Deploy Access-Denied Assistance (Demonstration Steps)

Applies To: Windows Server 2012

This topic explains how to configure access-denied assistance, and verify that it is working properly.

In this document

- [Step 1: Configure access-denied assistance](#)

- [Step 2: Configure the email notification settings](#)

- [Step 3: Verify that access-denied assistance is configured correctly](#)

Note

This topic includes sample Windows PowerShell cmdlets that you can use to automate some of the procedures described. For more information, see [Using Cmdlets](#).

[Step 1: Configure access-denied assistance](#)

You can configure access-denied assistance within a domain by using Group Policy, or you can configure the assistance individually on each file server by using the File Server Resource Manager console. You can also change the access-denied message for a specific shared folder on a file server.

You can configure access-denied assistance for the domain by using Group Policy as follows:

[Do this step using Windows PowerShell](#)

[To configure access-denied assistance by using Group Policy](#)

1. Open Group Policy Management. In Server Manager, click **Tools**, and then click **Group Policy Management**.
2. Right-click the appropriate Group Policy, and then click **Edit**.
3. Click **Computer Configuration**, click **Policies**, click **Administrative Templates**, click **System**, and then click **Access-Denied Assistance**.
4. Right-click **Customize message for Access Denied errors**, and then click **Edit**.
5. Select the **Enabled** option.
6. Configure the following options:
    1. In the **Display the following message to users who are denied access** box, type a message that users will see when they are denied access to a file or folder.

You can add macros to the message that will insert customized text. The macros include:

- **[Original File Path]** The original file path that was accessed by the user.

- **[Original File Path Folder]** The parent folder of the original file path that was accessed by the user.

- **[Admin Email]** The administrator email recipient list.

- **[Data Owner Email]** The data owner email recipient list.

2. Select the **Enable users to request assistance** check box.

3. Leave the remaining default settings.

Windows PowerShell equivalent commands

The following Windows PowerShell cmdlet or cmdlets perform the same function as the preceding procedure. Enter each cmdlet on a single line, even though they may appear word-wrapped across several lines here because of formatting constraints.

```
Set-GPRegistryValue –Name "Name of GPO" –key
"HKLM\Software\Policies\Microsoft\Windows\ADR\AccessDenied" –ValueName
AllowEmailRequests –Type DWORD –value 1
Set-GPRegistryValue –Name "Name of GPO" –key
"HKLM\Software\Policies\Microsoft\Windows\ADR\AccessDenied" –ValueName
GenerateLog –Type DWORD –value 1
Set-GPRegistryValue –Name "Name of GPO" –key
"HKLM\Software\Policies\Microsoft\Windows\ADR\AccessDenied" –ValueName
IncludeDeviceClaims –Type DWORD –value 1
Set-GPRegistryValue –Name "Name of GPO" –key
"HKLM\Software\Policies\Microsoft\Windows\ADR\AccessDenied" –ValueName
IncludeUserClaims –Type DWORD –value 1
Set-GPRegistryValue –Name "Name of GPO" –key
"HKLM\Software\Policies\Microsoft\Windows\ADR\AccessDenied" –ValueName
PutAdminOnTo –Type DWORD –value 1
Set-GPRegistryValue –Name "Name of GPO" –key
"HKLM\Software\Policies\Microsoft\Windows\ADR\AccessDenied" –ValueName
PutDataOwnerOnTo –Type DWORD –value 1
Set-GPRegistryValue –Name "Name of GPO" –key
"HKLM\Software\Policies\Microsoft\Windows\ADR\AccessDenied" –ValueName
ErrorMessage –Type MultiString –value "Type the text that the user will see
in the error message dialog box."
Set-GPRegistryValue –Name "Name of GPO" –key
"HKLM\Software\Policies\Microsoft\Windows\ADR\AccessDenied" –ValueName
Enabled –Type DWORD –value 1
```

Alternatively, you can configure access-denied assistance individually on each file server by using the File Server Resource Manager console.

1. Open File Server Resource Manager. In Server Manager, click **Tools**, and then click **File Server Resource Manager**.
2. Right-click **File Server Resource Manager (Local)**, and then click **Configure Options**.
3. Click the **Access-Denied Assistance** tab.
4. Select the **Enable access-denied assistance** check box.
5. In the **Display the following message to users who are denied access to a folder or file** box, type a message that users will see when they are denied access to a file or folder.

   You can add macros to the message that will insert customized text. The macros include:

   - **[Original File Path]** The original file path that was accessed by the user.

   - **[Original File Path Folder]** The parent folder of the original file path that was accessed by the user.

   - **[Admin Email]** The administrator email recipient list.

   - **[Data Owner Email]** The data owner email recipient list.

