**Introduction**

**Source:** [**file:///C:/Program%20Files%20%28x86%29/SolarWinds/PermissionsAnalyzerTool/PermissionsAnalyzer.htm**](file:///C:/Program%20Files%20%28x86%29/SolarWinds/PermissionsAnalyzerTool/PermissionsAnalyzer.htm)

SolarWinds Permissions Analyzer for Active Directory allows a domain administrator to break down and analyze effective permissions for a group or user accessing a share, folder, or file over the network. It allows you to select a share, folder, or file and a user or group and view the NTFS (New Technology File System) permissions by breaking them down by which permissions are provided by which group memberships and direct grants. The membership checks will span multiple domains if necessary. The tool takes into account local group memberships as well. All of this data will be combined to show the effective NTFS permissions. The same information will be provided for the share permissions. The Share and NTFS permissions are then combined to show the total effective permissions for the selected user or group on the specified share, folder, or file object.  
  
**For support,** [**click to visit the SolarWinds Permissions Analyzer for Active Directory forum on thwack.**](http://thwack.com/forums/54/free-tools/209/permissions-analyzer-for-active-directory/)

**Table of Contents**

[Requirements](file:///C:\Program%20Files%20%28x86%29\SolarWinds\PermissionsAnalyzerTool\PermissionsAnalyzer.htm#Requirements)  
[Installing and Running SolarWinds Permissions Analyzer for Active Directory](file:///C:\Program%20Files%20%28x86%29\SolarWinds\PermissionsAnalyzerTool\PermissionsAnalyzer.htm#Installing)  
[Using Active Domain Controllers](file:///C:\Program%20Files%20%28x86%29\SolarWinds\PermissionsAnalyzerTool\PermissionsAnalyzer.htm#ActiveDomainControllers)  
[Impersonating Privilege on a Domain Controller](file:///C:\Program%20Files%20%28x86%29\SolarWinds\PermissionsAnalyzerTool\PermissionsAnalyzer.htm#ImpersonatingPrivilege)  
[Configuring SolarWinds Permissions Analyzer for Active Directory](file:///C:\Program%20Files%20%28x86%29\SolarWinds\PermissionsAnalyzerTool\PermissionsAnalyzer.htm#Configuring)  
[Using SolarWinds Permissions Analyzer for Active Directory](file:///C:\Program%20Files%20%28x86%29\SolarWinds\PermissionsAnalyzerTool\PermissionsAnalyzer.htm#Using)  
[Sharing SolarWinds Permissions Analyzer for Active Directory](file:///C:\Program%20Files%20%28x86%29\SolarWinds\PermissionsAnalyzerTool\PermissionsAnalyzer.htm#Sharing)

**Requirements**

|  |  |
| --- | --- |
| **Need** | **Item** |
| Operating System | Install on a 32-bit or 64-bit edition of one of the following operating systems:   * Microsoft Windows XP SP2 or later * Microsoft Windows Vista Business and Ultimate Editions * Microsoft Windows Server 2003 SP1 or later * Microsoft Windows 2000 SP4 or later * Microsoft Windows Server 2008 * Microsoft Windows 7 |
| .NET Framework | Microsoft .NET Framework 3.5 SP1 or later. |
| Hard Drive space | 50MB |

**Installing SolarWinds Permissions Analyzer for Active Directory**

You can modify the installation location and other settings using the SolarWinds Permissions Analyzer for Active Directory setup program.  
  
**Note:** The Windows user account used to install SolarWinds Permissions Analyzer for Active Directory must have administrator rights.

**To install SolarWinds Permissions Analyzer for Active Directory:**

1. Run the setup program (SolarWindsPermissionsAnalyzerTool.msi).
2. Complete the setup wizard, providing the appropriate information as necessary.

**Using Active Domain Controllers**

To allow the tool access to permission and security information, admin rights are needed for any paths that are being analyzed. Usually (but not always) the domain admin account has admin rights to local machines. The "active" domain controller account is used when accessing the specified path's local file system permissions and memberships. The "non-active" credentials are used when collecting membership information from active directory. The user may be a member of a group which, in turn, may be a member of another group, etc. Because one of those groups may originate from another domain, the tool checks the credential collection for a credential set that can be used on the remote domain to acquire information. If no match is found the active domain credentials are used. By allowing the IP address or device name the user is able to specify the exact domain controller they wish to use for a given domain.

**Impersonating Privilege on a Domain Controller**

In order to function properly, the SolarWinds Permissions Analyzer for Active Directory tool must impersonate a domain admin account. Impersonation is a privilege that that most workstations are granted by default. Most servers are granted this privilege by default as well, however domain controllers are generally not granted the impersonation privilege by default. Running this tool on a domain server will fail to access all the required security elements for analysis unless the following actions are taken to prevent issues. SolarWinds does not recommend running this tool on domain controllers, but if you are required to do so, complete the following procedure.

