Profile Management 7.15

Aug 14, 2017

Profile Management is intended as a profile solution for XenApp servers, virtual desktops created with XenDesktop, and physical desktops. You install Profile Management on each computer whose profiles you want to manage.

Active Directory Group Policy Objects allow you to control how Citrix user profiles behave. Although many settings can be adjusted, in general you only need to configure a subset, as described in these topics.

The best way of choosing the right set of policy selections to suit your deployment is to answer the questions in the topic called Decide on a configuration.

Usage rights for this feature are described in the end-user license agreement (EULA).

For information on the terminology used in these topics, see Profile Management glossary.

What's new

Aug 14, 2017

This version includes the following key enhancement and addresses several customer reported issues to improve the user experience.

Enhancement for using wildcards. You can use the vertical bar '|' for applying a policy to only the current folder without propagating it to the subfolders. For details, see Using wildcards.

Fixed issues

Aug 14, 2017

Compared to: Citrix Profile Management 5.8

Profile Management 7.15 contains the following fixes compared to Profile Management 5.8:

- When you attempt to open files in a profile with Profile Streaming enabled, the file might appear empty after you log on.

  [#LC6996]

- Servers might experience a fatal exception, displaying a blue screen, on upmjit.sys with bugcheck code 0x135.

  [#UPM-514, #LC7841]

- UserProfileManager.exe might exit unexpectedly when you log on to a VDA.

  [#UPM-576, #LC7952]

- The Folders to mirror policy is not working when it is configured within an excluded folder and you have enabled logon exclusion check.

  [#UPM-578, #LC8153]

- Group policies in Citrix Studio are missing if the policy "UPM - Software\Microsoft\Speech_OneCore" under "Profile Management - Registry - Default Exclusion" was configured before upgrading the Delivery Controller from 7.13 to 7.14.

  [#UPM-538, #LC8155]

Known issues

Aug 14, 2017

The following known issue exists in this version:

There might be logon delay for the published desktop when you have enabled Profile Management.

[#UPM-552, #LC7596]

System requirements

Aug 14, 2017

Systems running Profile Management 5.x must be based on one of the following operating systems:

- **Desktops** - Microsoft Windows 7, Windows 8, Windows 8.1, and Windows 10.
  In XenDesktop environments, Windows Store applications (also known as Metro apps) are supported on dedicated desktops and on desktops with personal vDisks, but not on other desktop types.

- **Servers** - Standard, Enterprise, and Datacenter Editions of Windows Server 2016, Windows Server 2008 (including Windows Server 2008 R2) and Windows Server 2012 (including Windows Server 2012 R2).

With Enhanced Protected Mode (EPM), cookies in Microsoft Internet Explorer 10 or later are not supported on Windows 7 or later. When EPM is enabled, cookies are not processed or handled by Profile Management.

Every user should have access to the user store, a network folder where profiles are stored centrally. Alternatively, profiles can be stored in users' home drives if preferred. For more information, see Profile Management architecture.

Unless you use XenDesktop 7, where Profile Management is integrated into Desktop Studio, Active Directory (AD) Group Policy Objects (GPOs) are required for configuration. AD forest functional and domain functional levels of Windows Server 2008 and Windows Server 2012 native mode are supported. For more information, see Domain and forest support in Profile Management. Alternatively, you can use a local .ini file for configuration settings, but in general the .ini file should be used for testing purposes only. Note that settings in the .ini file are applied for any setting not configured in the GPO, that is any Group Policy setting that is left in the Not Configured state.

If short file names (also known as 8.3 file names) are mandated in a Citrix product or component you are using with Profile Management, do not turn off support for short file names in your Profile Management deployment. Doing so may cause issues when files are copied to and from the user store.

On computers running the Profile Management Service, store profiles on a single disk mounted by drive letter. If a disk is mounted into a folder that is used to store a user's profile (a typical example is C:\Users), it might be masked from the Service and not processed.

Profile Management 5.x can be used with these Citrix products:

- XenDesktop
- XenApp
- VDI-in-a-Box

For the compatibility matrix of Profile Management and XenApp and XenDesktop, see Additional Lifecycle Information for Citrix Profile Management.

To download Profile Management

1. Navigate to the Citrix download page.
2. Log on to My Account. Your account must be associated with the licensing entitlement for the Citrix product that you

have deployed. If your account is not associated with your license entitlement, contact Citrix Customer Service.
3. In Find Downloads, select your product and select Components as the download type.
4. Download the latest version of Profile Management.

Before you can use Citrix Diagnostic Facility to capture trace logs, ensure it is available with the Citrix product or component that is used on the device, virtual desktop, or Citrix server whose profiles you want to monitor.

If you use Citrix XenApp to stream applications to user devices, install the Citrix offline plug-in (formerly called XenApp Plug-in for Streamed Apps) 1.3.1 or later on user devices. Version 1.2 of this plug-in changed the location of per-user disk storage for streamed application settings, resulting in user preferences being lost at logoff. With Version 1.3.1 or later, these settings are stored in %LOCALAPPDATA%, and follow the user from device to device without data loss. No configuration of Profile Management is required with this later version of the plug-in.

Although it is unsupported, if you must use XenApp Plugin for Streamed Apps 1.2 see CTX120006 for a workaround to the data-loss issue.

To use the cross-platform settings feature in this release, Microsoft Core XML Services (MSXML) 6.0 Service Pack 1 or later must be installed on all computers running the Profile Management Service. This component is part of Microsoft .NET Framework 3.5 and is required in order to process definition files. For more information on MSXML 6.0 Service Pack 1, including its system requirements, see http://www.microsoft.com/downloads/en/details.aspx?FamilyID=d21c292c-368b-4ce1-9dab-3e9827b70604&displaylang=en.

Use this feature only with the supported set of operating systems and applications. For more information, see Operating systems and applications supported By cross-platform settings.

Migration from the following profile types to Citrix user profiles is supported:

- Windows roaming profiles
- Local profiles based on any of the following operating systems:
  - Windows 10
  - Windows 8
  - Windows 7
  - Windows Vista
  - Windows XP
  - Windows Server 2016
  - Windows Server 2012 R2
  - Windows Server 2012
  - Windows Server 2008 R2
  - Windows Server 2008
  - Windows Server 2003
- Citrix user profiles created with User Profile Manager 2.0

Migration from the following profile types to Citrix user profiles is unsupported:

- Microsoft mandatory profiles.
  Tip: You can use the template profile feature of Profile Management to configure a Microsoft mandatory profile as a Citrix mandatory profile. Citrix mandatory profiles are used for all logons and function exactly like regular Citrix user profiles except that no user changes are saved. For information, see To specify a template or mandatory profile.
- Citrix mandatory profiles.
- Citrix user profiles created with a User Profile Manager Technical Preview release or beta release.
- Third-party profiles (including sepagoPROFILEs).

You cannot upgrade from a 32-bit Citrix user profile to a 64-bit one.

How Profile Management works

Aug 14, 2017

Profile Management addresses user profile deficiencies in environments where simultaneous domain logons by the same user introduce complexities and consistency issues to the profile. For example, if a user starts sessions to two different virtual resources based on a roaming profile, the profile of the session that terminates last overrides the profile of the first session. This problem, known as "last write wins", discards any personalization settings that the user makes in the first session.

You can tackle the problem by using separate profiles for each resource silo. However, this results in increased administration overhead and storage capacity requirements. Another drawback is that users will experience different settings depending on the resource silo they access.

Profile Management optimizes profiles in an easy and reliable way. At interim stages and at logoff, registry changes, as well as files and folders in the profile, are saved to the user store for each user. If, as is common, a file already exists, it is overwritten if it has an earlier time stamp.

At logon, users' registry entries and files are copied from the user store. If a locally cached profile exists, the two sets are synchronized. This makes all settings for all applications and silos available during the session and it is no longer necessary to maintain a separate user profile for each silo. Citrix streamed user profiles can further enhance logon times.

Profile Management helps to safeguard application settings for mobile users who experience network disruption (if the offline profiles features is configured) and users who access resources from different operating systems (if the cross-platform settings feature is configured).

Note: Profile Management processes domain user logons not local accounts.
For a more detailed overview of Profile Management, search the Profile Management blog at http://blogs.citrix.com/tag/user_profile_manager.

