Legal Notice

The information in this publication is furnished for information use only, and does not constitute a commitment from Netwrix Corporation of any features or functions, as this publication may describe features or functionality not applicable to the product release or version you are using. Netwrix makes no representations or warranties about the Software beyond what is provided in the License Agreement. Netwrix Corporation assumes no responsibility or liability for the accuracy of the information presented, which is subject to change without notice. If you believe there is an error in this publication, please report it to us in writing.

Netwrix is a registered trademark of Netwrix Corporation. The Netwrix logo and all other Netwrix product or service names and slogans are registered trademarks or trademarks of Netwrix Corporation. Active Directory is a trademark of Microsoft Corporation. All other trademarks and registered trademarks are property of their respective owners.

Disclaimers

This document may contain information regarding the use and installation of non-Netwrix products. Please note that this information is provided as a courtesy to assist you. While Netwrix tries to ensure that this information accurately reflects the information provided by the supplier, please refer to the materials provided with any non-Netwrix product and contact the supplier for confirmation. Netwrix Corporation assumes no responsibility or liability for incorrect or incomplete information provided about non-Netwrix products.

© 2015 Netwrix Corporation.

All rights reserved.
Table of Contents

1. Introduction .................................................................................................................. 4
   1.1. Netwrix Effective Permissions Reporting Tool Overview ......................................... 4
2. System Requirements ........................................................................................................ 5
   2.1. Requirements for Target Environments ..................................................................... 5
   2.2. Requirements to Install Netwrix Effective Permissions Reporting Tool ..................... 5
       2.2.1. Hardware Requirements ..................................................................................... 5
       2.2.2. Software Requirements .................................................................................... 6
   2.3. Deployment Options ................................................................................................ 6
3. Configure Rights And Permissions .................................................................................. 7
   3.1. Configure Account to Scan Permissions on Active Directory Objects ......................... 7
   3.2. Configure Account to Scan Permissions on Shared Files and Folders ......................... 11
       3.2.1. Configure Account to Scan NTFS Permissions on Shared Files and Folders .......... 11
       3.2.2. Configure Account to Scan Share Permissions on Shared Files and Folders ........ 16
4. Start Using Netwrix Effective Permissions Reporting Tool ............................................ 17
5. See How Effective Permissions Are Reported ................................................................. 19
1. Introduction

This guide is intended for the first-time users of Netwrix Effective Permissions Reporting Tool. It can be used for evaluation purposes, therefore, it is recommended to read it sequentially, and follow the instructions in the order they are provided. After reading this guide you will be able to:

- Start network scanning
- See how effective permissions are reported

1.1. Netwrix Effective Permissions Reporting Tool Overview

Netwrix Effective Permissions Reporting Tool is a freeware product that collects data on effective permissions for selected network resources.

Netwrix Effective Permissions Reporting Tool checks effective permissions granted to a user or group by providing a report on who has access to what across your Active Directory domain or shared folders/files.
2. System Requirements

This section lists the requirements for the target environments that are going to be audited with Netwrix Effective Permissions Reporting Tool, and for the computer where the product is going to be installed.

2.1. Requirements for Target Environments

The table below provides the requirements for the target environments that can be audited with Netwrix Effective Permissions Reporting Tool:

<table>
<thead>
<tr>
<th>Target Environment</th>
<th>Supported Versions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Directory</td>
<td>• Domain Controllers OS versions: Windows Server 2008 and above</td>
</tr>
<tr>
<td>Files and Shares</td>
<td>• Desktop OS: Windows 7 (32 and 64-bit) and above</td>
</tr>
<tr>
<td></td>
<td>• Server OS: Windows Server 2008 and above</td>
</tr>
</tbody>
</table>

2.2. Requirements to Install Netwrix Effective Permissions Reporting Tool

This section provides the requirements for the computer where Netwrix Effective Permissions Reporting Tool is going to be installed.

Review the following for additional information:

- Hardware Requirements
- Software Requirements

2.2.1. Hardware Requirements

The table below lists the minimum hardware requirements for the Netwrix Effective Permissions Reporting Tool installation:

<table>
<thead>
<tr>
<th>Hardware Component</th>
<th>Minimum</th>
<th>Recommended</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor</td>
<td>Intel or AMD 32 bit, 2 GHz</td>
<td>Intel Core 2 Duo 2x or AMD 64 bit, 3GHz</td>
</tr>
<tr>
<td>RAM</td>
<td>512 MB</td>
<td>4 GB</td>
</tr>
</tbody>
</table>
2. System Requirements

---

### Hardware Requirements

<table>
<thead>
<tr>
<th>Component</th>
<th>Minimum</th>
<th>Recommended</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disk Space</td>
<td>50 MB physical disk space</td>
<td>100 MB physical disk space</td>
</tr>
<tr>
<td>Screen resolution</td>
<td>1024 x 768</td>
<td>Screen resolution recommended by your screen manufacturer.</td>
</tr>
</tbody>
</table>

---

### Software Requirements

The table below lists the minimum software requirements for the Netwrix Effective Permissions Reporting Tool installation:

