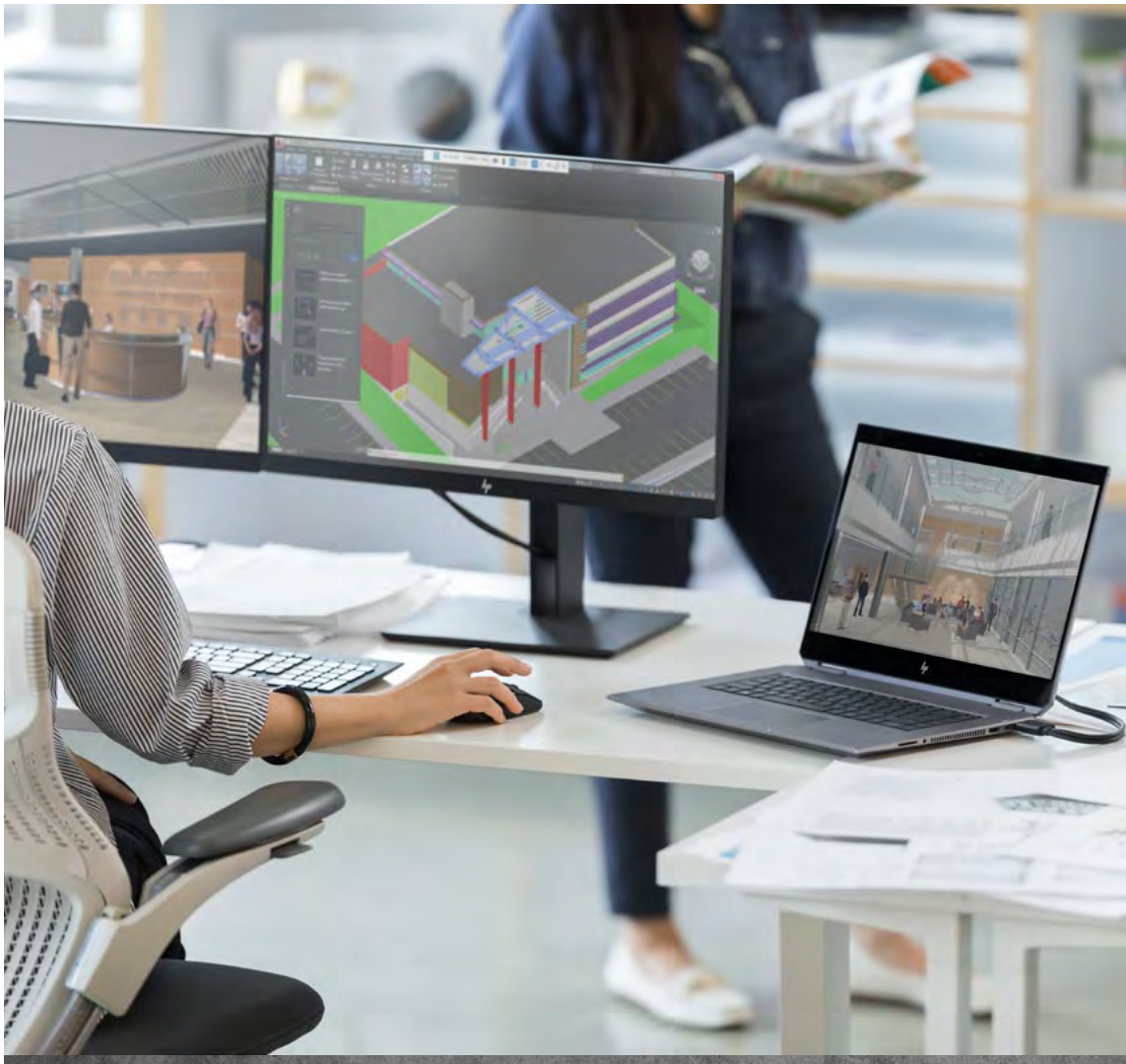
TECHNICAL WHITE PAPER

CONTENTS & NAVIGATION



HP INC. CENTRALIZED WORKSTATIONS

USER PROFILES AND FOLDER REDIRECTION IN A CENTRALIZED WORKSTATION ENVIRONMENT

Choosing the right type of User Profile

Below we will evaluate each profile type so you can choose which type of profile will work best in your environment. First we will discuss the different types of user profiles and then how to choose the best user profile for your organization. We will in detail discuss the pros and cons of each profile type and further in this document will be a tutorial for setting up each type based on best practices.

Profile's supported by Microsoft natively

Local Profile: Is a profile that exists only on the local computer that the user work on. That profile is created from the Default's user's folder (c:\user\default or c:\document and setting\default) and it copy the Default's user registry hive (HKEY_USERS\.Default).

Pros:

- Allows for much faster login times because the user's data is all stored locally.
- Cuts down on bandwidth and storage consumption because less data is transferred during login and logoff and data is stored on local computer.
- Great for people who have a designated desk where they use the same computer every time.

Cons:

- If the user gets on a different PC, they may not be able to access their local data unless they stored some of it in a separate folder on a server.
- Security issues since local profiles store the data locally, which could present a security problem if that PC is stolen.
- Potential for data loss due to loss, theft or hard drive failure.

Roaming Profile: Is a profile that roams/travels with the user. A network's administrator is needed to configure roaming profiles since they are usually centralized in on a file server. In the Active Directory User and Computer's applet, a GPO or in the Remote Desktop Service Profile's tab you can configure the network path to each user profile. Often file re-direction is used in combination with roaming profiles to reduce profile size.

Pros:

- Users can keep the settings they set.
- The settings follow them around different computers and they only have to enter details once (e.g. first start notifications on programs).
- Data can be backed up on the server file store so whenever users log out, they don't have to remember to do so.
- Allows users to log into multiple computers. This works great in an environment where people don't have designated desks, such as an open lab.

Cons:

- They can get quite large and take a while to log on depending on your network speeds.
- They have a tendency to get corrupted over time and have to be restored from backup or given a fresh profile.
- They can rapidly grow in size and consume a lot of disk space.
- Security issues. After the user has logged on, a copy of their profile is left on the hard drive. If the computer were to be stolen, this data could easily be compromised.
- Slow login times - If a user puts too much data in their profile, it could take a very long time to transfer all that data whenever they log on or off. This could also lead to profile corruption.
- Bandwidth consumption - Large user profiles take a lot of network bandwidth to transfer data back and forth. Much of this amounts to wasted bandwidth since many of the files and data transferred are not accessed every time the user logs on.
- Maintenance issues - Old profiles left behind can fill the hard drive up to point where they prevent other users from logging in.

Mandatory Profiles: Is a profile that works the same way as the roaming's profile, except that it does not save back the change when the user log off. The NTUSER.DAT is renamed NTUSER.MAN in the profile's directory.

Pros:

- The User experience is always the same (as nothing can change between sessions).
- Fast Login as profile size does not grow since nothing can be written to it.
- Profile corruption issues are virtually eliminated.

Cons:

- Settings are not saved so any access to files is dependent on mapped drives to access data.
- Users are not able to save any application and desktop customizations.

Supported by Microsoft but not native

FSLogix Profile: Is also a profile that works the same way as the roaming user profile, except that the profile is stored in a VHD(X) container on server store that mounts as a storage device when the user logs into the host.

Pros:

- Faster Login times than Roaming Profiles.
- Users can keep the settings they set.
- The settings follow them around different computers.
- They only have to enter details once (e.g. first start notifications on programs).
- Less susceptible to profile corruption.

Cons:

- User can only log into 1 host at a time since profile container can only mount once per login.
- Bandwidth and disk space consumption. Large user profiles take a lot of network bandwidth to mount.
- Log in time is dependent on profile container size, disk I/O, and bandwidth but much faster than a comparable roaming profile.

Listed below is a scenario matrix to help guide the user on profile scenarios that may work for them depending on their situation and objectives. There are many more variables when it comes to choosing the right solution than can be put in a simple table, but this is meant only as a guide. Sometimes the best results can be achieved by combining more than one profile type.

