Knowledge Base

HOW TO: Use Group Policy to Audit Registry Keys in Windows 2000

PSS ID Number: 315416

Article Last Modified on 9/19/2003

The information in this article applies to:

- Microsoft Windows 2000 Server
- Microsoft Windows 2000 Advanced Server
- Microsoft Windows 2000 Professional

This article was previously published under Q315416

IN THIS TASK

- SUMMARY
-
  - How to Create a Group Policy Object
  - How to Enable Auditing in Group Policy
  -
    - How to Enable Auditing on a Computer That Is a Member of a Domain
    - How to Enable Auditing on a Computer That Is Not a Member of a Domain
  - How to Audit a Registry Key
  - How to Use a Security Template to Audit Registry Keys
  -
    - How to Create a Security Template
    - How to Apply the Security Template
  - Troubleshooting
- REFERENCES

SUMMARY

This article describes how to use Group Policy to configure auditing of Windows registry keys.

back to the top

How to Create a Group Policy Object

To create a Group Policy object (GPO) that you can use to enable auditing in a domain, follow these steps:

1. Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**.
2. Right-click your domain, and then click **Properties**.
3. Click the **Group Policy** tab, and then click **New**.
4. Type the name that you want to use for this policy (for example, `Enable auditing policy`), and then press ENTER.
5. Click **Properties**, and then click the **Security** tab.
6. Click to clear the **Apply Group Policy** check box for the security groups that you want to prevent from having this policy applied.
7. Click the select the **Apply Group Policy** check box for the groups to which you want to apply this policy, and then click **OK**.

back to the top

How to Enable Auditing in Group Policy

If auditing is not already enabled, you must enable it. In a domain, enable auditing in a GPO that is linked to the domain. On either a server or a workstation that is not a member of the domain, enable auditing in a local GPO.

back to the top

How to Enable Auditing on a Computer That Is a Member of a Domain

1. Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**.
2. Right-click your domain, and then click **Properties**.
3. Click the **Group Policy** tab, click the group policy object that you want to use, and then click **Edit**.
4. Under **Computer Configuration**, click to expand **Windows Settings**, click to expand **Security Settings**, click to expand **Local Policies**, and then click **Audit Policy**.
5. Double-click **Audit object access**.
6. Click to select the **Define these policy settings** check box, click to select the **Success** check box, click to select the **Failure** check box, and then click **OK**.

   NOTE: The Audit object access policy setting is sufficient to enable auditing for the Windows registry.
7. Quit the Group Policy snap-in, and then click **Close**.

back to the top

How to Enable Auditing on a Computer That Is Not a Member of a Domain

1. Click **Start**, and then click **Run**.
2. In the **Open** box, type `gpedit.msc`, and then click **OK**.

3. Under **Computer Configuration**, click to expand **Windows Settings**, click to expand **Security Settings**, click to expand **Local Policies**, and then click **Audit Policy**.
4. Double-click **Audit object access**.
5. Click to select the **Define these policy settings** check box, click to select the **Success** check box, click to select the **Failure** check box, and then click **OK**.

   NOTE: The Audit object access policy is sufficient to enable auditing for the Windows registry.
6. Quit the Group Policy snap-in.

back to the top

How to Audit a Registry Key

WARNING: If you use Registry Editor incorrectly, you may cause serious problems that may require you to reinstall your operating system. Microsoft cannot guarantee that you can solve problems that result from using Registry Editor incorrectly. Use Registry Editor at your own risk.

1. Click **Start**, and then click **Run**.
2. In the **Open** box, type `regedt32`, and then click **OK**.
3. Locate and click the registry key that you want to audit, for example:

   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
4. On the **Security** menu, click **Permissions**.
5. Click **Advanced**, click the **Auditing** tab, and then click **Add**.
6. Click the account whose access to this registry key you want to audit, for example, **Authenticated Users**, and then click **OK**.
7. Click to select the following check boxes under both **Successful** and **Failed**:

   Set Value
   Create Subkey
8. Click **OK**, and then click **OK**.