<table>
<thead>
<tr>
<th>Component</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating system</td>
<td>• Desktop OS: Windows 7 (32 and 64-bit) and above</td>
</tr>
<tr>
<td></td>
<td>• Server OS: Windows Server 2008 R2 and above</td>
</tr>
<tr>
<td>Framework</td>
<td>• <a href="#">.Net Framework 3.5 SP1</a></td>
</tr>
</tbody>
</table>

---

### Deployment Options

The table below provides recommendations on how best to deploy Netwrix Effective Permissions Reporting Tool:

<table>
<thead>
<tr>
<th>Install on...</th>
<th>To check effective permissions for...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any computer that belongs to the monitored Active Directory domain or trusted domain</td>
<td>• Domains, OUs, etc.</td>
</tr>
<tr>
<td></td>
<td>• Domain users and groups</td>
</tr>
<tr>
<td></td>
<td>• Shared folders/files</td>
</tr>
</tbody>
</table>
3. Configure Rights And Permissions

To ensure successful network resources scanning, the account used by Netwrix Effective Permissions Reporting Tool to collect audit data from the monitored domain or shared folders/files must comply with the following requirements:

<table>
<thead>
<tr>
<th>To check the effective permissions for...</th>
<th>Required Permissions</th>
</tr>
</thead>
</table>
| Users, Active Directory objects (domains, OUs, etc.) | • Read all properties  
• List contents  
• Read permissions |
| Shared folders/files (based on share permissions) | • Member of the local Administrators group on the computer where the target shared folder/file is located. |
| Shared folders/files (based on the NTFS permissions) | • List folder contents  
• Read permissions |

Perform the following procedures:

- [Configure Account to Scan Permissions on Active Directory Objects](#)
- [Configure Account to Scan Permissions on Shared Files and Folders](#)

3.1. Configure Account to Scan Permissions on Active Directory Objects

Perform the following procedures:

- [To configure account to scan permissions on AD objects on pre-Windows Server 2012 versions](#)
- [To configure account to scan permissions on AD objects on Windows Server 2012 and above](#)
To configure account to scan permissions on AD objects on pre-Windows Server 2012 versions


2. In the Active Directory Users and Computers dialog, click View in the main menu and ensure that the Advanced Features are enabled.

3. Right-click the Active Directory object for which you want to be able to check effective permissions and select Properties. Select the Security tab and click Advanced.

4. In the Advanced Security Settings for <Object_Name> dialog, click Add.

5. In the Select user, Computer, Service account, or Group dialog, type the name of the account or group you want to be able to check effective permissions.

6. In the Permission Entry for <Object_Name> dialog, set the “Allow” flag next to the following options:
   - List contents
   - Read all properties
   - Read permissions
NOTE: Make sure that Apply onto is set to "This object and all descendant objects", and Apply these auditing entries to objects and/or containers within this container only is cleared.

To configure account to scan permissions on AD objects on Windows Server 2012 and above


2. In the Active Directory Users and Computers dialog, click View in the main menu and ensure that the Advanced Features are enabled.
3. Right-click the Active Directory object for which you want to check effective permissions and select Properties. Select the Security tab and click Advanced.

4. In the Advanced Security Settings for <object name> dialog, click Add.

5. In the Permission Entry for <Object_Name> dialog, click Select a Principal link.

6. In the Select user, Computer, Service account, or Group dialog, type the name of an account or group you want to be able to check effective permissions.
7. Set Type to "Allow" and Applies to to "This object and all descendant objects". Under Permissions, select the List Contents, Read all properties and Read permissions checkboxes.

3.2. Configure Account to Scan Permissions on Shared Files and Folders

Perform the following procedures:

- Configure Account to Scan NTFS Permissions on Shared Files and Folders
- Configure Account to Scan Share Permissions on Shared Files and Folders

3.2.1. Configure Account to Scan NTFS Permissions on Shared Files and Folders

Do one of the following depending on the OS:

- To configure account to scan NTFS permissions on pre-Windows Server 2012 versions
- To configure account to scan NTFS permissions on Windows Server 2012 and above
To configure account to scan NTFS permissions on pre-Windows Server 2012 versions

- To grant the List Folder Content permission on pre-Windows Server 2012 versions

1. Navigate to the target shared folder/file, right-click it and select Properties.
2. In the <Share_Name> Properties dialog, select the Security tab and click Edit.
3. In the Permissions for <Share_Name> dialog, click Add to add an account or group you want to be able to check effective permissions.

4. Locate the newly added account or group and set the "Allow" flag next to the following options:
   - List folder contents

- To grant Read Permissions on pre-Windows Server 2012 versions

1. Navigate to the target shared folder/file, right-click it and select Properties.
2. In the <Share_Name> Properties dialog, select the Security tab and click Advanced.
3. In the Advanced Security Settings for <Share_Name> dialog, click Change Permissions.
4. Click **Add** to add an account or group you want to be able to check effective permissions.

5. In the **Select user, Computer, Service account, or Group** dialog, type the name of the account or group you want to be able to check effective permissions.