Scenarios - These scenarios are based on your network and user situation	Desired Behavior - These are broken in to how you prefer to setup profiles	Local Profiles	Mandatory Profiles	Roaming Profiles	FSLogix
All my users are local and on our local area network Characteristics: High Bandwidth Network Stable Low Latency	I want my users to have customized profiles on all local and remote computers	Good		Best	
	I want my users to have customized profiles on local computers but static profile for remote computers	Best Local System	Best Remote System		
	I want my users to have the same profile for all computers		Good Static Profile	Better Synchronized Profile	Best Sender Must be a Local Profile
	I want my users to have customized profiles on all local computers and pre-defined static profiles on all remote computers	Best Local System	Best Remote System		
All my users are remote, not on our local area network unless they VPN into the network Characteristics: Low Bandwidth Network Stable High Latency	I want my users to have customized profiles on all local and remote computers	Best			
	I want my users to have customized profiles on local computers but static profile for remote computers	Best Local System	Best Remote System		
	I want my users to have the same profile for all computers		Good Static Profile	Good Synchronized Profile	Better Sender Must be a Local Profile
	I want my users to have customized profiles on all local computers and pre-defined static profiles on all remote computers	Best Local System	Best Remote System		
Some of my users are remote and have undependable networks Characteristics: Average Bandwidth Unstable High Latency	I want my users to have customized profiles on all local and remote computers	Best		Will work but will be slow for the remote users	
	I want my users to have customized profiles on local computers but static profile for remote computers	Best Local System	Best Remote System	Ok	
	I want my users to have the same profile for all computers		Best	Good	
	I want my users to have customized profiles on all local computers and pre-defined static profiles on all remote computers	Best Local System	Best Remote System	Good	

The Roaming Profile and FSLogix solutions are dependent on a network. The performance of the solution will vary with network performance

DEPLOYING USER PROFILES

This topic describes how to use Windows Server to deploy Roaming User Profiles to Windows client computers. Roaming User Profiles redirects user profiles to a file share so that users receive the same operating system and application settings on multiple computers.

Prerequisites

Roaming User Profiles has the following software requirements:

- If you are deploying Roaming User Profiles with Folder Redirection in an environment with existing local user profiles, deploy Folder Redirection before Roaming User Profiles to minimize the size of roaming profiles. After the existing user folders have been successfully redirected, you can deploy Roaming User Profiles.
- To administer Roaming User Profiles, you must be signed in as a member of the Domain Administrators security group, the Enterprise Administrators security group, or the Group Policy Creator Owners security group.
- Client computers must run Windows 10, Windows 8.1, Windows 8, Windows 7, Windows Vista, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2, or Windows Server 2008.
- Client computers must be joined to the Active Directory Domain Services (AD DS) that you are managing.
- A computer must be available with Group Policy Management and Active Directory installed.
- A file server with sufficient storage capacity must be available to host roaming user profiles.
  Note: The layout of a user's Start menu won't roam on Windows 10, Windows Server 2019, or Windows Server 2016 if they're using more than one PC, Remote Desktop Session Host, or Virtualized Desktop Infrastructure (VDI) server. FSLogix described further in this document will address this issue and allow user's Start menu to roam on Windows 10 and other Operating Systems.

Considerations when using Roaming User Profiles on multiple versions of Windows

- We do not recommend using Roaming User Profiles across multiple versions of Windows. Roaming between Windows Vista/Windows Server 2008 and Windows 7/Windows Server 2008 R2 operating system versions are not supported due to incompatibilities in their profile version which would create undesirable and unpredictable issues such as profile corruption.
- Use Folder Redirection to store user files such as documents and pictures outside of user profiles. This enables the same files to be available to users across operating system versions. It also keeps profiles small and sign-ins quick.
- Don't use Roaming User Profiles across computers running different operating systems or your users that changes made on one operating system version won't roam to another operating system version.

Deploy Roaming User Profiles

Step 1:

Create a Roaming User Profiles security group

If your environment is not already set up with Roaming User Profiles, the first step is to create a security group that contains all users and/or computers to which you want to apply Roaming User Profiles policy settings.

- Administrators of general-purpose roaming user profiles deployments typically create a security group for users.
- Administrators of Remote Desktop Services or virtualized desktop deployments typically use a security group for users and the shared computers.

Create a security group for Roaming User Profiles:

1. On the AD Server Manager open Active Directory Users and Groups.
2. Right-click the appropriate domain or OU, select New, and then select Group.
3. In the Create Group window, in the Group section, specify the following settings:
   - In Group name, type the name of the security group, for example: Roaming User Profiles
   - In Group scope, select Security, and then select Global.
4. In the Members section, select Add. The Select Users, Contacts, Computers, Service Accounts or Groups dialog box appears.
5. If you want to include computer accounts in the security group, select Object Types, select the Computers check box and then select OK.
6. Type the names of the users, groups, and/or computers to which you want to deploy Roaming User Profiles, select OK, and then select OK again.

Step 2:

Create a file share for roaming user profiles

If you do not already have a separate file share for roaming user profiles (independent from any shares for redirected folders to prevent inadvertent caching of the roaming profile folder), use the following procedure to create a file share on a server running Windows Server.

Note: Some functionality might differ or be unavailable depending on the version of Windows Server you're using.

Create a file share on Windows Server:

1. In the Server Manager navigation pane, select File and Storage Services, and then select Shares to display the Shares page.
2. In the Shares tile, select Tasks, and then select New Share. The New Share Wizard appears.
3. On the Select Profile page, select SMB Share – Quick. If you have File Server Resource Manager installed and are using folder management properties, instead select SMB Share - Advanced.
4. On the Share Location page, select the server and volume on which you want to create the share.
5. On the Share Name page, type a name for the share (for example, User Profiles$) in the Share name box.
   Note: When creating the share, hide the share by putting a $ after the share name. This hides the share from casual browsers.
6. On the Other Settings page, clear the Enable continuous availability checkbox, if present, and optionally select the Enable access-based enumeration and Encrypt data access checkboxes.
7. On the Permissions page, select Customize permissions. The Advanced Security Settings dialog box appears.
8. Select Disable inheritance, and then select Convert inherited permissions into explicit permission on this object.
9. Set the permissions as described in Required permissions for the file share hosting roaming user profiles and shown in the following screen shot, removing permissions for unlisted groups and accounts, and adding special permissions to the Roaming User Profiles Users and Computers group that you created in Step 1.

Figure 1 Setting the permissions for the roaming user profiles share

10. If you chose the SMB Share - Advanced profile, on the Management Properties page, select the User Files Folder Usage value.
11. If you chose the SMB Share - Advanced profile, on the Quota page, optionally select a quota to apply to users of the share.
12. On the Confirmation page, select Create.

Required permissions for the file share hosting roaming user profiles

User Account	Access	Applies to
System	Full control	This folder, subfolders and files
Administrators	Full Control	This folder only
Creator/Owner	Full Control	Subfolders and files only
Security group of users needing to put data on share (Roaming User Profiles Users and Computers)	List folder / read data (Advanced permissions) Create folders / append data (Advanced permissions)	This folder only
Other groups and accounts	None (remove)	This Folder, Sub-Folders, and File

Step 3:

Create a GPO for Roaming User Profiles

If you do not already have a GPO created for Roaming User Profiles settings, use the following procedure to create an empty GPO for use with Roaming User Profiles. This GPO allows you to configure Roaming User Profiles settings and can also be used to enable Roaming User Profiles on computers, as is typically done when deploying in virtualized desktop environments or with Remote Desktop Services.

Create a GPO for Roaming User Profiles:

1. Open Group Policy Management from your AD Server.
2. Right-click the domain or OU in which you want to setup Roaming User Profiles, then select Create a GPO in this domain, and Link it here.
3. In the New GPO dialog box, type a name for the GPO (for example, Roaming User Profile Settings), and then select OK.