Where network-based profiles are employed, consider adopting Profile Management in your organization. You may be able to implement other solutions such as mandatory or roaming profiles, and maintain them with standard knowledge of Microsoft Windows. However, unless your deployment is very restricted (for example, a call center where user customization is very limited so mandatory profiles are appropriate), Profile Management may be preferred.

Citrix recommends using folder redirection so that user-specific data is saved separately from the profile.

The home-folder and template paths must be configured only with the network location.

About profiles

Aug 14, 2017

A Windows user profile is a collection of folders, files, registry settings, and configuration settings that define the environment for a user who logs on with a particular user account. These settings may be customizable by the user, depending on the administrative configuration. Examples of settings that can be customized are:

- Desktop settings such as wallpaper and screen saver
- Shortcuts and Start menu setting
- Internet Explorer Favorites and Home Page
- Microsoft Outlook signature
- Printers

Some user settings and data can be redirected by means of folder redirection. However, if folder redirection is not used these settings are stored within the user profile.

Windows includes several types of profiles:

Profile Type	Storage Location	Configuration Location	Application	Save Changes?
Local	Local device	Local device	Local device only	Yes
Roaming	Network	Active Directory	Any device accessed	Yes
Mandatory (Mandatory Roaming)	Network	Active Directory	Any device accessed	No
Temporary	Not Applicable	Not Applicable	Local device only	No

A temporary profile is only assigned when a specific profile type cannot be assigned. With the exception of mandatory profiles, a distinct profile typically exists for each user. In addition, mandatory profiles do not allow users to save any customizations.

For Remote Desktop Services users, a specific roaming or mandatory profile can be assigned to avoid issues that may occur if the same profile is assigned to a user within a Remote Desktop Services session and a local session.

Windows user profiles are versioned by Microsoft as follows:

- Version 5 – Windows 10
- Version 4 – Windows 8.1 and Windows Server 2012 R2
- Version 3 - Windows 8 and Windows Server 2012

- Version 2 - Windows Vista, Windows 7, Windows Server 2008, and Windows Server R2
- Version 1 – Operating systems earlier than Windows Vista and Windows Server 2008

The folder structure (or namespace) of Microsoft's Version 1 profiles is mostly interchangeable. For example, the folders on Windows XP and Windows Server 2003 are almost identical. Likewise, the structure of Version 2 profiles is mostly interchangeable.

However, the namespace is different between Version 1 and later profiles. This folder structure was changed in the later operating systems to provide user-specific folders isolated for user and application data. Version 1 profiles store data in the root folder, Documents and Settings. Version 2 profiles store data in a more intuitively named folder called Users. For example, the folder contents of AppData\Local in Windows Vista is the same as the contents of Documents and Settings\<username>\Local Settings\Application Data in Windows XP.

For more information about the differences between Version 1 and later profiles, see Managing Roaming User Data Deployment Guide.

Assign profiles

Aug 14, 2017

This topic refers to the assignment of profiles in Microsoft Windows not Citrix Profile Management.

You can assign profiles to users in several ways:

- Using their user account properties in Active Directory (AD)
- Using Group Policy (GP)
- Using the above methods to assign profiles specific to Remote Desktop Services (formerly known as Terminal Services) sessions

Some of these methods are only available in specific operating systems:

- **Remote Desktop Services**. To assign Remote Desktop Services profiles on Windows Server 2008 R2, use the GPO setting Set path for Remote Desktop Services Roaming User Profile, which is located in Computer Configuration\Administrative Templates\Windows Component\Remote Desktop Services\Remote Desktop Session Host\Profiles. On earlier server operating systems, use the setting Set path for TS Roaming Profiles, which is located in Computer Configuration\Administrative Templates\Windows Components\Terminal Services.
  To configure profiles for individual users, you can also set Set path for TS Roaming Profiles on the individual accounts in the User Account Properties pages in AD. However, typically it is much better to make this assignment in GP.

  You can use the setting Use mandatory profiles on the terminal server to force the use of mandatory profiles.

- **Windows 7, Windows 8, and Windows Server**: Set roaming profiles on individual accounts using the User Account Properties pages. Additionally, for Windows Server 2008 AD and Windows 7 devices, you can use the GPO setting Set roaming profile path for all users logging onto this computer. This is located in Computer\Administrative Templates\System\User Profiles. For users logging on to Windows 8 or Windows Server 2012 computers, you can also set users' home folders using Active Directory in Windows Server 2012.

When Profile Management is used to manage a user's profile, it takes precedence over any other profile assignment method. A user whose profile data is not managed by Profile Management might be assigned a profile using multiple methods. The actual profile used is based on the following precedence:

1. Citrix user profile (that is, a profile created by Profile Management)
2. Remote Desktop Services profile assigned by a GPO
3. Remote Desktop Services profile assigned by a User Property
4. Roaming profile assigned by a GPO (Windows Server 2008 AD and Windows 7 only)
5. Roaming profile assigned by a User Property

Profile Management architecture

Aug 14, 2017

This topic describes the folder structure of the user store and of the cross-platform settings store. The user store is the central location for Citrix user profiles. The cross-platform settings store is a separate location.

The structures of the user store and cross-platform settings store are described here for information purposes and to assist with localizing and troubleshooting. Follow these important recommendations, which are designed to minimize problems with profile data and maintain security:

- Do not change the structure of either store.
- Do not write files and folders directly to any part of a store. The user store is different in this respect from any redirected folders.
- Keep the user store separate from any redirected folders. You can keep them on disjoint shares of the same file server or DFS namespace, for example \\server1\profiles\%username% and \\server1\folders\%username%. This technique also makes it much easier to support Version 1 and Version 2 profiles together, and to support a single set of redirected folders shared by both profile versions.
- Users do not need to see the user store, so do not map a drive letter to it.
- Do not impose quotas on the user store. If you need to restrict profile size, consider excluding items rather than using a quota.

The user store defaults to the WINDOWS folder in the user's home directory. This simplifies pilot installations, but for production systems, you should configure the user store to be a network share or (for best scalability) a DFS namespace. Supported configurations for enterprise-ready user stores are described in High availability and disaster recovery with Profile Management.

Recommendations on creating secure user stores are available in the article called Create a file share for roaming user profiles on the Microsoft TechNet Web site. These are minimum recommendations that ensure a high level of security for basic operation. Additionally, when configuring access to the user store include the Administrators group, which is required in order to modify or remove a Citrix user profile.

Note: On Windows 7 and Windows 2008 R2 client devices, do not select the Encrypt data access checkbox while creating the share on Windows 2012 R2 File Server.

The folder structure of the user store at the root level is shown in this table.

Folder	Notes
\	The root of a profile in the user store.
\UPM_Profile	This contains files and folders from the profile.
\UPM_Drive_C	This folder contains any included items from outside the profile (in this case from drive C). This folder will only be present during upgrades from Profile Management 4.x or earlier. Managing items outside

Folder	Notes
	the profile is not supported in Profile Management 5.0.
\Pending	This folder contains the lock file, any pending files, and the stamp file if the streaming feature is in use.

Some examples are shown in this table.

Example Folder Name	Notes
\UPM_Profile\Data	The synchronized content of the Data folder in the user profile.
\UPM_Profile\AppData_upm_var	The synchronized content of the de-localized Application Data folder in the user profile. This folder will only be present during upgrades from Profile Management 4.x or earlier. Managing Version 1 profiles (of which Application Data is an example folder) is not supported in Profile Management 5.0.

The user store includes the pending area. This is a holding area used by the streamed user profiles and active write back features. All files are synchronized from the pending area to the user store after a user logs off from their last session. New sessions download files from both the user store and the pending area, so the user always experiences an up-to-date profile.

In the event that a server becomes unresponsive, a timeout can be set that releases files in the pending area back to the user store (if configured as part of the streamed user profiles feature).

When using the cross-platform settings feature, multiple platforms are involved. This means you must define platform-specific folders to separate the profiles for each platform. Typically, you do this using Profile Management variables in the Path to user store policy (for example, using %USERNAME%\!CTX_OSNAME!!CTX_OSBITNESS! in the path).

The cross-platform settings store holds the settings for supported applications after the cross-platform settings feature is configured. You specify the name and location of the store during configuration (using the Path to cross-platform settings store policy). The store holds the subset of the user's settings that roam between operating systems.

