: contoso.com**, double-click **Domains**, and then double-click **contoso.com**.
4. Right-click **Default Domain Policy**, and then click **Edit**.
5. Double-click **Computer Configuration**, double-click **Policies**, and then double-click **Windows Settings**.
6. Double-click **Security Settings**, double-click **Advanced Audit Policy Configuration**, and then double-click **System Audit Policies**.
7. Double-click **Logon/Logoff**, and then double-click **Logon**.

8. Select the **Configure the following audit events** check box, select the **Success** check box, select the **Failure** check box, and then click **OK**.

When you use Advanced Audit Policy Configuration settings, you need to confirm that these settings are not overwritten by basic audit policy settings. The following procedure shows how to prevent conflicts by blocking the application of any basic audit policy settings.

To ensure that Advanced Audit Policy Configuration settings are not overwritten

---

1. On CONTOSO-SRV, click **Start**, point to **Administrative Tools**, and then click **Group Policy Management**.
2. In the console tree, double-click **Forest: contoso.com**, double-click **Domains**, and then double-click **contoso.com**.
3. Right-click **Default Domain Policy**, and then click **Edit**.
4. Double-click **Computer Configuration**, double-click **Policies**, and then double-click **Windows Settings**.
5. Double-click **Security Settings**, and then click **Security Options**.
6. Double-click **Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings**, and then click **Define this policy setting**.
7. Click **Enabled**, and then click **OK**.

Before you can verify the functionality of advanced security audit policy settings in the contoso.com domain, you will log on to CONTOSO-CLNT as the domain administrator of the contoso.com domain and ensure that the Group Policy settings have been applied.

To update Group Policy settings

---

1. Log on to CONTOSO-CLNT as CONTOSO\Administrator.
2. Click **Start**, point to **All Programs**, click **Accessories**, right-click **Command Prompt**, and then click **Run as administrator**.
3. If the **User Account Control** dialog box appears, confirm that the action it displays is what you want, and then click **Yes**.
4. Type **gpupdate**, and then press ENTER.

After the Group Policy settings have been applied, you can verify that the audit policy settings were applied correctly.

To verify that the advanced logon security audit policy settings were applied correctly

---

1. Log on to CONTOSO-CLNT as CONTOSO\Administrator.
2. Click **Start**, point to **All Programs**, click **Accessories**, right-click **Command Prompt**, and then click **Run as administrator**.

3. If the **User Account Control** dialog box appears, confirm that the action it displays is what you want, and then click **Yes**.
4. Type **auditpol.exe /get /category:***, and then press ENTER.
5. Verify that **Success**, **Failure**, or **Success and Failure** are shown to the right of **Logon**.

Step 3: Creating and verifying an audit policy that provides the reason for object access

---

One of the most common auditing needs is to track access to a particular file or folder. For example, you might need to identify an activity such as a user writing to a file that he or she should not have had access to. By enabling "reason for access" auditing, not only will you be able to track this type of activity, but you will also be able to identify the exact access control entry that allowed the undesired access, which can significantly simplify the task of modifying access control settings to prevent similar undesired object access in the future.

To configure, apply, and validate a reason for object access policy, you must:

- Configure the file system audit policy.
- Enable auditing for a file or folder.
- Enable the handle manipulation audit policy.
- Ensure that Advanced Audit Policy Configuration settings are not overwritten.
- Update Group Policy settings.
- Review and verify reason for access auditing data.

To configure the file system audit policy

---

1. Log on to CONTOSO-SRV as a member of the local **Administrators** group.
2. Click **Start**, point to **Administrative Tools**, and then click **Group Policy Management**.
3. In the console tree, double-click **Forest: contoso.com**, double-click **Domains**, and then double-click **contoso.com**.
4. Right-click **Default Domain Policy**, and then click **Edit**.
5. Double-click **Computer Configuration**, double-click **Policies**, and then double-click **Windows Settings**.
6. Double-click **Security Settings**, double-click **Advanced Audit Policy Configuration**, and then double-click **System Audit Policies**.
7. Double-click **Object Access**, and then double-click **File System**.
8. Select the **Configure the following events** check box, and then select the **Success**, **Failure**, or both **Success** and **Failure** check boxes.
9. Click **OK**.

The file system audit policy is only used to monitor objects for which auditing SACLs have been configured. The following procedure shows how to configure auditing for a file or folder.

To enable auditing for a file or folder

---

1. Log on to CONTOSO-CLNT as a member of the local **Administrators** group.
2. Create a new folder or .txt document.
3. Right-click the new object, click **Properties**, and click the **Security** tab.
4. Click **Advanced**, and then click the **Auditing** tab.
5. If the **User Account Control** dialog box appears, confirm that the action it displays is what you want, and then click **Yes**.
6. Click **Add**, type a user name or computer name in the format **contoso\user1**, and then click **OK**.
7. In the **Auditing Entries for** dialog box, select the permissions that you want to audit, such as **Full Control** or **Delete**.
8. Click **OK** four times to complete configuration of the object SACL.