4. Right-click the newly created GPO and then clear the Link Enabled checkbox. This prevents the GPO from being applied until you finish configuring it.
5. Select the GPO. In the Security Filtering section of the Scope tab, select Authenticated Users, and then select Remove to prevent the GPO from being applied to everyone.
6. In the Security Filtering section, select Add.
7. In the Select User, Computer, or Group dialog box, type the name of the security group you created in Step 1 (for example, Roaming User Profiles Users and Computers), and then select OK.
8. Select the Delegation tab, select Add, type Authenticated Users, select OK, and then select OK again to accept the default Read permissions.

Step 4:

Option 1: set up Roaming User Profiles on user accounts

If you are deploying Roaming User Profiles to user accounts, use the following procedure to specify roaming user profiles for user accounts in Active Directory Domain Services. If you are deploying Roaming User Profiles to computers, as is typically done for Remote Desktop Services or virtualized desktop deployments, instead use the procedure documented in Step 5: Option 2: set up Roaming User Profiles on computers.

Note: If you set up Roaming User Profiles on user accounts by using Active Directory and on computers by using Group Policy, the computer-based policy setting takes precedence.

Setup up Roaming User Profiles on user accounts:

1. In Active Directory Users and Groups, navigate to the Users container (or OU) in the appropriate domain.
2. Select all users to which you want to assign a roaming user profile, right-click the users and then select Properties.
3. In the Profile section, select the Profile path: checkbox and then enter the path to the file share where you want to store the user's roaming user profile, followed by %username% (which is automatically replaced with the user name the first time the user signs in). For example: \\fs1.corp.contoso.com\User Profiles$\%username%
4. Select OK.

Step 5:

Option 2: set up Roaming User Profiles on computers

If you are deploying Roaming User Profiles to computers, as is typically done for Remote Desktop Services or virtualized desktop deployments, use the following procedure. If you are deploying Roaming User Profiles to user accounts, instead use the procedure described in Step 4: Option 1: set up Roaming User Profiles on user accounts.

If you set up Roaming User Profiles on computers by using Group Policy and on user accounts by using Active Directory, the computer-based policy setting takes precedence.

Set up Roaming User Profiles on computers:

1. Open Group Policy Management from your AD Server.
2. In Group Policy Management, right-click the GPO you created in Step 3 (e.g. Roaming User Profiles Settings), and then select Edit.
3. In the Group Policy Management Editor window, navigate to Computer Configuration, then Policies, then Administrative Templates, then System, and then User Profiles.
4. Right-click Set roaming profile path for all users logging onto this computer and then select Edit.
5. In the Properties dialog box, select Enabled.
6. In the Users logging onto this computer should use this roaming profile path box, enter the path to the file share where you want to store the user's roaming user profile, followed by %username% (which is automatically replaced with the user name the first time the user signs in). For example: \\fs1.corp.contoso.com\User Profiles$\%username%
7. Select OK.

Note: To Further decrease sign-in times by removing unnecessary apps from the Windows 10 base image you use to deploy client PCs. Windows Server 2019 and Windows Server 2016 don't have any pre-provisioned apps, so you can skip this step on server images.

- To remove apps, use the Remove-AppxProvisionedPackage cmdlet in Windows PowerShell to uninstall the following applications. If your PCs are already deployed, you can script the removal of these apps using the Remove-AppxPackage.
  - Microsoft.windowscommunicationsapps_8wekyb3d8bbwe
  - Microsoft.BingWeather_8wekyb3d8bbwe
  - Microsoft.DesktopAppInstaller_8wekyb3d8bbwe
  - Microsoft.Getstarted_8wekyb3d8bbwe
  - Microsoft.Windows.Photos_8wekyb3d8bbwe
  - Microsoft.WindowsCamera_8wekyb3d8bbwe
  - Microsoft.WindowsFeedbackHub_8wekyb3d8bbwe
  - Microsoft.WindowsStore_8wekyb3d8bbwe
  - Microsoft.XboxApp_8wekyb3d8bbwe
  - Microsoft.XboxIdentityProvider_8wekyb3d8bbwe
  - Microsoft.ZuneMusic_8wekyb3d8bbwe

Uninstalling these apps decreases sign-in times, but you can leave them installed if your deployment needs any of them.

Step 6:

Enable the Roaming User Profiles GPO

If you set up Roaming User Profiles on computers by using Group Policy, or if you customized other Roaming User Profiles settings by using Group Policy, the next step is to enable the GPO, permitting it to be applied to affected users.

Enable the Roaming User Profile GPO:

1. Open Group Policy Management.
2. Right-click the GPO that you created and then select Link Enabled. A checkbox appears next to the menu item.

Step 7:

Test Roaming User Profiles

To test Roaming User Profiles, sign in to a computer with a user account configured for Roaming User Profiles, or sign in to a computer configured for Roaming User Profiles. Then confirm that the profile is redirected.

1. Sign in to a primary computer (if you enabled primary computer support) with a user account for which you have enabled Roaming User Profiles enabled. If you enabled Roaming User Profiles on specific computers, sign in to one of these computers.
2. If the user has previously signed in to the computer, open an elevated command prompt, and then type the following command to ensure that the latest Group Policy settings are applied to the client computer: GpUpdate /Force
3. To confirm that the user profile is roaming, open Control Panel, select System and Security, select System, select Advanced System Settings, select Settings in the User Profiles section and then look for Roaming in the Type column.

CREATING MANDATORY USER PROFILES

This topic describes how to use Windows Server to deploy Mandatory User Profiles to Windows client computers. A mandatory user profile is a roaming user profile that has been pre-configured by an administrator to specify settings for users. Settings commonly defined in a mandatory profile include (but are not limited to): icons that appear on the desktop, desktop backgrounds, user preferences in Control Panel, printer selections, and more. Configuration changes made during a user's session that are normally saved to a roaming user profile are not saved when a mandatory user profile is assigned.

Mandatory user profiles are useful when standardization is important, such as on a kiosk device or in educational settings. Only system administrators can make changes to mandatory user profiles.

When the server that stores the mandatory profile is unavailable, such as when the user is not connected to the corporate network, users with mandatory profiles can sign in with the locally cached copy of the mandatory profile, if one exists. Otherwise, the user will be signed in with a temporary profile.

User profiles become mandatory profiles when the administrator renames the NTuser.dat file (the registry hive) of each user's profile in the file system of the profile server from NTuser.dat to NTuser.man. The .man extension causes the user profile to be a read-only profile.

Profile extension for each Windows version

The name of the folder in which you store the mandatory profile must use the correct extension for the operating system it will be applied to. The following table lists the correct extension for each operating system version.

Client operating system version	Server operating system version	Profile extension
Windows Vista Windows 7	Windows Server 2008 Windows Server 2008 R2	v2
Windows 8	Windows Server 2012	v3
Windows 8.1	Windows Server 2012 R2	v4
Windows 10, versions 1507 and 1511	N/A	v5
Windows 10, versions 1607, 1703, 1709, 1803, 1809 and 1903	Windows Server 2016 and Windows Server 2019	v6

How to create a mandatory user profile

First, you create a default user profile with the customizations that you want, run Sysprep with CopyProfile set to **True** in the answer file, copy the customized default user profile to a network share, and then you rename the profile to make it mandatory.

To create a default user profile

1. Sign in to a computer running Windows 10 as a member of the local Administrator group. Do not use a domain account.
   Note: Use a lab or extra computer running a clean installation of Windows 10 to create a default user profile. Do not use a computer that is required for business (that is, a production computer). This process removes all domain accounts from the computer, including user profile folders.
2. Configure the computer settings that you want to include in the user profile. For example, you can configure settings for the desktop background, uninstall default apps, install line-of-business apps, and so on.
   Note: Unlike previous versions of Windows, you cannot apply a Start and taskbar layout using a mandatory profile. For alternative methods for customizing the Start menu and taskbar.
3. Create an answer file (Unattend.xml) that sets the CopyProfile parameter to True. The CopyProfile parameter causes Sysprep to copy the currently signed-on user's profile folder to the default user profile. You can use Windows System Image Manager, which is part of the Windows Assessment and Deployment Kit (ADK) to create the Unattend.xml file.
4. Uninstall any application you do not need or want from the PC. For examples on how to uninstall Windows 10 Application see Remove-AppxProvisionedPackage. For a list of uninstallable applications.