For example, you may want to roam settings between Windows XP and Windows 7. The platform-specific folders contain the user settings that are unique to Windows XP and Windows 7; the cross-platform settings store contains the subset of the settings that roam between these operating systems. At logon, this subset is copied into, and remains part of, the platform-specific folders. At logoff, any changes to the subset are extracted and placed back into the cross-platform settings store.

Each platform-specific folder contains standard subfolders (for example, UPM_Profile). For information on these, see Folder structure of the user store. In addition, the UPM_CPS_Metadata subfolder is present. This system-created folder contains temporary settings that are shared across operating systems.

Citrix user profiles cannot be managed across forests. They can be managed across domains in the same forest allowing

multiple users with the same logon name to access the same resources in the forest. This involves uniquely identifying profiles with the %USERDOMAIN% and %USERNAME% variables in the path to the user store.

However, in this case you must use variables to disambiguate identical logon names when setting the path to the user store. To do this, append the domain name variable to the path. You must also set permissions on the user store and enable Profile Management's Processed Groups setting using Active Directory's Universal Groups.

You can use a manually defined system variable such as %ProfVer% to set the operating system version, or a Profile Management variable to set the operating system name, bitness, or the profile version. For examples of user store paths in AD forests, see To specify the path to the user store.

The following table provides an overview of how Profile Management localizes and de-localizes folders when profile data is moved to and from the user store. Only folder names are localized and de-localized. For example, Start menu entries and registry settings are not translated into the correct language by Profile Management.

This information is relevant only when upgrading from Profile Management 4.x or earlier, when Version 1 profiles may be present. Managing Version 1 profiles is not supported in Profile Management 5.0.

Version 1 English Folder	User Store Folder	Full Path Relative to the User Profile
Accessibility	Accessibility_upm_var	\Start Menu\Programs\Accessories\
Accessories	Accessories_upm_var	\Start Menu\Programs\
Administrative Tools	AdminTools_upm_var	\Start Menu\Programs\
Application Data	AppData_upm_var	\Local Settings\
Cookies	Cookies_upm_var	\
Desktop	Desktop_upm_var	\
Entertainment	Entertainment_upm_var	\Start Menu\Programs\Accessories\
Favorites	Favorites_upm_var	\
History	History_upm_var	\Local Settings\
Links	Links_upm_var	\Favorites\
Local Settings	LocalSettings_upm_var	\

Version 1 English Folder	User Store Folder	Full Path Relative to the User Profile
My Documents	MyDocuments_upm_var	\
My Music	MyMusic_upm_var	\My Documents\
My Pictures	MyPictures_upm_var	\My Documents\
My Videos	MyVideos_upm_var	\My Documents\
NetHood	NetHood_upm_var	\
PrintHood	PrintHood_upm_var	\
Programs	Programs_upm_var	\Start Menu\
Recent	Recent_upm_vars	\
Start Menu	StartMenu_upm_var	\
Templates	Templates_upm_var	\
Temporary Internet Files	TemporaryInternetFiles_upm_var	\Local Settings\
SendTo	SendTo_upm_var	\
Startup	Startup_upm_var	\Start Menu\Programs\
System Tools	SystemTools_upm_var	\Start Menu\Programs\Accessories\

Profile Management use cases

Aug 14, 2017

Citrix Profile Management can be implemented to manage users' profiles in different scenarios regardless of how applications are delivered to users or where they are housed. The following are examples of these scenarios:

- Citrix XenApp with published applications
- Citrix XenApp with published desktops
- Citrix XenApp with applications streamed into an isolation environment
- Applications streamed to XenDesktop virtual desktops
- Applications installed on XenDesktop virtual desktops
- Applications streamed to physical desktops
- Applications installed locally on physical desktops

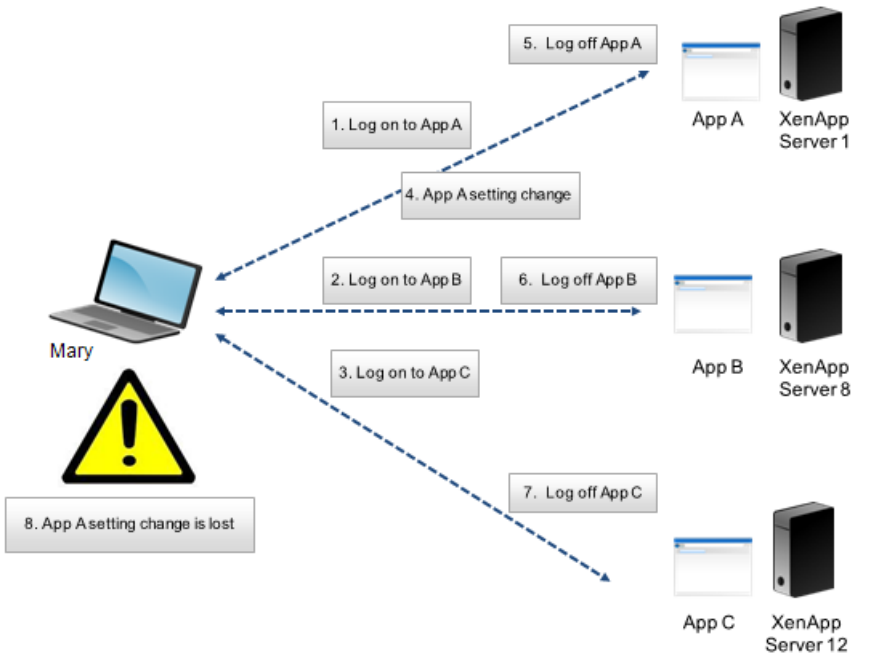
Of these, Citrix sees the following as the most common use cases:

- **Multiple sessions** - The user accesses multiple XenApp server silos and therefore has multiple sessions open. Note however that application isolation and streaming on the server are alternatives to server silos. This scenario is described in more detail in this topic.
- **"Last write wins" and roaming profile consistency issues** - Because the last write to the roaming profile causes all settings to be saved, roaming profiles may not retain the right data if multiple sessions are open and interim changes are made. In addition, settings may not be written correctly to the profile as a result of network, storage issues, or other problems. This scenario is described in more detail in this topic.
- **Large profiles and logon speed** - Profile bloat can make user profiles unwieldy resulting in storage and management issues. Typically, during logon Windows copies the user's entire profile over the network to the local user device. For bloated profiles, this can prolong the user's logon time.

Especially in large environments, it may be necessary for users to open multiple sessions to access different applications that are housed on different XenApp servers, whether in the same farm or multiple farms. Where possible, Citrix administrators should consider application isolation or streaming in order to house applications on the same XenApp server to allow users to access all applications from a single server and thus a single session. However, this may not be possible if a business unit controls specific servers or applications cannot be streamed.

Once it has been determined that it is indeed necessary for users to access applications from various XenApp servers, the impact on profiles should be ascertained.

This diagram illustrates the example below, where application settings may be lost when multiple sessions exist.



For example, Mary has the need to access AppA, AppB, and AppC and she is routed to Server 1, Server 8, and Server 12 respectively. Upon logon to each application, her Terminal Services roaming profile is loaded onto each server and folders are redirected for each session. When she is logged onto AppA on Server1, Mary changes Setting1 and logs off that session. She then completes her work in the other two applications and logs off.

At logoff, the change that Mary made within her session on Server 1 is overwritten because the settings within the last closed session are retained, not the interim change. When Mary logs onto AppA the next day, she is frustrated because the change she made is not visible.

Profile Management can generally prevent this situation from occurring. Profile Management only writes back the specific settings that were changed during a session; all other unchanged settings remain untouched. So the only potential conflict that would arise is if Mary changed Setting1 within another session. However, the user would likely expect that the most recent change was retained, which is the case, if Profile Management is used in this scenario.

This scenario is similar to the first one in this topic. "Last write wins" issues can present themselves in a variety of ways, and user frustration can mount as the number of devices accessed increases.

Because the roaming profile retains all profile data, with the exception of folders that have been redirected, the user profile can grow quite large. Not only does this add to the logon time because the profile must be downloaded, the potential for inconsistency grows during the write phase of the logoff, especially where network issues exist.