**To manually assign Impersonate a client after authentication:**

1. Click **Start > Programs > Administrative Tools > Domain Controller Security Policy.**
2. Click **Security Settings**.
3. Click **Local Policies**, and then click **User Rights Assignment**.
4. In the right pane, double-click **Impersonate a client after authentication**.
5. In the Security Policy Setting window, click **Define these policy settings**.
6. Click **Add**, and then click **Browse**.
7. In the Select Users or Groups window, select the account name or names (admin, user, etc), click **Add**, and then click **OK.**
8. Click **OK**, and then click **OK** again.
9. To enforce an update of computer policy use either the secedit or gpupdate commands depending upon your operating system

**Configuring SolarWinds Permissions Analyzer for Active Directory**

Complete the following procedure to configure SolarWinds Permissions Analyzer for Active Directory:  
  
**Notes:**

* The first time you start SolarWinds Permissions Analyzer for Active Directory, the settings window will be displayed automatically.
* Secure connections to Active Directory are not supported.

**To configure SolarWinds Permissions Analyzer for Active Directory:**

1. Start **SolarWinds Permissions Analyzer for Active Directory** from the SolarWinds Permissions Analyzer for Active Directory folder.
2. Click Settings (Settings).
3. Type the domain controller hostname or IP address in the **Domain Controller Name or IP Address** field.
4. Type the name of the domain in the **Domain Name** field. *Use the full name of the domain.*
5. Type the domain admin username and password in the associated fields, and then click **Add Domain Credential**.
6. ***If you want to add additional domain controllers,*** repeat **Steps 3** through **5**. Add a domain entry for each domain your query will need file, user, or parent information for.
7. Select one entry to be the **Active Domain**. This is the domain that is hosting the share, folder, or file you are finding permissions for.
8. Click **OK**.

**Using SolarWinds Permissions Analyzer for Active Directory**

The following procedure details how to use SolarWinds Permissions Analyzer for Active Directory.

**To use SolarWinds Permissions Analyzer for Active Directory:**

1. Type the user name or account name of the group or user you to view in the **Group or User** field.
2. Click the search button to the right of the **Group or User** field. This allows you to verify the account exists before performing the analysis.
3. Click **Browse**, and then navigate to the file or folder you want to view permissions for, and then click **OK**.
4. Click **Analyze**.

**Accessing Share Permissions**

To analyze Share Permissions, the tool needs to read the selected target machine's registry. This functionality is provided by Remote Registry Service on the target machine. If the service is not running, the tool will not be able to read the machine's registry and will not show Share Permissions.

**To enable Remote Registry Service on a target machine:**

1. Click Start, click Run, and type **services.msc**, and then press ENTER. Microsoft Management Console will start with the Services snap-in open.
2. In the console pane, right-click **Remote Registry** and click **Start**.

**Sharing SolarWinds Permissions Analyzer for Active Directory**

Complete the following procedure to send the SolarWinds Permissions Analyzer for Active Directory to a friend or colleague.

**To share SolarWinds Permissions Analyzer for Active Directory:**

1. Share This Tool: Click **Email, Facebook, or Twitter** buttons.
2. For email: Provide the email addresses in the appropriate fields within you email client, and then click **Send**.

**Legal**

Copyright 1995-2010 SolarWinds, Inc. All rights reserved worldwide. No part of this document may be reproduced by any means nor modified, decompiled, disassembled, published or distributed, in whole or in part, or translated to any electronic medium or other means without the written consent of SolarWinds. All right, title and interest in and to the software and documentation are and shall remain the exclusive property of SolarWinds and its licensors. SolarWinds Orion™, SolarWinds Permissions Analyzer for Active Directory™, and SolarWinds Toolset™ are trademarks of SolarWinds. SolarWinds® and the SolarWinds logo are registered trademarks of SolarWinds. Microsoft Windows Server, Windows Vista, and Windows XP are registered trademarks or trademarks of Microsoft Corporation in the United States and other countries. All other trademarks contained in this document and in the Software are the property of their respective owners.

SOLARWINDS DISCLAIMS ALL WARRANTIES, CONDITIONS OR OTHER TERMS, EXPRESS OR IMPLIED, STATUTORY OR OTHERWISE, ON SOFTWARE AND DOCUMENTATION FURNISHED HEREUNDER INCLUDING WITHOUT LIMITATION THE WARRANTIES OF DESIGN, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL SOLARWINDS, ITS SUPPLIERS OR ITS LICENSORS BE LIABLE FOR ANY DAMAGES, WHETHER ARISING IN TORT, CONTRACT OR ANY OTHER LEGAL THEORY EVEN IF SOLARWINDS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.