Note: It is highly recommended to uninstall unwanted or unneeded apps as it will speed up user sign-in times.

5. At a command prompt, type the following command and press **ENTER**.
   sysprep /oobe /reboot /generalize /unattend:unattend.xml
   (Sysprep.exe is located at: C:\Windows\System32\sysprep. By default, Sysprep looks for unattend.xml in this same folder.)
   Tip
   If you receive an error message that says "Sysprep was not able to validate your Windows installation", open %WINDIR%\System32\Sysprep\Panther\setupact.log and look for an entry like the following:
   Use the **Remove-AppxProvisionedPackage** and **Remove-AppxPackage -AllUsers** cmdlet in Windows PowerShell to uninstall the app that is listed in the log.
6. The sysprep process reboots the PC and starts at the first-run experience screen. Complete the set up, and then sign in to the computer using an account that has local administrator privileges.
7. Right-click Start, go to **Control Panel** (view by large or small icons) **> System > Advanced system settings,** and click **Settings** in the **User Profiles** section.
8. In **User Profiles**, click **Default Profile**, and then click **Copy To**.
9. In **Copy To**, under **Permitted to use**, click **Change**.
10. In **Select User or Group**, in the **Enter the object name to select** field, type everyone, click **Check Names**, and then click **OK**.
11. In **Copy To**, in the **Copy profile to** field, enter the path and folder name where you want to store the mandatory profile. The folder name must use the correct extension for the operating system version. For example, the folder name must end with ".v6" to identify it as a user profile folder for Windows 10, version 1607.
    1. If the device is joined to the domain and you are signed in with an account that has permissions to write to a shared folder on the network, you can enter the shared folder path.
    2. If the device is not joined to the domain, you can save the profile locally and then copy it to the shared folder location.
12. Click **OK** to copy the default user profile.

To make the user profile mandatory

1. In File Explorer, open the folder where you stored the copy of the profile.
   Note: If the folder is not displayed, click **View > Options > Change folder and search options**. On the **View** tab, select **Show hidden files and folders**, clear **Hide protected operating system files**, click **Yes** to confirm that you want to show operating system files, and then click **OK** to save your changes.
2. Rename Ntuser.dat to Ntuser.man.

How to apply a mandatory user profile to users

In a domain, you modify properties for the user account to point to the mandatory profile in a shared folder residing on the server.

To apply a mandatory user profile to users

1. Open **Active Directory Users and Computers** (dsa.msc).
2. Navigate to the user account that you will assign the mandatory profile to.
3. Right-click the user name and open **Properties**.
4. On the **Profile** tab, in the **Profile path** field, enter the path to the shared folder without the extension.
   For example, if the folder name is \\server\profile.v6, you would enter \\server\profile.
5. Click **OK**.

It may take some time for this change to replicate to all domain controllers.

Apply policies to improve sign-in time

When a user is configured with a mandatory profile, Windows 10 starts as though it was the first sign-in each time the user signs in. To improve sign-in performance for users with mandatory user profiles, apply the Group Policy settings shown in the following table. (The table shows which operating system versions each policy setting can apply to).

Group Policy setting	Windows 10	Windows Server 2016	Windows 8.1	Windows Server 2012
Computer Configuration > Administrative Templates > System > Logon > **Show first sign-in animation** = Disabled	Yes	Yes	Yes	Yes
Computer Configuration > Administrative Templates > Windows Components > Search > **Allow Cortana** = Disabled	Yes	Yes	No	No
Computer Configuration > Administrative Templates > Windows Components > Cloud Content > **Turn off Microsoft consumer experience** = Enabled	Yes	No	No	No

DEPLOYING PROFILES WITH FSLOGIX

What is FSLogix?

FSLogix is a set of solutions that enhance, enable, and simplify non-persistent Windows computing environments. FSLogix solutions are appropriate for Virtual environments in both public and private clouds. FSLogix solutions may also be used to create more portable computing sessions when using physical devices.

FSLogix solutions include:

- Profile Container
- Office Container
- Application Masking
- Java Version Control

Here's what you can do with FSLogix solutions:

- Maintain user context in non-persistent environments
- Minimize sign in times for non-persistent environments
- Optimize file IO between host/client and remote profile store
- Native (Local) profile experience, eliminating many compatibility issues with solutions using visible redirection, such as User Profile Disk (UPD)
- Simplify the management of applications and 'Gold Images'
- Specify the version of Java to be utilized by specific URL and applications

Key capabilities

- Redirect user profiles to a network location using Profile Container. Profiles are placed in VHD (X) files and mounted at run time. It's common to copy a profile to and from the network, when a user signs in and out of a remote environment. Because user profiles can often be large, sign in and sign out times often became unacceptable. Mounting and using the profile on the network eliminates delays often associated with solutions which copy files.
- Redirect only the portion of the profile that contains Office data by using Office Container. Office Container allows an organization already using an alternate profile solution to enhance Office in a non-persistent environment. This functionality is useful with the Outlook .OST file.
- Applications use the profile as if it were on the local drive. Because the FSLogix solutions use a Filter Driver to redirect the profile, applications don't recognize that the profile is on the network. Obscuring the redirection is important because many applications won't work properly with a profile stored on remote storage.
- Profile Container is used with Cloud Cache to create resilient and highly available environments. Cloud Cache places a portion of the profile VHD on the local hard drive. Cloud Cache also allows an administrator to specify multiple remote profile locations. The Local Cache, with multiple remote profile containers, insulates users from network and storage failures and or outages.
- Application Masking manages access to an application, font, printer, or other items. Access can be controlled by user, IP Address range, and other criteria. Application Masking significantly decreases the complexity of managing large numbers of gold images.

Requirements

You are eligible to access FSLogix Profile Container, Office 365 Container, Application Masking, and Java Redirection tools if you have one of the following licenses:

- Microsoft 365 E3/E5
- Microsoft 365 A3/A5/ Student Use Benefits
- Microsoft 365 F1
- Microsoft 365 Business
- Windows 10 Enterprise E3/E5
- Windows 10 Education A3/A5
- Windows 10 VDA per user
- Remote Desktop Services (RDS) Client Access License (CAL)
- Remote Desktop Services (RDS) Subscriber Access License (SAL)

FSLogix solutions may be used in any public or private datacenter, as long as a user is properly licensed. FSLogix tools operate on all operating systems newer than, and including:

- Desktop - Windows 7
- Server - 2008 R2
- FSLogix solutions support both 32 bit and 64 bit where applicable
- In no instance are FSLogix solutions supported in an environment that is not supported by Microsoft, or the original software or equipment vendor

Benefits of FSLogix:

Architectural Simplicity

FSLogix is built on simplicity, even its architecture is a simple one, comprising of the user Profile and Office 365 Container spaces of three main components;

1. A simple secured file share to host the Container disks (VHD, VHDX).
2. A single agent installed onto your base image or template of choice.
3. Group Policy or registry settings to control the behaviour of the agent.

As simplistic as this seems, there are of course considerations associated with each of the above control points which we will cover throughout the remainder of this document.

FSLogix Profile Containers

Profile Containers offer a full redirection of the existing profile into a container which is connected to the machine as soon as a user session is initiated. It is simply a redirection of the local profile to an alternate location, which happens to be a virtual disk or “container”. It also supports folder redirection for those that would still like to centralise their user data.

What are profile containers?

Profile Containers are not a traditional profile management solution. It’s not managing the profile as such, its managing an alternate location for an existing profile to live, its effectively combining the speed of a local profile, with the benefits of roaming, and trying to negate the negatives associated with both.

Profile Containers can be configured via a few different tools:

1. Group Policy ADMX files provided as part of the installation download.
2. Profile containers configuration tool: These settings are configured on your base VDA and allow for basic configuration of your Profile Containers.
3. Registry keys.