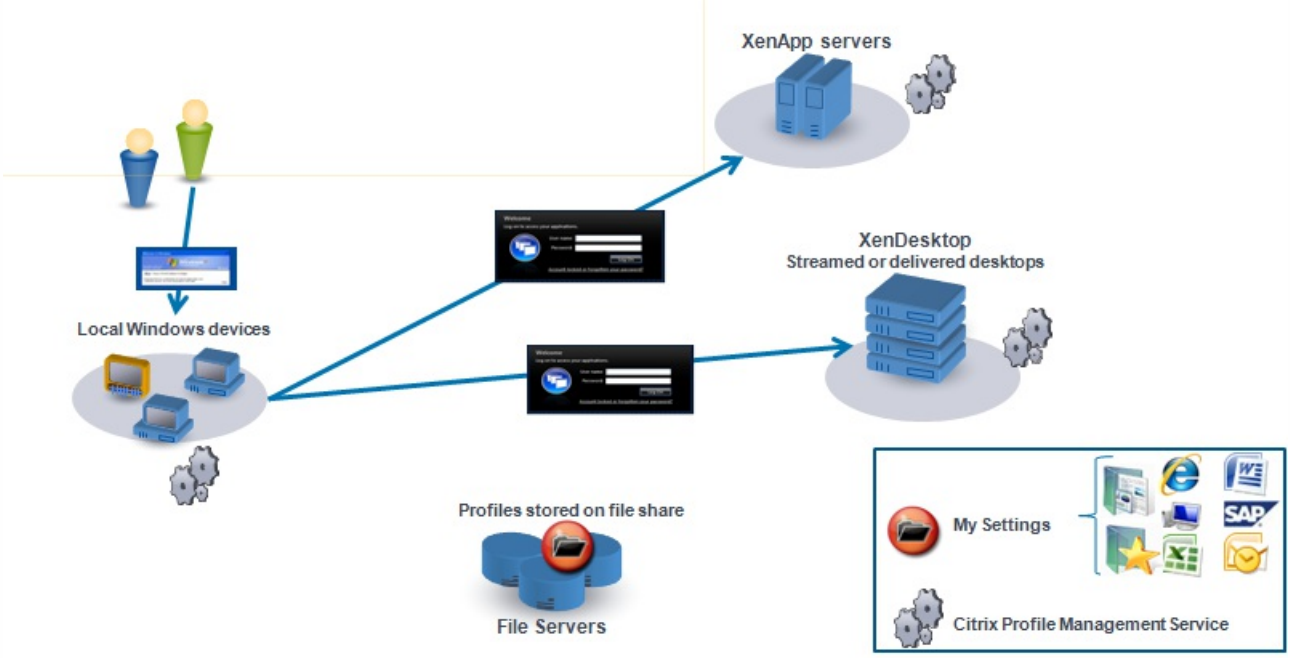
Profile Management enables specific data to be excluded from the user profile, enabling the user profile to be kept to a minimal size. Because only differences are written to the profile, the write phase of the logoff involves less data and is faster. Profile Management can be beneficial for applications that use profiles for temporary data but do not clean them up when the applications terminate.

Access multiple resources

Aug 14, 2017

Profiles become more complex as users access multiple resources. With profiles stored on a network, Microsoft Windows uses the registry to store user settings. Profiles are copied from the network to the local device at logon, and copied back to the network at logoff. On a daily basis, users access multiple computers, switch between desktops and laptops, and access virtual resources created with Citrix XenDesktop and Citrix XenApp.

This diagram illustrates how a single Citrix user profile follows a user who logs on to multiple resources.



For example, a user has a local, physical desktop and from it accesses applications published with XenApp. They also access a virtual desktop created with XenDesktop. The user's settings will not be uniform across all of these resources unless the settings are appropriately configured.

In addition, when they access a shared resource, the behavior of roaming profiles means that the "last write wins". For example, an administrator enables a roaming profile and a user changes the background color of the local desktop. The user then logs on to a XenDesktop virtual desktop, logs off the local desktop, and logs off the virtual desktop. Because both the local and virtual desktops were open at the same time and the last logoff was from the virtual desktop, the settings from the virtual desktop session were the last written to the profile, and the change to the background color is lost.

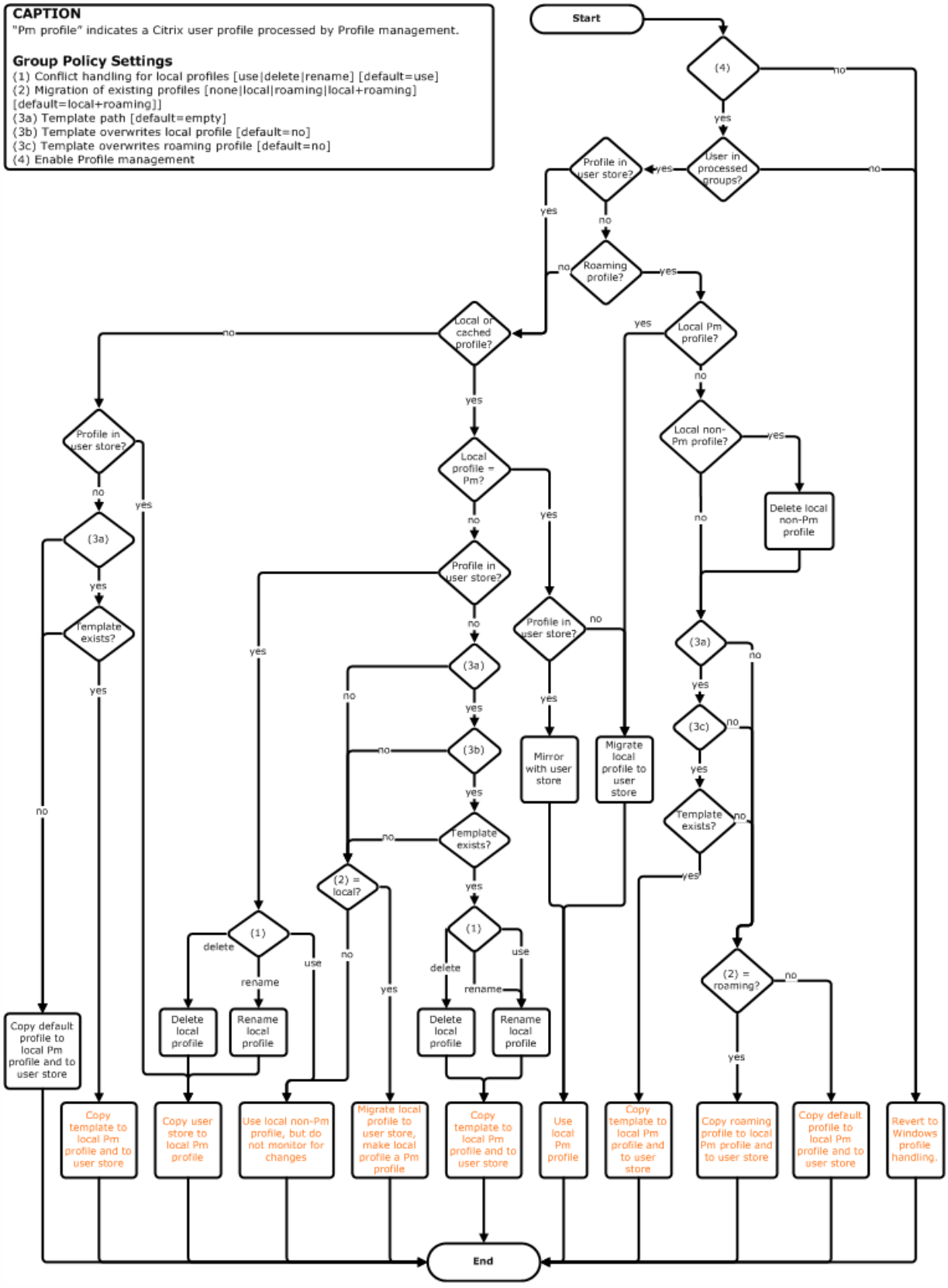
Logon diagram

Aug 14, 2017

This diagram helps you work out the details of your user profile migration strategy. It also explains these aspects of performance:

- When you migrate a profile, two network copies can take place, which slows down the logon process. For example, the operation “Copy default profile to local Pm profile and to user store” first involves a full profile copy from the roaming profile store to the local computer and then a second full profile copy from the local computer to the user store.
- When a cached profile is used, no copying of profile data across the network takes place.