6. In the **Permissions Entry for <Share_Name>** dialog, set the "Allow" flag next to the following options:
   - Read permissions
NOTE: Make sure that Apply to: is set to "This folder, subfolders and files", and Apply these auditing entries to objects and/or containers within this container only is cleared.

To configure account to scan NTFS permissions on Windows Server 2012 and above

- To grant the List Folder Content permission on Windows Server 2012 and above
  1. Navigate to the target shared folder/file, right-click it and select Properties.
  2. In the <Share_Name> Properties dialog, select the Security tab and click Edit.
  3. In the Permissions for <Share_Name> dialog, click Add to add an account or group you want to be able to check effective permissions.
4. Locate the newly added account or group and set the "Allow" flag next to the following options:
   - List folder contents

   **To grant Read Permissions on Windows Server 2012 and above**

1. Navigate to the target shared folder/file, right-click it and select Properties.
2. In the `<Share_Name>` Properties dialog, select the Security tab and click Advanced.
3. In the Advanced Security Settings for `<Share_Name>` dialog, click Add.
4. In the Permission Entry for `<Share_Name>` dialog, click the Select a principal link.
5. In the Select user, Computer, Service account, or Group dialog, type the name of an account or group you want to be able to check effective permissions.
6. In the Permission Entry for `<Share_Name>` dialog, click Advanced.
7. Set Type to “Allow” and Applies to to “This folder, subfolders and files”. Under Permissions, select the Read permissions checkbox.

**NOTE:** Make sure that the Only apply these auditing settings to objects and/or containers within this container checkbox is cleared.

### 3.2.2. Configure Account to Scan Share Permissions on Shared Files and Folders

To ensure successfull scanning your shared folder/file, the account used by Netwrix Effective Permissions Reporting Tool to check permissions must be a member of the local Administrators group on the computer where the target shared folder/file is located.
4. Start Using Netwrix Effective Permissions Reporting Tool

To start collecting data on your IT Infrastructure, you must configure Netwrix Effective Permissions Reporting Tool.

1. Run the installation package.

**NOTE:** To invoke Netwrix Effective Permissions Reporting Tool again, navigate to the `%Netwrix Effective Permissions Reporting Tool installation folder%` and click on the product icon.

2. Complete the following fields:
4. Start Using Netwrix Effective Permissions Reporting Tool

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User or group to check effective permissions for:</td>
<td>Specify a user name or group name for whom you want to check effective permissions in the DOMAIN\user format.</td>
</tr>
<tr>
<td>List objects with inherited permissions</td>
<td>Enable the checkbox to include objects with inherited permissions to the report.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> Refer to the Windows Server TechCenter article for more information: <a href="#">Inherited Permissions</a>.</td>
</tr>
</tbody>
</table>

**Scan the following network resources:**

1. Click **Add**.

2. In the Specify Network Resource dialog, select one of the following:

   - **Active Directory**—Provide the audited Active Directory object name (domain, OU, etc.) in the FQDN format, e.g. CORP.local.

     In the screenshot above, the report on effective permissions granted to the **CORP\Administrator** user for the **CORP.local** domain will be shown.

   - **File Path**—Provide the UNC file path, e.g. \ROOTDC2\shared.

     In the screenshot above, the report on effective permissions granted to the **CORP\Administrator** user for the **\ROOTDC2\shared** file share will be shown.

3. Click **Start scanning** to launch data collection.

4. In the Save Effective Permissions Report dialog that opens, specify the name of the new report and select its location. The report file will be saved in the HTML format and displayed in a default web browser.

5. In the Netwrix Effective Permissions Reporting Tool dialog, click **OK** to save the report.
5. See How Effective Permissions Are Reported

After the data collection has completed, see how effective permissions are reported by the product. This section explains how to review the Effective Permissions Report.

The example report provides the following information:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;User_Name&gt; is a member of the following groups:</td>
<td>The list of Active Directory groups where the user belongs to.</td>
</tr>
</tbody>
</table>
### 5. See How Effective Permissions Are Reported

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Effective permissions for <code>&lt;User_Name&gt;</code> (objects with inherited permissions are shown/hidden)</strong></td>
<td></td>
</tr>
<tr>
<td>Network Resource: <code>&lt;Resource_Name&gt;</code></td>
<td>The name of the network resource: <strong>Active Directory domain</strong> or <strong>File Path</strong>.</td>
</tr>
<tr>
<td>Object Path</td>
<td>• When <strong>Active Directory domain</strong> selected: Active Directory object (the audited OU, container within a domain, domain user, etc.) name in the FQDN format.</td>
</tr>
<tr>
<td></td>
<td>• When <strong>Files and Shares</strong> selected: the UNC file path.</td>
</tr>
<tr>
<td>Permissions</td>
<td>Contains a list of effective permissions granted to groups which are shown in the <strong>Has Access via Groups</strong> column for the selected network resource.</td>
</tr>
<tr>
<td>Has Access via Groups</td>
<td>The list of Active Directory groups where the user belongs to with effective permissions for the selected network resource.</td>
</tr>
</tbody>
</table>