In Windows 7 and Windows Server 2008 R2, the reason why someone has been granted or denied access is added to the open handle event. This makes it possible for administrators to understand why someone was able to open a file, folder, or file share for a specific access. To enable this functionality, the handle manipulation audit policy also needs to be enabled so that success events record access attempts that were allowed and failure events record access attempts that were denied.

To enable the handle manipulation audit policy

---

1. Log on to CONTOSO-SRV as a member of the local **Administrators** group.
2. Click **Start**, point to **Administrative Tools**, and then click **Group Policy Management**.
3. In the console tree, double-click **Forest: contoso.com**, double-click **Domains**, and then double-click **contoso.com**.
4. Double-click the **Finance** OU, right-click **Finance Audit Policy**, and click **Edit**.
5. Double-click **Computer Configuration**, double-click **Policies**, and then double-click **Windows Settings**.
6. Double-click **Security Settings**, double-click **Advanced Audit Policy Configuration**, and then double-click **System Audit Policies**.
7. Double-click **Object Access**, right-click **Handle Manipulation**, and click **Properties**.
8. Select the **Configure the following audit events** check box, select the **Success** and **Failure** check boxes, and then click **OK**.

After you have created this audit policy, confirm that these advanced audit policy settings cannot be overwritten. For more information, see the "To ensure that Advanced Audit Policy Configuration settings are not overwritten" procedure in the Step 2: Creating and verifying an advanced audit policy section.

Then apply the Group Policy updates by using the "To update Group Policy settings" procedure in the Step 2: Creating and verifying an advanced audit policy section.

After the updated Group Policy settings have been applied, be sure to log on to and log off from CONTOSO-CLNT and complete some tasks that will generate reason for object access events. Once you have completed these steps, you can review the auditing data that provides the reason for access.

To review reason for access auditing data

---

1. On CONTOSO-CLNT, click **Start**, point to **Administrative Tools**, and then click **Event Viewer**.
2. Click **Windows Logs**, and then click **Security**.
3. In the **Actions** pane, click **Clear Log**.
4. Find the file or folder that you configured in the domain-level object access procedure, and modify the file or folder by using the permissions that you configured for the user account.
5. Go back to **Event Viewer**, and in the **Actions** pane, click **Refresh**.
6. In the **Event ID** column, click the event or events titled **4656**, scroll down to the **Access Request Information** section, and confirm the permissions that were used to perform the task.

Step 4: Creating and verifying a global object access policy

A global object access audit policy can be used to enforce object access audit policy for a computer, file share, or registry without having to configure and propagate conventional SACLs. Configuring and propagating SACLs is a more complex administrative task and is difficult to verify, particularly if you need to verify to an auditor that security policy is being enforced. By using a global object access audit policy, you can enforce a security policy such as "Log all administrative Write activity on servers containing Finance information" and verify that critical assets are being protected.

In this case, you will be auditing any changes made to registry keys by members of a specified group rather than changes made to file system objects.

To configure, apply, and validate a global object access audit policy, you must:

- Configure a domain global object access audit policy.
- Ensure that Advanced Audit Policy Configuration settings are not overwritten.
- Update Group Policy settings.
- Confirm that global object access auditing is taking place.

To configure a domain global object access audit policy

---

1. Log on to CONTOSO-SRV as a member of the local **Administrators** group.
2. Click **Start**, point to **Administrative Tools**, and then click **Group Policy Management**.
3. In the console tree, double-click **Forest: contoso.com**, double-click **Domains**, and then double-click **contoso.com**.
4. Right-click **Default Domain Policy**, and then click **Edit**.
5. Double-click **Computer Configuration**, double-click **Policies**, and then double-click **Windows Settings**.
6. Double-click **Security Settings**, double-click **Advanced Audit Policy Configuration**, and then double-click **System Audit Policies**.
7. Double-click **Object Access**, and then double-click **Registry**.
8. Select the **Configure the following events** check box, select the **Success** and **Failure** check boxes, and then click **OK**.
9. Double-click **Global Object Access Policies**, and then double-click **Registry**.
10. Select the **Define this policy setting** check box, and click **Configure**.
11. In the **Advanced Security Settings for Registry SACL** box, click **Add**.
12. Type a user name or computer name in the format **contoso\user1**, **user1@contoso.com**, or **CONTOSO-CLNT**, and click **OK**.
13. In the **Auditing Entry for Global Registry SACL** box, select the **Successful** or **Failed** activities for which you want to log audit entries—for example, **Create Subkey**, **Delete**, or **Read**.
14. Click **OK** three times to complete the audit policy configuration.

After you have created the audit policy, confirm that these advanced audit policy settings cannot be overwritten. For more information, see the "To ensure that Advanced Audit Policy Configuration settings are not overwritten" procedure in the Step 2: Creating and verifying an advanced audit policy section.