Read the diagram from the bottom to the top. Check the desired operations in the boxes at the bottom (for example, “Copy default profile to local Pm profile and to user store”) and track a path back to identify the required migration settings.



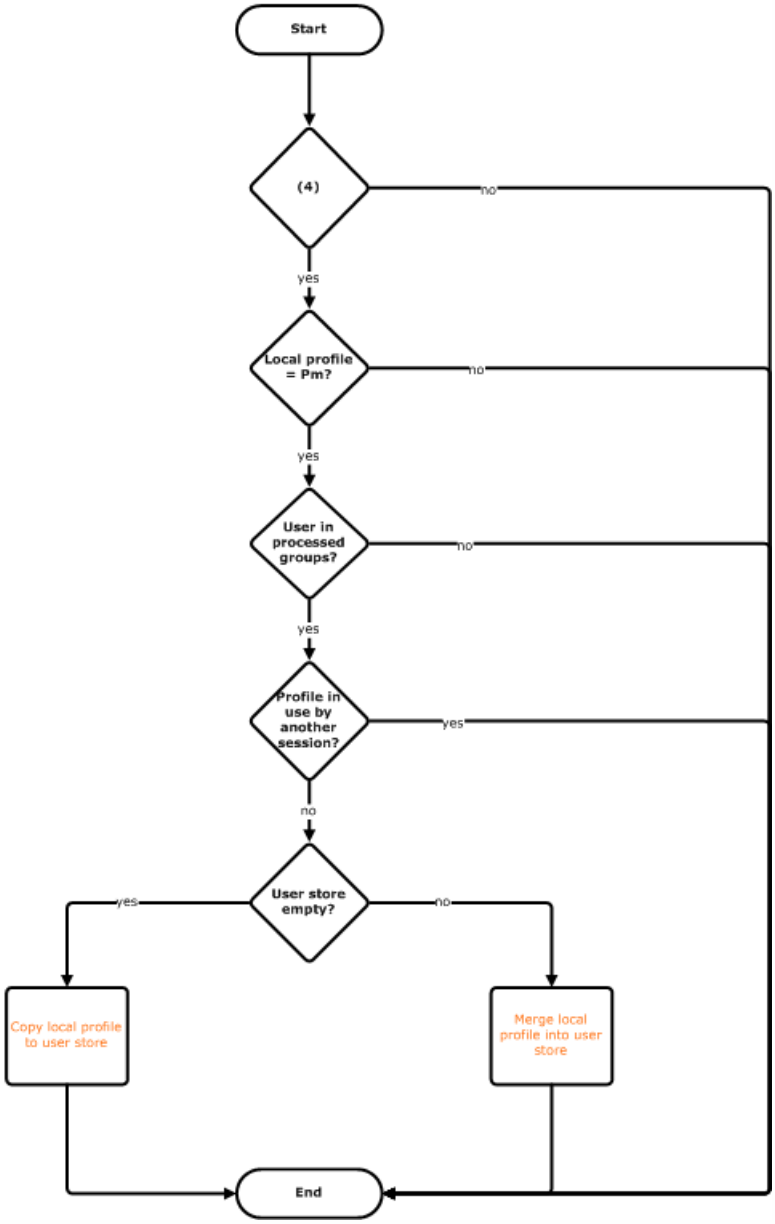
Logoff diagram

Aug 14, 2017

This diagram describes the logic used to copy or merge profile data at logoff.

CAPTION
"Pm" indicates a Citrix user profile processed by Profile management.

Group Policy Settings
(1) Conflict handling for local profiles [use|delete|rename] [default=use]
(2) Migration of existing profiles [none|local|roaming|local+roaming] [default=local+roaming]]
(3a) Template path [default=empty]
(3b) Template overwrites local profile [default=no]
(3c) Template overwrites roaming profile [default=no]
(4) Enable Profile management



Plan your deployment

Aug 14, 2017

The first stage in planning a Profile Management deployment is to decide on a set of policy settings that together form a configuration that is suitable for your environment and users. The automatic configuration feature simplifies some of this decision-making for XenDesktop deployments. As a guide to carrying out this important task on any deployment, see Decide on a configuration.

Having decided on a configuration, and reviewed and tested it, a typical deployment then consists of:

1. Creating the user store
2. Installing Profile Management
3. Enabling Profile Management

The following information is intended to assist you using the Profile Management .ini file during a pilot study or evaluation.

Important: If you intend to use the .ini file (UPMPolicyDefaults_all.ini) for evaluation purposes, rename the file (for example, to UPMPolicyDefaults_all_old.ini) before you switch to using Group Policy (GP) in a production environment. Renaming the file allows you to be certain that only production settings are applied, and that no settings you specified during your evaluation are used.
If the file is not renamed, Profile Management examines it for any settings not configured in Group Policy and adopts any non-default settings it finds. So, to eliminate the risk of unwanted settings being introduced, configure all settings you want to use in your production environment using Group Policy, not the .ini file.

The .ini file contains the same policies as the .adm and .admx files, but the policies have different names. If you are familiar with the names in GP and are planning a pilot study with the .ini file, compare the names using the tables in Profile Management policies.

For more information on .ini file deployments, see Upgrade Profile Management and Test Profile Management with a local GPO.

Decide on a configuration

Aug 14, 2017

To configure Profile management, the recommended approach is to answer these basic questions about your environment:

1. Pilot? Production?
2. Migrate profiles? New profiles?
3. Persistent? Provisioned? Dedicated? Shared?
4. Mobile? Static?
5. Which applications?

Depending on the answer to each question, you configure Profile management differently as explained in the remaining topics in this section of eDocs. You only need to configure the policies that fit the answers to these questions; you can leave other policies in their default setting. Some policies should not be configured; for a list of these, see Manage.

After you have answered each question and configured Profile management appropriately, you should anticipate:

- Review, test, and activate Profile management
- Troubleshoot

UPMConfigCheck is a PowerShell script that examines a live Profile management deployment and determines whether it is optimally configured. For more information on this tool, see CTX132805.

If your answers to the questions are the same for different sets of computers, consider grouping them into an Active Directory Organizational Unit (OU) and configuring Profile management using a single Group Policy Object (GPO) attached to that OU. If your answers to these questions are different, consider grouping the computers into separate OUs.

Alternatively, where a domain supports WMI filtering, you can group all computers into the same OU and use WMI filtering to select between appropriately configured GPOs.

Pilot? Production?

Aug 14, 2017

The aim of a pilot deployment is to be able to demonstrate a solution quickly and reliably, and an important goal may be to reduce the number of components in the pilot. For Profile management, two components are the user store and the selection of users whose profiles are processed.

Setting up a user store for Citrix user profiles is exactly like setting up a profile store for Windows roaming profiles.

For a pilot deployment, you can often ignore these considerations. The default value for the Path to user store policy is the Windows folder in the user's home directory. This works well for a single-platform pilot so long as only one operating system (and therefore only one profile version) is deployed. For information on profile versions, see About profiles. This option assumes that enough storage is available in users' home directories and that no file-server quotas are applied; Citrix does not recommend the use of file-server quotas with profiles. The reasons for this are given in Share Citrix user profiles on multiple file servers.

For a production deployment, you must carefully consider security, load balancing, high availability, and disaster recovery. Follow the recommendations in these topics for creating and configuring the user store:

- Profile management architecture
- Create the user store
- To specify the path to the user store
- High availability and disaster recovery with Profile management

The complexity of production deployments means that you may need to phase the rollout of Profile management, rather than release it to all users at the same time. You may also need to tell users that they will receive different profile experiences when connecting to different resources while the deployment is in the process of being rolled out.

For performance reasons, Profile management is licensed by an End-User License Agreement (EULA) not built-in license checking. You may choose to manage license allocation by assigning users to an Active Directory (AD) user group or using an existing AD group if a suitable one exists.

In pilot deployments, use of Profile management is usually restricted by invitation to a small group of users, possibly from several departments, where no single, representative AD group can be used. In this case, leave the Processed groups and Excluded groups policies unconfigured; Profile Management performs no checking on group membership and all users are processed.

For more information on these policies, see To define which groups' profiles are processed.

Important: In all cases you must ensure that the number of users processed by Profile management does not exceed the limits set by the relevant EULA.