   You may receive the following message:

   > The current Audit Policy for this computer does not have auditing turned on. If this computer gets audit policy from the domain, please ask a domain administrator to turn on auditing using Group Policy Editor. Otherwise, use the Local Computer Policy Editor to configure the audit policy locally on this computer.

   If auditing is not enabled, you must enable it by following the steps in the How to Enable Auditing in Group Policy section of this article.
9. Click **OK**, and then click **OK**.
10. Quit Registry Editor.

Audit events are displayed in the Security log of Event Viewer.

back to the top

How to Use a Security Template to Audit Registry Keys

You can also use a security template to audit registry keys. To configure the audit policy, either create a custom security template or modify an existing template, and then use Group Policy to apply this template to multiple computers in a domain or an organizational unit.

back to the top

How to Create a Security Template

To create a new security template or to modify an existing template, follow these steps:

1. Click **Start**, and then click **Run**.
2. In the **Open** box, type `mmc`, and then click **OK**.
3. On the **Console** menu, click **Add/Remove Snap-in**.
4. Click **Add**, and then click **Security Template**.
5. Click **Add**, click **Close**, and then click **OK**.
6. Under the Console root folder, click to expand **Security Templates**.
7. Click to expand ***drive*:\WINNT\Security\Templates**, where *drive* is the drive on which Windows is installed.
8. Do one of the following steps:
   - If you want to modify an existing template, click to expand the template that you want to use, for example, **hisecws** (high-security workstation template).

     -or-
   - If you want to create a new security template, follow these steps:
     a. Right-click ***drive*:\WINNT\Security\Templates**, and then click **New Template**.
     b. Type a name for the template in the **Template name** box, and then click **OK**.
     c. Click to expand the new template that you created.
9. Right-click **Registry**, and then click **Add Key**.
10. In the **Registry** list, click to expand the registry key that you want to use, for example:

    HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
11. Click **Advanced**, click the **Auditing** tab, and then click **Add**.
12. Click the account whose access to this registry key you want to audit, for example, **Authenticated Users**, and then click **OK**.
13. In the **Access** list, click to select the check boxes under **Successful** and under **Failed** for the type of access that you want to audit for either the selected user or the selected security group, and then click **OK**.

For example, click to select the **Set Value** check boxes under both **Successful** and **Failed**.

14. Click **OK**.

    If you receive the following message, click **OK**:

    The current Audit Policy for this computer does not have auditing turned on. If this computer gets audit policy from the domain, please ask a domain administrator to turn on auditing using Group Policy Editor. Otherwise, use the Local Computer Policy Editor to configure the audit policy locally on this computer.

15. Click **OK**, and then click **OK**.
16. Click to expand **Local Policies**, and then click **Audit Policy**.
17. In the **Policy** list, double-click **Audit object access**.
18. Click to select the **Define these policy settings** check box, click to select the **Success** check box, click to select the **Failure** check box, and then click **OK**.

    NOTE: The Audit object access policy setting is sufficient to enable auditing for the Windows registry.

19. Quit the Security Templates snap-in.
20. If a **Save Security Templates** dialog box is displayed, click **Yes** to save the custom security template that you have created.

back to the top

How to Apply the Security Template

Use Group Policy to apply the security template that contains the audit policy that you configured. To do so, follow these steps:

1. Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**.
2. Do one of the following steps:
   - If you want to apply the security template to the entire domain, right-click the domain, and then click **Properties**.

     -or-

   - If you want to apply the security templates to an organizational unit, click to expand the domain, right-click the organizational unit, and then click **Properties**.
3. Create a GPO to use to apply the security template. To do so:
   a. Click **New**.
   b. Type a name for the GPO in the **New Group Policy Object** box (for example, `Apply Audit Policy Security Template`), and then press ENTER.
4. In the **Group Policy Object Links** list, click the GPO that you want, and then click **Edit**.
5. Under **Computer Configuration**, click to expand **Windows Settings**, right-click **Security Settings**, and then click **Import Policy**.
6. Click the security template that you created, click to select the **Clear this database before importing** check box, and then click **Open**.