All of the FSLogix functionality is provided via a single agent. Even extending out to additional tools and offerings that FSLogix have in their suite of solutions. FSlogix functions as below:

1. User Initiates a logon request to Windows.
2. FSLogix agent kicks in and mounts the Profile Container from the network location.
3. FSLogix agent rewrites the profile location at a kernel level to the Profile Container. (This is the true beauty in its simplicity: Windows doesn’t think anything has changed).
4. FSLogix agent then mounts the Office 365 Container.
5. FSLogix writes the location of specific data repositories stored in the %UserProfile%\ location to the Office 365 container in the same fashion as above.
6. FSLogix makes a decision on where to store the Search Database for the user. By default, if both technologies are in play, the search index will exist in the profile container, however depending on your deployment model this can be altered.
7. User Logon is completed by Windows.

This entire process takes a matter of seconds at most, typically less than this and governed by your storage and network capability, hence the importance of sizing and testing in any environment.

Access Methods

Containers are a pretty simple concept once you draw it out, however there are some not so simple scenarios that we need to consider such as multi session RDSH or SBC environments, multiple VDI sessions, combine VDI and physical PC access requirements etc.

Folder Redirection

FSLogix can existing perfectly alongside folder redirection with no extra configuration required, alternatively, it can simply house the data within the container for increased performance, albeit at the expense of multi environment access (more fit for VDI or RDSH only access).

Folders can also be redirected into OneDrive for Business, allowing for sync back to Office 365 rather than a traditional File Share redirection. This would grant the benefits of increased performance around logons and file access, as the cache for this data would exist within the FSLogix Container itself, local to the user. Obviously, the existing considerations of OneDrive for Business and user data need to be taken into consideration.

Specific folders can also be exempted from Profile Containers and redirected to a local location as required.

Considerations

- IOPS: IO in any profile solution is critical. If you have rubbish IO capability, your environment suffers, and this applies directly to profile containers.
- File system: If using Windows Server 2016 to host containers, use REFS file system, particularly if using differencing disks as the merge operations are almost instantaneous.
- Keep ADMX files up to date. With the release of 2.8.10, there is a huge amount of capability in the ADMX files that didn't exist before, and its much nicer to be able to view your configurations in one place.
- Single user login: With FSLogix a user can only log in to one session at a time to a host due to the profile being mounted to a host on login; a second concurrent session to another host is not possible.

FSLogix Roaming Profile Set up

This topic describes how to use Microsoft FSLogix to deploy Roaming Profiles to Windows client computers. We will configure an FSLogix profile container which will hold the user's profile and store it to a file share so that users receive the same desktop and application settings on multiple computers. When using a Profile Container, both applications and users see the profile as if it's located on the local drive.

In this tutorial, learn how to:

- Install a FSLogix Agent
- Set up a File Share for the profile containers
- Configure GPO Profile Container Registry Settings
- Set up Include and Exclude User Groups
- Test FSLogix user profiles

FSLogix Roaming User Profiles has the following software requirements:

Before configuring Profile Container:

- Verify that you meet all **entitlement and configuration requirements.**
- **Download and install** FSLogix Software on both Server and all Host computers.
- Profile Container is installed and configured after stopping use of other solutions used to manage remote profiles.
- Exclude the VHD(X) files for Profile Containers from Anti Virus (AV) scanning.
- If you are deploying FSLogix for roaming User Profiles with Folder Redirection in an environment with existing local user profiles, deploy Folder Redirection before Roaming User Profiles to minimize the size of roaming profiles. After the existing user folders have been successfully redirected, you can deploy Roaming User Profiles.
- To administer Roaming User Profiles, you must be signed in as a member of the Domain Administrators security group, the Enterprise Administrators security group, or the Group Policy Creator Owners security group.
- Client computers must run Windows 10, Windows 8.1, Windows 8, Windows 7, Windows Vista, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2, or Windows Server 2008.
- Client computers must be joined to the Active Directory Domain Services (AD DS) that you are managing.
- A computer must be available with Group Policy Management and Active Directory installed.
- A file server with sufficient storage capacity must be available to host roaming user profiles.

Download and Install FSLogix

The FSLogix software no longer requires license keys. It is recommended that the latest version of FSLogix is downloaded and installed. If legacy FSLogix customers must continue to use an older version, the following key may be used MSFT0-YXKIX-NVQI4-I6WIA-O4TXE. All users must be appropriately entitled and agree to license terms before using FSLogix.

Download FSLogix

FSLogix is available for download **here.**

Install Microsoft FSLogix components

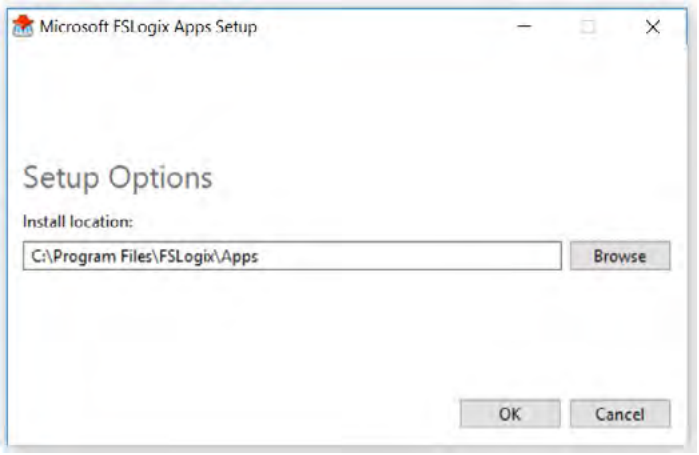
The download for FSLogix includes three installers that are used to install the specific component(s) necessary for your use.

Microsoft FSLogix Apps Installation

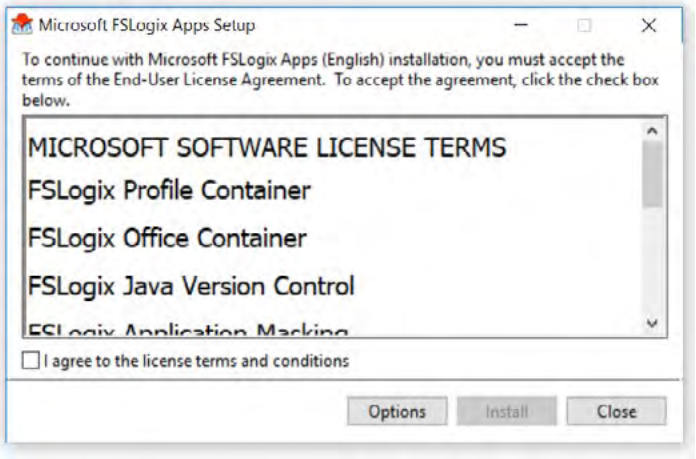
Microsoft FSLogix Apps installs the core drivers and components for all FSLogix solutions. Any environment using FSLogix must install FSLogix Apps. After installation configure **Profile Container** or **Office Container** before using for proFolder Redirection.

To install FSLogix Applications:

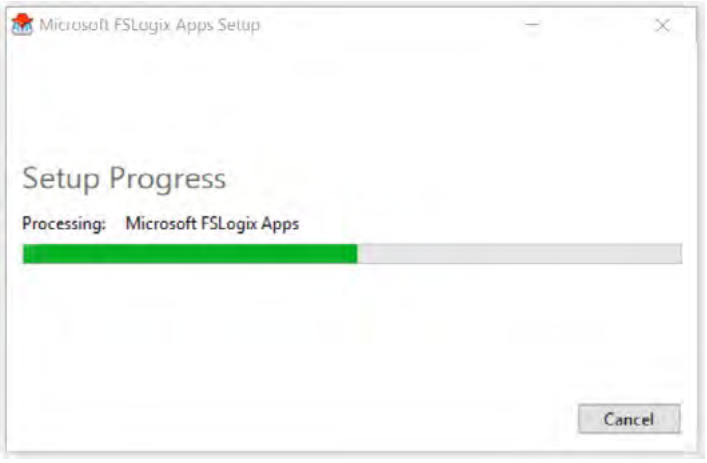
- From the FSLogix download file, select 32 bit or 64 bit depending on your environment
- Run FSLogixAppSetup.exe
- Click Options to specify an installation folder



- Accept the license agreement and click Install



- Microsoft FSLogix Apps will install



Application Masking Rule Editor Installation

The Application Masking Rule Editor is used to define rules used by **Application Masking**.