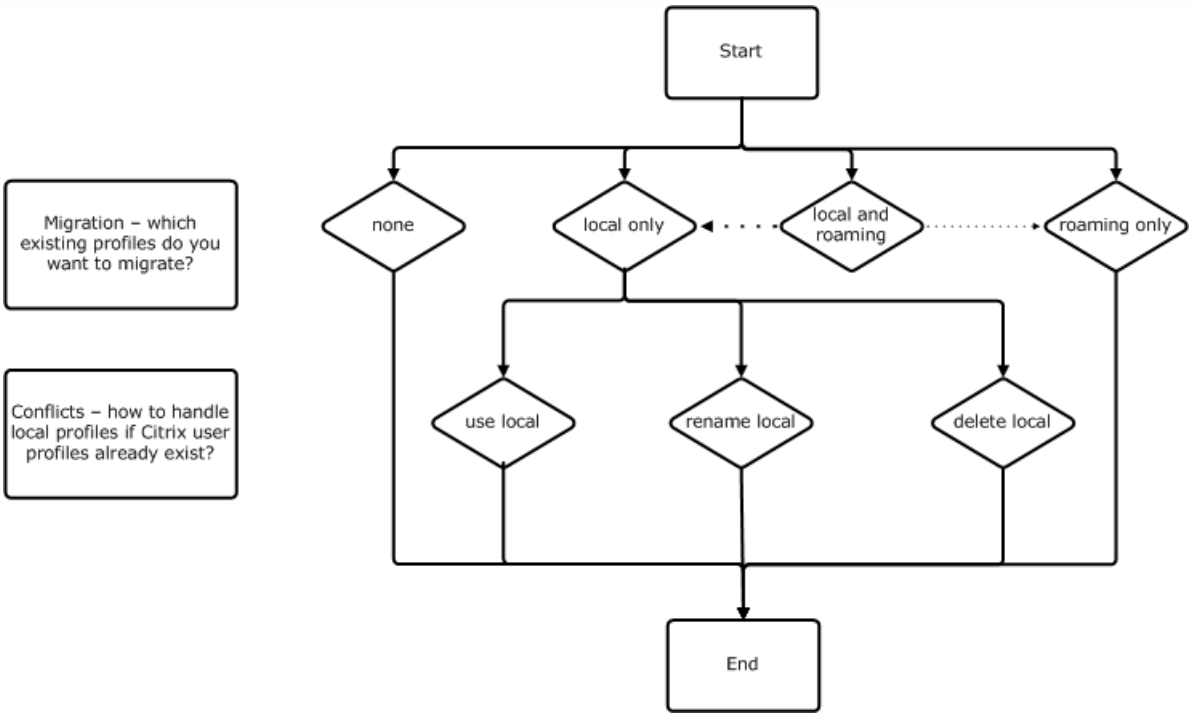
Migrate profiles? New profiles?

Aug 14, 2017

You can take advantage of a Profile management deployment to refresh your organization's profiles, initially using a small, customized profile and rigidly controlling additions to it. Alternatively, you may need to migrate existing profiles into the Profile management environment and preserve the personalizations that have built up over many years. With Citrix VDI-in-a-Box deployments, you will likely be migrating existing local profiles rather than starting from scratch.

If you decide to migrate existing profiles, configure the Migration of existing profiles and Local profile conflict handling policies.

The following diagram illustrates how to configure these policies based on your answer to this question.



If you decide to create an entirely new set of profiles, consider creating a template for this purpose using the Template profile policy. For information, see To specify a template or mandatory profile. If you do not create a template, Profile management will give users the default Windows profile, for example, from a VDI-in-a-Box master image. If no template is required, leave this policy disabled.

The **Template profile** policy is similar to the **Path to user store** policy because it specifies the location of a profile that can be used as the basis for creating a new user's profile when they first log on to a computer managed by Profile management.

You can optionally use the template as a Citrix mandatory profile for all logons. As part of your planning for this, you should perform tasks such as identifying the applications that users will access; configuring the registry states, shortcuts, and desktop settings in the profile accordingly; setting permissions on profile folders; and modifying users' logon scripts.

Note: When selecting mandatory profiles in XenDesktop deployments, Citrix recommends using Desktop Studio rather than the Profile management .adm or .admx file.

Persistent? Provisioned? Dedicated? Shared?

Aug 14, 2017

The types of machines that create profiles affect your configuration decisions. The primary factors are whether machines are persistent or provisioned, and whether they are shared by multiple users or dedicated to just one user.

Persistent systems have some type of local storage, the contents of which can be expected to persist when the system turns off. Persistent systems may employ storage technology such as storage area networks (SANs) to provide local disk mimicking. In contrast, provisioned systems are created "on the fly" from a base disk and some type of identity disk. Local storage is usually mimicked by a RAM disk or network disk, the latter often provided by a SAN with a highspeed link. The provisioning technology is generally Provisioning Services or Machine Creation Services (or a third-party equivalent). Sometimes provisioned systems have persistent local storage, which may be provided by Personal vDisks; these are classed as persistent.

Together, these two factors define the following machine types:

- **Both persistent and dedicated** - Examples are Desktop OS machines with a static assignment and a Personal vDisk that are created with Machine Creation Services (in XenDesktop), desktops with Personal vDisks that are created with VDI-in-a-Box, physical workstations, and laptops
- **Both persistent and shared** - Examples are Server OS machines that are created with Machine Creation Services (in XenDesktop), and XenApp servers
- **Both provisioned and dedicated** - Examples are Desktop OS machines with a static assignment but without a Personal vDisk that are created with Provisioning Services (in XenDesktop)
- **Both provisioned and shared** - Examples are Desktop OS machines with a random assignment that are created with Provisioning Services (in XenDesktop), desktops without Personal vDisks that are created with VDI-in-a-Box, and XenApp servers

The following Profile management policy settings are suggested guidelines for the different machine types. They work well in most cases, but you may want to deviate from these as your deployment requires.

Note: In XenDesktop deployments, Delete locally cached profiles on logoff, Profile streaming, and Always cache are enforced by the auto-configuration feature.

Policy	Both persistent and dedicated	Both persistent and shared	Both provisioned and dedicated	Both provisioned and shared
Delete locally cached profiles on logoff	Disabled	Enabled	Disabled (note 5)	Enabled
Profile streaming	Disabled	Enabled	Enabled	Enabled
Always cache	Enabled (note 1)	Disabled (note 2)	Disabled (note 6)	Disabled
Active write back	Disabled	Disabled (note 3)	Enabled	Enabled

Policy	Both persistent and dedicated	Both persistent and shared	Both provisioned and dedicated	Both provisioned and shared
Process logons of local administrators	Enabled	Disabled (note 4)	Enabled	Enabled (note 7)

1. Because Profile streaming is disabled for this machine type, the Always cache setting is always ignored.
2. Disable Always cache. However, you can ensure that large files are loaded into profiles as soon as possible after logon by enabling this policy and using it to define a file size limit (in MB). Any file this size or larger is cached locally as soon as possible.
3. Disable Active write back except to save changes in profiles of users who roam between XenApp servers. In this case, enable this policy.
4. Disable Process logons of local administrators except for Hosted Shared Desktops. In this case, enable this policy.
5. Disable Delete locally cached profiles on logoff. This retains locally cached profiles. Because the machines are assigned to individual users, logons are faster if their profiles are cached.
6. Disable Always cache. However, you can ensure that large files are loaded into profiles as soon as possible after logon by enabling this policy and using it to define a file size limit (in MB). Any file this size or larger is cached locally as soon as possible.
7. Enable Process logons of local administrators except for profiles of users who roam between XenApp servers. In this case, disable this policy.

Mobile? Static?

Aug 14, 2017

Are your machines permanently connected to the Active Directory domain? Laptops and similar mobile devices probably are not. Similarly, some deployments may have fixed machines with persistent local storage but the machines are separated from the data center for significant periods of time (for example, a remote branch office that is linked to the corporate headquarters by satellite communications). Another example is disaster recovery, where infrastructure is being restored and power or communications are intermittent.

Typically, Profile management is resilient to short network outages (less than 24 hours) so long as the user does not log off while the network is unavailable. In these circumstances, you can optimize Profile management in several ways that significantly speed up the logon process. This is the static case.