6. Click **Configure email requests**, select the **Enable users to request assistance** check box, and then click **OK**.
7. Click **Preview** if you want to see how the error message will look to the user.
8. Click **OK**.

Windows PowerShell equivalent commands

The following Windows PowerShell cmdlet or cmdlets perform the same function as the preceding procedure. Enter each cmdlet on a single line, even though they may appear word-wrapped across several lines here because of formatting constraints.

```
Set-FSRMAdrSetting -Event "AccessDenied" –DisplayMessage "Type the text that
the user will see in the error message dialog box." -Enabled:$true -
AllowRequests:$true
```

After you configure the access-denied assistance, you must enable it for all file types by using Group Policy.

1. Open Group Policy Management. In Server Manager, click **Tools**, and then click **Group Policy Management**.

2. Right-click the appropriate Group Policy, and then click **Edit**.
3. Click **Computer Configuration**, click **Policies**, click **Administrative Templates**, click **System**, and then click **Access-Denied Assistance**.
4. Right-click **Enable access-denied assistance on client for all file types**, and then click **Edit**.
5. Click **Enabled**, and then click **OK**.

Windows PowerShell equivalent commands

The following Windows PowerShell cmdlet or cmdlets perform the same function as the preceding procedure. Enter each cmdlet on a single line, even though they may appear word-wrapped across several lines here because of formatting constraints.

```
Set-GPRegistryValue –Name "Name of GPO" –key
"HKLM\SOFTWARE\Policies\Microsoft\Windows\Explorer" –ValueName
EnableShellExecuteFileStreamCheck –Type DWORD –value 1
```

You can also specify a separate access-denied message for each shared folder on a file server by using the File Server Resource Manager console.

Do this step using Windows PowerShell

To specify a separate access-denied message for a shared folder by using File Server Resource Manager

1. Open File Server Resource Manager. In Server Manager, click **Tools**, and then click **File Server Resource Manager**.
2. Expand **File Server Resource Manager (Local)**, and then click **Classification Management**.
3. Right-click **Classification Properties**, and then click **Set Folder Management Properties**.
4. In the **Property** box, click **Access-Denied Assistance Message**, and then click **Add**.
5. Click **Browse**, and then choose the folder that should have the custom access-denied message.
6. In the **Value** box, type the message that should be presented to the users when they cannot access a resource within that folder.

    You can add macros to the message that will insert customized text. The macros include:

    o **[Original File Path]** The original file path that was accessed by the user.

    o **[Original File Path Folder]** The parent folder of the original file path that was accessed by the user.

    o **[Admin Email]** The administrator email recipient list.

- o **[Data Owner Email]** The data owner email recipient list.

7. Click **OK**, and then click **Close**.

Windows PowerShell equivalent commands

The following Windows PowerShell cmdlet or cmdlets perform the same function as the preceding procedure. Enter each cmdlet on a single line, even though they may appear word-wrapped across several lines here because of formatting constraints.

```
Set-FSRMMgmtProperty -Namespace "folder path" -Name "AccessDeniedMessage_MS"
-Value "Type the text that the user will see in the error message dialog
box."
```
Step 2: Configure the email notification settings

You must configure the email notification settings on each file server that will send the access-denied assistance messages.

Do this step using Windows PowerShell

1. Open File Server Resource Manager. In Server Manager, click **Tools**, and then click **File Server Resource Manager**.
2. Right-click **File Server Resource Manager (Local)**, and then click **Configure Options**.
3. Click the **Email Notifications** tab.
4. Configure the following settings:
   - o In the **SMTP server name or IP address** box, type the name of IP address of the SMTP server in your organization.

   - o In the **Default administrator recipients** and **Default "From" e-mail address** boxes, type the email address of the file server administrator.

5. Click **Send Test E-mail** to ensure that the email notifications are configured correctly.
6. Click **OK**.

Windows PowerShell equivalent commands

The following Windows PowerShell cmdlet or cmdlets perform the same function as the preceding procedure. Enter each cmdlet on a single line, even though they may appear word-wrapped across several lines here because of formatting constraints.

```
set-FSRMSetting -SMTPServer "server1" -AdminEmailAddress
"fileadmin@contoso.com" -FromEmailAddress "fileadmin@contoso.com"
```
Step 3: Verify that access-denied assistance is configured correctly

You can verify that the access-denied assistance is configured correctly by having a user who is running Windows 8 try to access a share or a file in that share that they do not have access to. When the access-denied message appears, the user should see a **Request Assistance** button.

After clicking the Request Assistance button, the user can specify a reason for access and then send an email to the folder owner or file server administrator. The folder owner or file server administrator can verify for you that the email arrived and contains the appropriate details.

Important

If you want to verify access-denied assistance by having a user who is running Windows Server 2012, you must install the Desktop Experience before connecting to the file share.