   NOTE: When the **Clear this database before importing** check box is selected, all of the security settings in the GPO are replaced with those of the security template that you import.

7. Quit the Group Policy snap-in, and then click **Close**.
8. Quit Active Directory Users and Computers.

back to the top

Troubleshooting

After you configure auditing, the service may not work. This behavior can occur for any of the following reasons:

- A site, a domain, or an organizational unit policy setting overrides the audit policy that you configured. To troubleshoot this issue, follow these steps:
  1. Click **Start**, and then click **Run**.
  2. In the **Open** box, type `gpedit.msc`, and then click **OK**.
  3. Under **Computer Configuration**, click to expand **Windows Settings**, click to expand **Security Settings**, click to expand **Local Policies**, and then click **Audit Policy**.
  4. In the **Policy** pane, view the item in the **Effective Setting** column of the policy that you want to use.

     If the effective setting of the policy is **No auditing**, a higher-level GPO may be overriding the audit policy setting that you configured. To confirm this behavior, view the higher-level GPO items that are linked to either the organizational unit or to the domain for possible conflicts.
  5. Click to select the **Define these policy settings** check box, click to select the **Success** check box, click to select the **Failure** check box, and then click **OK**.

     NOTE: The Audit object access policy setting is sufficient to enable auditing for the Windows registry.
  6. Quit the Group Policy snap-in.
- A GPO that overrides the audit policy setting has a higher priority. To troubleshoot this issue, follow these steps:
  1. Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**.
  2. In the console tree, right-click your domain, and then click **Properties**.
  3. Click the **Group Policy** tab.

     View the **Group Policy Objects Links** list. Items that are higher in the list override other lower-level items.
  4. If the GPO that contains your audit policy setting is listed below a higher-priority GPO item that turns off auditing, do one of the following steps:
     - Click the GPO that contains the audit policy setting that you want to use, and then click **Up** to move it above the higher-priority item in the list.

WARNING: Ensure that other settings in your GPO do not conflict with the settings in the GPO items that are listed below it.

-or-

- Edit the GPO items that are listed above the GPO that contains the audit policy setting to remove conflicting policy settings.

  NOTE: You may want to combine the audit settings from one GPO with those of a higher-level GPO to resolve the audit policy conflict and to reduce the number of GPO items.

5. When you are finished, click **OK**, and then click **Exit** on the **Console** menu.

- The site, the domain, or the organizational unit policy setting that contains the audit policy setting has not replicated to other computers. To resolve this issue, use the Secedit.exe command-line utility to force Group Policy to be refreshed. For additional information about using Secedit, click the article number below to view the article in the Microsoft Knowledge Base:

  227302 Using SECEDIT to Force a Group Policy Refresh Immediately

back to the top

REFERENCES

For additional information about using Group Policy, click the article numbers below to view the articles in the Microsoft Knowledge Base:

214752 How to Add Custom Registry Settings to Security Configuration Editor

220862 Local Group Policy Settings Do Not Take Effect

227448 Using Secedit.exe to Force Group Policy to Be Applied Again

For additional information about auditing, click the article numbers below to view the articles in the Microsoft Knowledge Base:

248260 How to Enable Local Security Auditing in Windows 2000

234926 Windows 2000 Security Templates Are Incremental

299475 Windows 2000 Security Event Descriptions (Part 1 of 2)

301677 Windows 2000 Security Event Descriptions (Part 2 of 2)

300549 HOW TO: Enable and Apply Windows Security Auditing

back to the top

Keywords: kbHOWTOmaster KB315416
Technology: kbwin2000AdvServ kbwin2000AdvServSearch kbwin2000Pro kbwin2000ProSearch kbwin2000Search kbwin2000Serv kbwin2000ServSearch kbWinAdvServSearch

---