Where extended periods of disconnection are expected or users must be able to log off or shut down their computers while disconnected from the corporate network, you cannot optimize Profile management; when users reconnect, logons are slow while the entire profile is fetched from the user store. This is the mobile case.

For extended periods of disconnection (and only intermittent periods of connection to the Active Directory domain), enable the Offline profile support policy. This automatically disables the effect of the following policies, controlling optimizations that are not supported. The policies might not appear to be disabled in Group Policy but they have no effect:

- Profile streaming
- Always cache

Note: If Offline profile support is enabled, Active write back is honored but can only work when the computer is connected to the network.
Important: Do not enable Offline profile support with Citrix VDI-in-a-Box. This policy is not suitable for this product because desktops created with it do not have persistent local storage.

Policy: Offline profile support

For short periods of disconnection, disable the Offline profile support policy. This allows the configuration of any of the following policies.

Policy: Streamed user profile groups

Set the Streamed user profile groups policy to Unconfigured. Enabling this policy is effective only if Profile streaming is also enabled. Streamed user profile groups is used to limit the use of streamed profiles to specific Active Directory user groups. It is useful in some scenarios when migrating from older versions of Profile management. For instructions on setting this policy, see To stream user profiles.

For information on high availability and disaster recovery as it applies to this policy, see Scenario 4 - The traveling user.

Policy: Timeout for pending area lock files

Set the **Timeout for pending area lock files** policy to Unconfigured to apply the default operation, which is a one-day timeout for the pending area lock. This is the only supported value, so do not adjust this policy.

Policy: Active write back

For information on this policy, see Persistent? Provisioned? Dedicated? Shared?

Which applications?

Aug 14, 2017

The applications in use in your deployment affect how you configure Profile management. However, in contrast to the other configuration decisions you make, there are no simple yes-or-no recommendations because the decisions you take depend on where the applications store persistent customizations, which can either be in the registry or in the file system.

Analyze and understand your users' applications thoroughly to establish where the applications store their settings and users' customizations. Use a tool such as Procmon to monitor application binaries. Google is another resource. For information on Procmon, see http://technet.microsoft.com/en-gb/sysinternals/bb896645.

Once you understand how the applications behave, use inclusions to define which files and settings are processed by Profile management, and use exclusions to define which aren't. By default, everything in a profile is processed except for files in AppData\Local. If your deployment includes DropBox or Google Chrome, or applications created with the one-click publish in Visual Studio, you might need to explicitly include the subfolders of AppData\Local.

Simple applications are those that are well behaved; they store personalization settings in the HKCU registry hive and personalization files within the profile. Simple applications require basic synchronization and this in turn requires you to include and exclude items using:

- Relative paths (relative to %USERPROFILE%) in any of the following policies:
  - Directories to synchronize
  - Files to synchronize
  - Exclusion list - directories
  - Exclusion list - files
  - Folders to mirror

  Note: %USERPROFILE% is implied by Profile management. Do not add it explicitly to these policies.
- Registry-relative paths (that is, relative to the HKCU root) in either of these policies:
  - Exclusion list
  - Inclusion list

For instructions on including and excluding items, see To include and exclude items.

Legacy applications are badly behaved; they store their personalization files in custom folders outside the profile. The recommended solution is not to use Profile management with legacy applications but instead to use the Personal vDisk feature of XenDesktop.

Complex applications require special treatment. The application's files can cross-reference each other and must be treated as an inter-related group. Profile management supports two behaviors associated with complex applications: cookie management and folder mirroring.

Cookie management in Internet Explorer is a special case of basic synchronization in which both of the following policies are always specified:

- Process Internet cookie files on logoff
- Folders to mirror

For information on folder mirroring, more information on cookie management, and instructions on setting these policies, see To manage cookie folders and other transactional folders.

Cross-platform applications are those that may be hosted on multiple platforms. For specific versions of Internet Explorer and Microsoft Office, Profile management supports the sharing of personalization settings across platforms, whether the settings are stored in the registry or as files in the profile. Recommended policy settings for cross-platform applications are documented at Cross-platform settings - Case study.

If you want to share other applications' settings across platforms, Citrix recommends using Profile Migrator from Sepago.

Java applications can leave many small files in a profile, which can dramatically reduce profile load times. To prevent this, consider excluding AppData\Roaming\Sun\Java.

The following table summarizes the policies you use to configure Profile management for different types of applications. The following terms are used in the table:

- **Relative**. This is a relative path on a local volume, relative to %USERPROFILE% (which must not be specified). Examples: AppData\Local\Microsoft\Office\Access.qat, AppData\Roaming\Adobe\.
- **Absolute**. This is an absolute path on a local volume. Examples: C:\BadApp*.txt, C:\BadApp\Database\info.db.
- **Registry Relative**. This refers to a path within the HKCU hive. Examples: Software\Policies, Software\Adobe.
- **Flag**. Flags are used to enable or disable processing where no path information is required. Examples: Enabled, Disabled.

Policy	Policy Type (Registry, Folder, or File)	Wildcard Support?	Application Type		
			Simple	Legacy	Complex
Directories to synchronize	Folder		Relative	Absolute	
Files to synchronize	File	Yes	Relative	Absolute	
Exclusion list - directories	Folder		Relative	Absolute	
Exclusion list - files	File	Yes	Relative	Absolute	
Inclusion list	Registry		Registry relative		
Exclusion list	Registry		Registry relative		

Policy	Policy Type (Registry, Folder, or File)	Wildcard Support?	Application Type		
			Simple	Legacy	Absolute Relative Flag Complex
Folders to Mirror Process Internet cookie files on logoff	Folder				

Policies that refer to files (rather than folders or registry entries) support wildcards. For more information, see Using wildcards.

Profile management uses rules to include and exclude files, folders, and registry keys from user profiles in the user store. These rules result in sensible and intuitive behavior; all items are included by default. From that starting point, you can configure top-level exceptions as exclusions, then configure deeper exceptions to the top-level exceptions as inclusions, and so on. For more information on the rules, including instructions on including and excluding items, see To include and exclude items.

For non-English systems that use Version 1 profiles, specify relative paths in inclusion and exclusion lists in the local language (for example, on a German system use Dokumenten not Documents). If you support multiple locales, add each included or excluded item in each language.

Important: This topic describes the last of the questions that you must answer in order to configure your Profile management deployment. (The questions are listed in Decide on a configuration.) Once you have answered all of the questions and have configured the settings accordingly, you are ready to review the configuration and go live as described in Review, test, and activate Profile management. You can leave all other policies in their default setting. This includes some policies that you should not configure; for a list of these, see Policies not requiring configuration.

Review, test, and activate Profile Management

Aug 14, 2017

This topic assumes that you have answered all of the questions about your deployment listed in Decide on a configuration, and have configured Profile management policies accordingly. You are now ready to review the configuration and go live.

Ask a colleague to review your policy settings. Then, test the configuration. This can be done using the .ini file. Once testing is complete, manually transfer the settings to a Group Policy Object.

Until you enable this policy, Profile management is inactive.

Plan for multiple platforms

Aug 14, 2017

It is common for users to access multiple computing devices. The challenge with any type of roaming profile results from the differences between systems on these devices. For example, if I create a shortcut on my desktop to a local file that does not exist when I move to a different device, I have a broken shortcut on my desktop.

A similar issue exists when roaming between a desktop operating system (OS) and a server OS. Some settings may not be applicable on the server (such as power settings or video settings). Furthermore, if applications are not installed similarly on each device, when I roam other issues may emerge.

Some personalization settings (such as My Documents, Favorites, and other files that function independently of OS or application version) are much easier to manage than others. But even these settings may be difficult to roam when a document type is only supported on one system. For example, a user has Microsoft Project installed on one system, but on another device that file type is not recognized. This situation is exacerbated if the same application is present on two systems but on one different add-ons are installed and expected by a document.

Even though platforms are identically installed, if an application is configured differently on each, errors may occur when the application starts. For example, a macro or add-on might activate in Excel on one platform but not another.

The Start menu contains links (LNK and LNK2 files). The user-specific part of the menu is stored in the profile and can often be modified by users. Adding custom links (to executables or documents) is not uncommon. In addition, links that are language-specific result in multiple Start menu entries for the same application. Furthermore, links pointing to documents might be invalid on other computers because the path to the document is relative to another system, or it is a network path that is inaccessible.