- From the FSLogix Download file, select 32 bit or 64 bit depending on your environment
- Run FSLogixAppsRuleEditorSetup.exe
- Use Options to specify installation folder (see screenshot for Microsoft FSLogix Apps above)
- Accept the license agreement and click install

Java Version Control Rule Editor Installation

The Java Version Control Rule Editor is used to define rules used by **Java Version Control**.

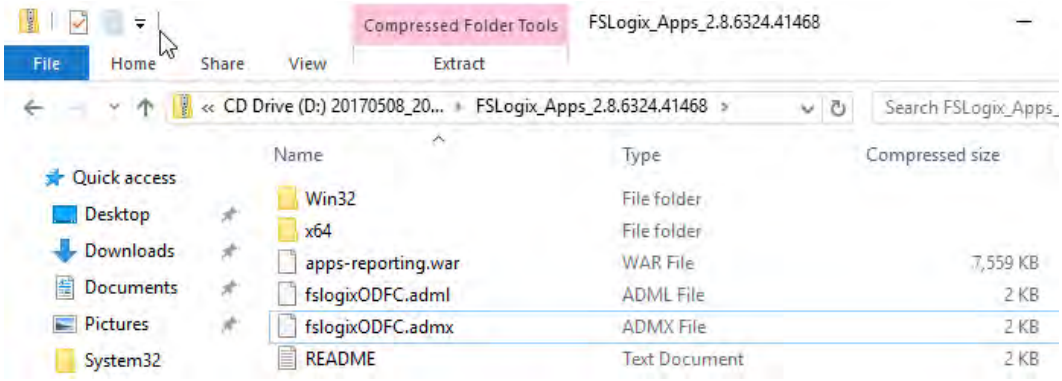
- From the FSLogix Download file, select 32 bit or 64 bit depending on your environment
- Run FSLogixAppsJavaRuleEditorSetup.exe
- Use Options to specify installation folder (see screenshot for Microsoft FSLogix Apps above)
- Accept the license agreement and click install

Install FSLogix Group Policy Template Files

From the FSLogix download folder are the included ADML files you will need to import into your Active Directory GPO central store repository.

To use the template files locally:

- Copy the ADMX file (fslogix.admx) to C:\Windows\PolicyDefinitions
- Copy the ADML file (fslogix.adml) to C:\Windows\PolicyDefinitions\en-US
- Run GPEDIT.MSC
- Browse to Computer Configuration then Administrative Templates then FSLogix



GPO Central Store

To populate the central store:

- Copy the ADMX file (fslogix.admx) to %logonserver%\sysvol%userdnsdomain%\policies\PolicyDefinitions
- Copy the ADML file (fslogix.adml) to %logonserver%\sysvol%userdnsdomain%\policies\PolicyDefinitions\en-US
- Run GPMC.MSC
- Browse to Computer Configuration then Administrative Templates then FSLogix

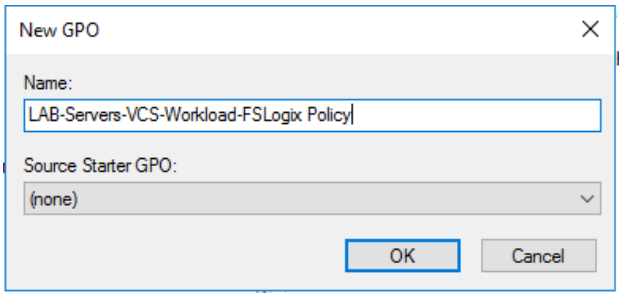
Create an FSLogix GPO

Step 1:

Open Group Policy Management.

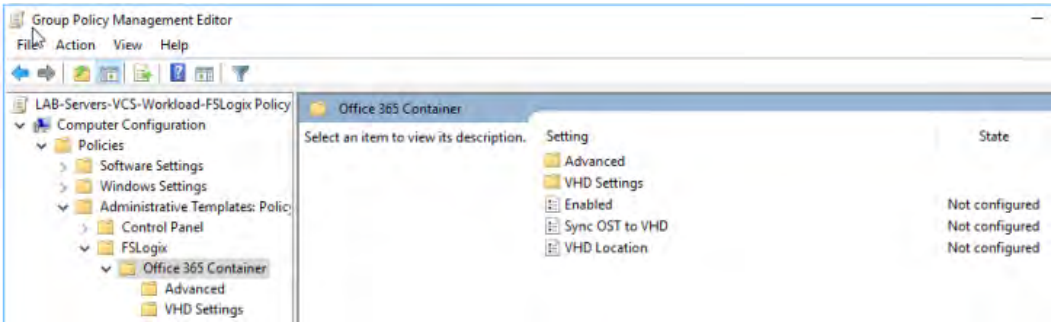
Step 2:

Create a new GPO (or existing) that will be used to apply the FSLogix Configuration to the necessary Computer Accounts.



Step 3:

Expand Computer Configuration\Administrative Templates and confirm FSLogix Folder exists.



Step 4:

Set the following Group Policy Settings:

- FSLogix\Office 365 Container **– Enable** = Option Enabled
- FSLogix\Office 365 Container **– Sync OST to VHD** = Option Enabled
- FSLogix\Office 365 Container **– VHD Location** = VHD Location : \\LAB-DC1\O365Container
- FSLogix\Office 365 Container\Advanced **– Swap Directory name components** = Tick Swap Directory name components
- FSLogix\Office 365 Container\Advanced **– Virtual Disk Type** = VHDX

List of other configurable GPO Setting can be found **here:**

LAB-Servers-VCS-Workload-FSLogix Policy

Scope | Details | Settings | Delegation | Status

Administrative Templates hide

Policy definitions (ADMX files) retrieved from the local computer.

FSLogix/Office 365 Container hide

Policy	Setting	Comment
Enabled	Enabled	
Enabled	Enabled	

Policy	Setting	Comment
Sync OST to VHD	Enabled	
Enabled	Enabled	

Policy	Setting	Comment
VHD Location	Enabled	
VHD Location	\\LAB-DC1\O365Container	

FSLogix/Office 365 Container/Advanced hide

Policy	Setting	Comment
Swap directory name components	Enabled	
Swap directory name components	Enabled	

FSLogix/Office 365 Container/VHD Settings hide

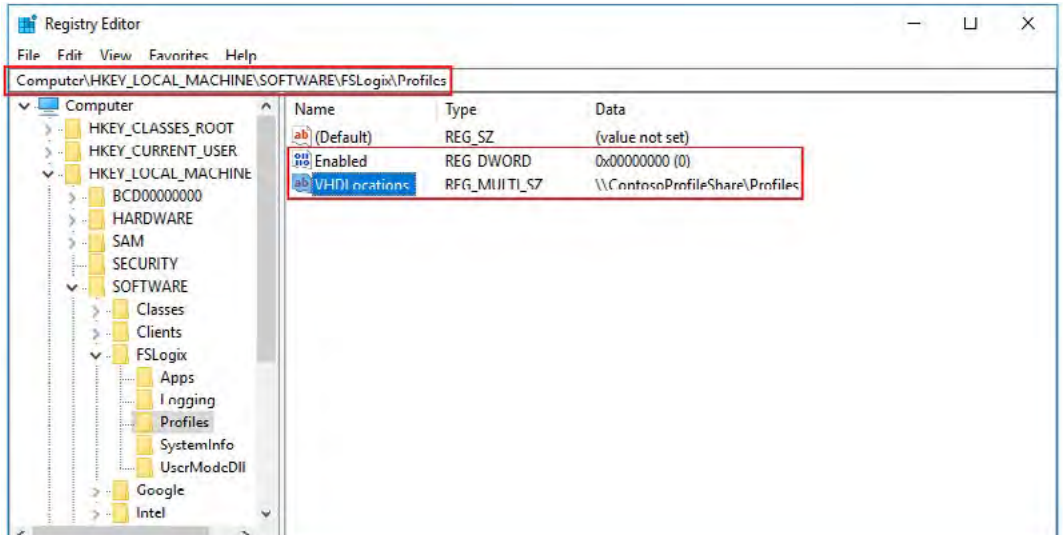
Policy	Setting	Comment
Virtual Disk Type	Enabled	
Virtual Disk Type	VHDX	

Configure Profile Container Registry settings from the local host

The configuration of Profile Container is accomplished through registry settings and user groups. Registry settings may be managed manually, with Group Policy, or using alternate preferred methods. Configuration settings for Profile Container are set in HKLM\SOFTWARE\FSLogix\Profiles.