Then apply the Group Policy updates by using the "To update Group Policy settings" procedure in the Step 2: Creating and verifying an advanced audit policy section. After the updated Group Policy settings have been applied, log on to and log off from CONTOSO-CLNT.

To verify that the global object access policy has been applied

---

1. Open Registry Editor, and create and modify one or more registry settings.
2. Delete one or more of the registry settings that you created.
3. Open Event Viewer, and confirm that your activities resulted in audit events, even though you did not set explicit auditing SACLs on the registry settings that you created, modified, and deleted.

Step 5: Creating and verifying additional advanced audit policies

---

Now that you have created, applied, and validated the three basic types of advanced security audit policy settings, continue to identify and test additional advanced security audit policy settings by using the basic procedures outlined in the previous sections.

To identify additional settings of potential interest to your organization, review the information in What's New in Windows Security Auditing.

Additional information is available in **Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\System Audit Policies** by right-clicking individual settings, clicking **Properties**, and clicking the **Explain** tab.

As you apply and test additional settings, consider how the audit event data that is generated can help you create a more secure network. In particular, consider the following:

- Is the information provided by these audit events useful?
- Is sufficient information provided by the audit data?
- Is too much information provided by the audit data?
- How can I adjust these audit policy settings to get only the information that I need?

Security auditing is a critical and essential tool to help you ensure that your network assets are secure. You should spend as much time as necessary to explore and understand the new advanced security audit policy settings in Windows 7 and Windows Server 2008 R2.

Managing per-user auditing in Windows 7 and Windows Server 2008 R2

Security audit policy settings in Windows 7 and Windows Server 2008 R2 can be configured and used only on a per-computer basis, not a per-user basis. However, there are several ways to apply audit settings to specific users:

- Where available, configure the advanced security permissions on the object being audited so that the audit policy applies only to a specific group. For example, if you want the **Object Access** policy setting to apply to a file or folder, you can configure permissions on the file or folder so that object access is only tracked for the individuals or groups you specify. The procedure titled "To enable auditing for a file or folder" earlier in this document describes how to complete this task.
- Define and deploy per-user audit settings by using an audit policy text file, a logon script, and the Auditpol.exe command-line tool.

  Important

  Per-user auditing based on logon scripts can only be applied to individual users, not groups. You cannot use logon scripts to exclude subcategories or categories of audit

policy settings for administrators.

The following procedure describes how to create an audit policy text file that can be deployed by using a logon script. For more information about using logon scripts to deploy an audit policy, see article 921469 in the Microsoft Knowledge Base (http://go.microsoft.com/fwlink/?LinkID=82447).

To create an audit policy text file

---

1. At a command prompt, type **auditpol /set /user:***securityprincipalname***/category:"***subcategoryname***" /include /***Success or Failure***:enable** to add a per-user audit setting. Repeat this step for each audit policy subcategory and user or group that you want to add to your audit policy text file.

   Note

   To obtain a list of possible audit settings in report format, open a Command Prompt window, type **auditpol /list /subcategory:* /r**, and press ENTER. For more information about using Auditpol, see Auditpol set and Auditpol list.

2. At a command prompt, type **auditpol /backup /file:** *auditpolicyfilename***.txt** to export the policy.
3. Format your policy by opening *auditpolicyfilename.txt* and removing all lines except the first line of text and the per-user audit lines of text.

   Note

   Per-user audit policy text will be in the form: *ComputerName,S-1-XXXX,SubcategoryName,GUID,TextIncludeSettings,TextExcludeSettings,#*. System settings will be in the form: *ComputerName,System,SubcategoryName,GUID,TextAuditSettings,#*. Also, be sure to remove the last six lines, which contain audit option settings.

4. When you have finished creating your file, on the **File** menu, click **Save As**, and confirm that **ANSI** is selected in the **Encoding** list. Click **OK**.
5. At a command prompt, type **auditpol /restore /file:** *auditpolicyfilename***.txt**, and press ENTER to confirm that the desired audit settings are configured. Type **auditpol /list /user**, and press ENTER to list any users with per-user audit settings.
6. Copy the *auditpolicyfilename.txt* file to the Netlogon share of the domain controller that holds the primary domain controller (PDC) emulator role in the domain.

   Important

   Do not import audit policies containing per-user auditing settings directly into a Group Policy object (GPO). When per-user audit settings are deployed through Group Policy and not through logon scripts as described in this procedure, this can cause unexpected

levels of failure events to appear in your security audit logs.

Optional section: Roll back security audit policy from Advanced Audit Policy to basic audit policy

---

Applying advanced audit policy settings replaces any comparable basic security audit policy settings. If you subsequently change the advanced audit policy setting to **Not configured**, you will need to complete the following steps to restore the original basic security audit policy settings:

1. Set all Advanced Audit Policy sub-categories to **Not configured**.
2. Delete all audit.csv files from the %SYSVOL% folder on the domain controller.
3. Reconfigure and apply the basic audit policy settings.

Unless you complete all of these steps, the basic audit policy settings will not be restored.