- **Full Profile Container Registry Settings Reference**
- **Create a Group Policy Object**

These settings are required to enable Office Container and to specify the location for the profile VHD to be stored. The minimum required settings to enable Profile Containers are:



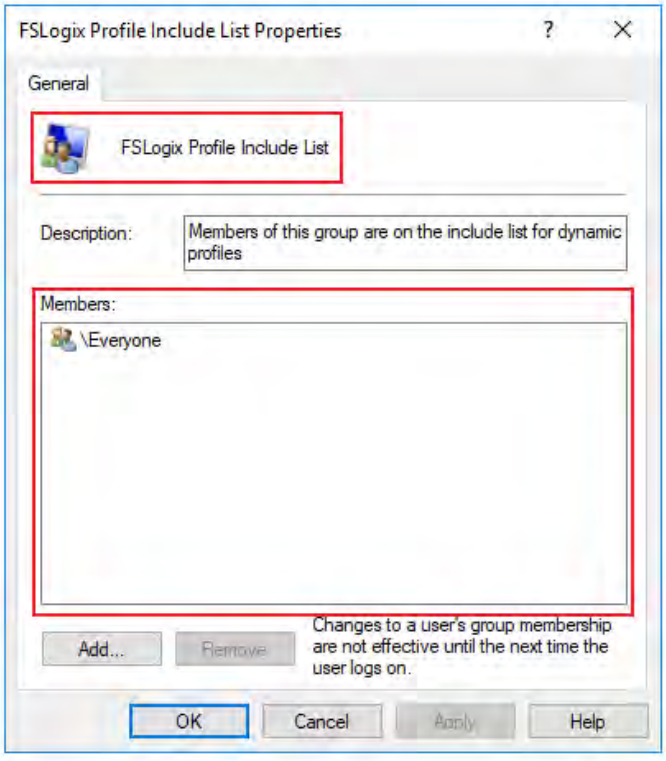
These settings are often helpful when configuring Profile Container but are not required.

Value	Type	Configured Value	Description
DeleteLocalProfileWhenVHDShouldApply	DWORD	0	0: no deletion. 1: delete local profile if exists and matches the profile being loaded from VHD. **NOTE: Use caution with this setting. When the FSLogix Profiles system determines a user should have a FSLogix profile, but a local profile exists, Profile Container permanently deletes the local profile. The user will then be signed in with an FSLogix profile.**
FlipFlopProfileDirectoryName	DWORD	0	When set to '1' the SID folder is created as "%username%%sid%" instead of the default "%sid%%username%". This setting has the same effect as setting **SIDDirNamePattern** = "%username%%sid%" and **SIDDirNameMatch** = "%username%%sid%".
PreventLoginWithFailure	DWORD	0	If set to 1 Profile Container will load FRXShell if there's a failure attaching to, or using an existing profile VHD(X). The user will receive the FRXShell prompt - default prompt to call support, and the users only option will be to sign out.
PreventLoginWithTempProfile	DWORD	0	If set to 1 Profile Container will load FRXShell if it's determined a temp profile has been created. The user will receive the FRXShell prompt - default prompt to call support, and the users only option will be to sign out.

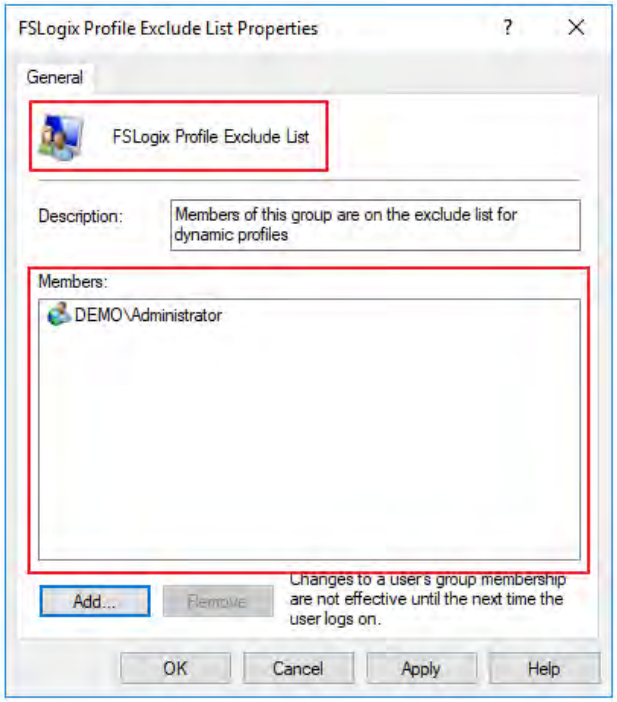
Set up Include and Exclude User Groups

There are often users, such as local administrators, that have profiles that should remain local. During installation, four user groups are created to manage users whose profiles are included and excluded from Profile Container and Office Container redirection.

By default, everyone is added to the FSLogix Profile Include List group.

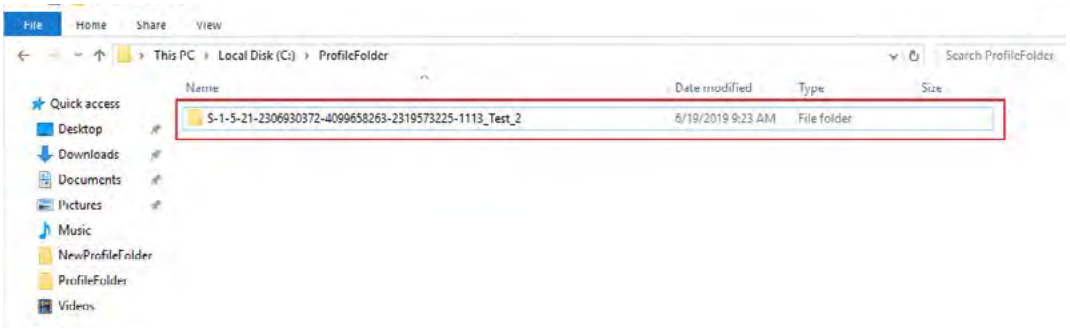


Adding a user to the FSLogix Profile Exclude List group means that the FSLogix agent will not attach a FSLogix profile container for the user. In the case where a user is a member of both the exclude and include groups, exclude takes priority.



Testing FSLogix

Profile Containers is now configured and ready to be used. In order to verify that Profile Container is working, sign in as a user in the Included List group. Using File Manager, navigate to the location specified in VHDLocations. Verify that a folder, with the user name and SID has been created.



The login profile and start menu layout should be identical from one computer to another. Once this is verified you can then start customizing your desired default profile layout.

This concludes our tutorial on setting up user profiles.

Folder Redirection

This topic describes how to use Windows Server to deploy Folder Redirection with Offline Files to Windows client computers.

Enables users and administrators to redirect the path of a known folder to a new network share or location either manually or by using Group Policy. The new location can be a folder on the local computer or a directory on a file server share. Users interact with files in the redirected folder as if it still existed on the local drive. For example, you can redirect the Documents folder and/or Email datafiles, which are usually stored on a local drive, to a network location. The files in the folder are then available to the user from any computer on the network.

Pros:

- Faster Login due to reduced data size within a profile
- Allows you to store mail datafiles and user data in a centralized share or other network location
- Protects data loss from user profile corruption

Cons:

- It adds a slight amount of complexity to the user login setup process
- Additional administration and data backup resources required

Prerequisites

Folder Redirection has the following software requirements:

- To administer Folder Redirection, you must be signed in as a member of the Domain Administrators security group, the Enterprise Administrators security group, or the Group Policy Creator Owners security group.
- To administer Roaming User Profiles, you must be signed in as a member of the Domain Administrators security group, the Enterprise Administrators security group, or the Group Policy Creator Owners security group.
- Client computers must run Windows 10, Windows 8.1, Windows 8, Windows 7, Windows Vista, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2, or Windows Server 2008.
- Client computers must be joined to the Active Directory Domain Services (AD DS) that you are managing.
- A computer must be available with Group Policy Management and Active Directory installed.
- A file server with sufficient storage capacity must be available to host roaming user profiles.

Step 1:

Create a folder redirection security group.

If your environment is not already set up with Folder Redirection, the first step is to create a security group that contains all users to which you want to apply Folder Redirection policy settings.

Create a security group for Folder Redirection:

1. Open Active Directory Users and Groups on your AD Server.
2. Right-click the appropriate domain or OU, select New, and then select Group.
3. In the Create Group window, in the Group section, specify the following settings:
   - In Group name, type the name of the security group, for example: Folder Redirection Users.
   - In Group scope, select Security, and then select Global.
4. In the Members section, select Add. The Select Users, Contacts, Computers, Service Accounts or Groups dialog box appears.
5. Type the names of the users or groups to which you want to deploy Folder Redirection, select OK, and then select OK again.

Step 2:

Create a file share for redirected folders. If you do not already have a file share for redirected folders, use the following procedure to create a file share on a server running Windows Server 2012 or later.

Create a file share on Windows Server 2019, Windows Server 2016, and Windows Server 2012:

1. In the Server Manager navigation pane, select File and Storage Services, and then select Shares to display the Shares page.
2. In the Shares tile, select Tasks, and then select New Share. The New Share Wizard appears.
3. On the Select Profile page, select SMB Share – Quick. If you have File Server Resource Manager installed and are using folder management properties, instead select SMB Share - Advanced.
4. On the Share Location page, select the server and volume on which you want to create the share.
5. On the Share Name page, type a name for the share (for example, Users$) in the Share name box.
   Note: When creating the share, hide the share by putting a $ after the share name. This will hide the share from casual browsers.
6. On the Other Settings page, clear the Enable continuous availability checkbox, if present, and optionally select the Enable access-based enumeration and Encrypt data access checkboxes.
7. On the Permissions page, select Customize permissions. The Advanced Security Settings dialog box appears.
8. Select Disable inheritance, and then select Convert inherited permissions into explicit permission on this object.
9. Set the permissions as described Table 1 and shown in Figure 1, removing permissions for unlisted groups and accounts, and adding special permissions to the Folder Redirection Users group that you created in Step 1.

User Account	Access	Applies to
System	Full control	This folder, subfolders and files
Administrators	Full control	This folder only
Creator/Owner	Full control	Subfolders and files only
Security group of users needing to put data on share (Roaming User Profiles Users and Computers)	List folder / read data (Advanced permissions) Create folders / append data (Advanced permissions)	This folder only
Other groups and accounts	None (remove)	

10. If you chose the SMB Share - Advanced profile, on the Management Properties page, select the User Files Folder Usage value.
11. If you chose the SMB Share - Advanced profile, on the Quota page, optionally select a quota to apply to users of the share.
12. On the Confirmation page, select Create.

Required permissions for the file share hosting redirected folders.

Step 3:

Create a GPO for Folder Redirection:

If you do not already have a GPO created for Folder Redirection settings, use the following procedure to create one.

Create a GPO for Folder Redirection:

1. Open Group Policy Management from your AD server.
2. From the Tools menu, select Group Policy Management.
3. Right-click the domain or OU in which you want to setup Folder Redirection, then select Create a GPO in this domain, and Link it here.
4. In the New GPO dialog box, type a name for the GPO (for example, Folder Redirection Settings), and then select OK.
5. Right-click the newly created GPO and then clear the Link Enabled checkbox. This prevents the GPO from being applied until you finish configuring it.
6. Select the GPO. In the Security Filtering section of the Scope tab, select Authenticated Users, and then select Remove to prevent the GPO from being applied to everyone.
7. In the Security Filtering section, select Add.
8. In the Select User, Computer, or Group dialog box, type the name of the security group you created in Step 1 (for example, Folder Redirection Users), and then select OK.
9. Select the Delegation tab, select Add, type Authenticated Users, select OK, and then select OK again to accept the default Read permissions.

Step 4:

Configure folder redirection with Offline Files.

After creating a GPO for Folder Redirection settings, edit the Group Policy settings to enable and configure Folder Redirection, as discussed in the following procedure.

Note: Offline Files is enabled by default for redirected folders on Windows client computers, and disabled on computers running Windows Server, unless changed by the user. To use Group Policy to control whether Offline Files is enabled, use the Allow or disallow use of the Offline Files feature policy setting.

Configure Folder Redirection in Group Policy:

1. In Group Policy Management, right-click the GPO you created (for example, Folder Redirection Settings), and then select Edit.
2. In the Group Policy Management Editor window, navigate to User Configuration, then Policies, then Windows Settings, and then Folder Redirection.
3. Right-click a folder that you want to redirect (for example, Documents), and then select Properties.
4. In the Properties dialog box, from the Setting box, select Basic - Redirect everyone's folder to the same location.
5. In the Target folder location section, select Create a folder for each user under the root path and then in the Root Path box, type the path to the file share storing redirected folders, for example: \\fs1.corp.contoso.com\users$
6. Select the Settings tab, and in the Policy Removal section, optionally select Redirect the folder back to the local user profile location when the policy is removed (this setting can help make Folder Redirection behave more predictably for administrators and users).
7. Select OK, and then select Yes in the Warning dialog box.

Step 5:

Enable the Folder Redirection GPO.

Once you have completed configuring the Folder Redirection Group Policy settings, the next step is to enable the GPO, permitting it to be applied to affected users.

Enable the Folder Redirection GPO:

1. Open Group Policy Management.
2. Right-click the GPO that you created, and then select Link Enabled. A checkbox will appear next to the menu item.

Step 6:

Test Folder Redirection.

To test Folder Redirection, sign in to a computer with a user account configured for Folder Redirection. Then confirm that the folders and profiles are redirected.

Test Folder Redirection:

1. Sign in to a primary computer with a user account for which you have enabled Folder Redirection.
2. If the user has previously signed in to the computer, open an elevated command prompt, and then type the following command to ensure that the latest Group Policy settings are applied to the client computer: gpupdate / force
3. Open File Explorer.
4. Right-click a redirected folder (for example, the My Documents folder in the Documents library), and then select Properties.
5. Select the Location tab and confirm that the path displays the file share you specified instead of a local path.

Checklist for deploying Folder Redirection

Status	Action
☐ ☐ ☐	1. Prepare domain - Join computers to domain - Create user accounts
☐	2. Create security group for Folder Redirection - Group name: - Members:
☐	3. Create a file share for redirected folders - File share name:
☐	4. Create a GPO for Folder Redirection - GPO name:
☐ ☐ ☐ ☐ ☐	5. Configure Folder Redirection and Offline Files policy settings - Redirected folders: - Offline Files enabled? (enabled by default on Windows client computers) - Always Offline Mode enabled? - Background file synchronization enabled? - Optimized Move of redirected folders enabled?
☐ ☐ ☐ ☐	6. (Optional) Enable primary computer support - Computer-based or User-based? - Designate primary computers for users - Location of user and primary computer mappings: - (Optional) Enable primary computer support for Folder Redirection - (Optional) Enable primary computer support for Roaming User Profiles
☐	7. Enable the Folder Redirection GPO
☐	8. Test Folder Redirection

4AA7-7144ENW, March 2020.