By default, the content of the Start menu folder is not saved by Profile management because links pointing to executables are often computer-dependent. However, in situations where the systems are very similar, including the Start menu in your Profile management configuration improves the consistency when users roam from desktop to desktop. Alternatively, you can process the Start menu with folder redirection.

Note: Unpredictable side effects can often result from what appears to be the most innocuous of changes. For example, see the article
— Citrix User Profile Manager (UPM) and the Broken Rootdrive
on the Sepago blog.
Always test and verify the behavior of the Start menu across platforms.

The Quick Launch toolbar contains links and is configurable by users. By default, the Quick Launch toolbar is saved by Profile management. In some environments this might not be desirable because the links may be computer-dependent.

To exclude the toolbar from profiles, add the following entry to the folder exclusion list:
AppData\Roaming\Microsoft\Internet Explorer\Quick Launch.

Important: Because of the difference in their structure, Citrix recommends creating separate Version 1 and Version 2 profiles for each user in any environment that contains multiple platforms. Differences between the Windows Vista and Windows 7 profile namespace make it difficult to share profiles across these platforms, and failures can also occur between Windows XP and Windows Server 2003. For more information on Version 1 and Version 2 profiles, see About profiles.

The definition of multiple platforms here includes not just multiple operating systems (including ones of different bitness) but also multiple application versions running on the same operating system. The following examples illustrate the reasons for this recommendation:

- 32-bit systems may contain registry keys that instruct the operating system to start applications in locations specific to 32-bit operating systems. If the keys are used by a Citrix user profile on a 64-bit system, the location might not exist on that system and the application will fail to start.
- Microsoft Office 2003, Office 2007, and Office 2010 store some Word settings in different registry keys; even if these applications run on the same operating system, you should create separate profiles for the three different versions of the Word application.

Citrix recommends using Microsoft folder redirection with Citrix user profiles to help ensure profile interoperability, but within an environment where Windows Vista or Windows 7 must co-exist with Windows XP, it is even more important.

Tip: Depending on your organization's data management policy, it is good practice to delete profiles from the user store and the cross-platform settings store for user accounts that have been removed from Active Directory.

Share Citrix user profiles on multiple file servers

Aug 14, 2017

The simplest implementation of Profile management is one in which the user store is on one file server that covers all users in one geographical location. This topic describes a more distributed environment involving multiple file servers. For information on highly distributed environments, see High availability and disaster recovery with Profile management.

Note: Disable server-side file quotas for the user store because filling the quota causes data loss and requires the profile to be reset. It is better to limit the amount of personal data held in profiles (for example, Documents, Music and Pictures) by using folder redirection to a separate volume that does have server-side file quotas enabled.

The user store can be located across multiple file servers, which has benefits in large deployments where many profiles must be shared across the network. Profile management defines the user store with a single setting, **Path to user store**, so you define multiple file servers by adding attributes to this setting. You can use any LDAP attributes that are defined in the user schema in Active Directory. For information on this, see http://msdn.microsoft.com/en-us/library/ms675090(VS.85).aspx.

Suppose your users are in schools located in different cities and the #l# attribute (lower case L, for location) is configured to represent this. You have locations in London, Paris, and Madrid. You configure the path to the user store as:

\\#l#.userstore.myschools.net\profile\#sAMAccountName#\%ProfileVer%\

For Paris, this is expanded to:

\\Paris.userstore.myschools.net\profile\JohnSmith\v1\

You then divide up your cities across the available servers, for example setting up Paris.userstore.myschools.net in your DNS to point to Server1.

Before using any attribute in this way, check all of its values. They must only contain characters that can be used as part of a server name. For example, values for #l# might contain spaces or be too long.

If you can't use the #l# attribute, examine your AD user schema for other attributes such as #company# or #department# that achieve a similar partitioning.

You can also create custom attributes. Use Active Directory Explorer, which is a sysinternals tool, to find which attributes have been defined for any particular domain. Active Directory Explorer is available at http://technet.microsoft.com/en-us/sysinternals/bb963907.aspx.

Note: Do not use user environment variables such as %homeshare% to distinguish profiles or servers. Profile management recognizes system environment variables but not user environment variables. You can, however, use the related Active Directory property, #homeDirectory#. So, if you want to store profiles on the same share as the users' HOME directories, set the path to the user store as #homeDirectory#\profiles .

The use of variables in the path to the user store is described in the following topics:

- To specify the path to the user store
- Administer profiles within and across OUs
- High availability and disaster recovery with Profile management

Administer profiles within and across OUs

Aug 14, 2017

You can control how Profile management administers profiles within an Organizational Unit (OU). In Windows Server 2008 environments, use Windows Management Instrumentation (WMI) filtering to restrict the .adm or .admx file to a subset of computers in the OU. WMI filtering is a capability of Group Policy Management Console with Service Pack 1 (GPMC with SP1). For more information on WMI filtering, see http://technet.microsoft.com/en-us/library/cc779036(WS.10).aspx and http://technet.microsoft.com/en-us/library/cc758471(WS.10).aspx. For more information on GPMC with SP1, see http://www.microsoft.com/DOWNLOADS/details.aspx?FamilyID=0a6d4c24-8cbd-4b35-9272-dd3cbfc81887&displaylang=en.

The following methods let you manage computers with different OSs using a single Group Policy Object (GPO) in a single OU. Each method is a different approach to defining the path to the user store:

- Hard-coded strings
- Profile management variables
- System environment variables

Hard-coded strings specify a location that contains computers of just one type. This allows profiles from those computers to be uniquely identified by Profile management. For example, if you have an OU containing only Windows 7 computers, you might specify \server\profiles$\%USERNAME%.%USERDOMAIN%\Windows7 in Path to user store. In this example, the Windows7 folder is hard-coded. Hard-coded strings do not require any setup on the computers that run the Profile Management Service.

Profile management variables are the preferred method because they can be combined flexibly to uniquely identify computers and do not require any setup. For example, if you have an OU containing Windows 7 and Windows 8 profiles running on operating systems of different bitness, you might specify \\server\profiles$\%USERNAME%.%USERDOMAIN%\!CTX_OSNAME!!CTX_OSBITNESS! in Path to user store. In this example, the two Profile management variables might resolve to the folders Win7x86 (containing the profiles running on the Windows 7 32-bit operating system) and Win8x64 (containing the profiles running on the Windows 8 64-bit operating system). For more information on Profile management variables, see Profile Management Policies.

System environment variables require some configuration; they must be set up on each computer that runs the Profile Management Service. Where Profile management variables are not suitable, consider incorporating system environment variables into the path to the user store as follows.

On each computer, set up a system environment variable called %ProfVer%. (User environment variables are not supported.) Then, set the path to the user store as:

\\upmserver\upmshare\%username%.%userdomain%\%ProfVer%

For example, set the value for %ProfVer% to Win7 for your Windows 7 32-bit computers and Win7x64 for your Windows 7 64-bit computers. For Windows Server 2008 32-bit and 64-bit computers, use 2k8 and 2k8x64 respectively. Setting these values manually on many computers is time-consuming, but if you use Provisioning Services, you only have to add the variable to your base image.

An example of how to script this is at:

http://forums.citrix.com/thread.jspa?threadID=241243&tstart=0

This sample script includes lines for Windows Server 2000, which is unsupported by Profile management.

Tip: In Windows Server 2008 R2 and Windows Server 2012, you can speed up the creation and application of environment variables using Group Policy; in Group Policy Management Editor, click Computer Configuration > Preferences > Windows Settings > Environment, and then Action > New > Environment Variable.

You can control how Profile management administers profiles across OUs. Depending on your OU hierarchy and GPO inheritance, you can separate into one GPO a common set of Profile management policies that apply to multiple OUs. For example, Path to user store and Enable Profile management must be applied to all OUs, so you might store these separately in a dedicated GPO, enabling only these policies there (and leaving them unconfigured in all other GPOs).

You can also use a dedicated GPO to override inherited policies. For information on GPO inheritance, see the Microsoft Web site.

Domain and forest support in Profile Management

Aug 14, 2017

Domain and forest functional levels of Windows Server 2008 and Windows Server 2012 are supported by Profile management. Older operating systems are unsupported.

The use of system environment variables can help to disambiguate user names in multiple domains. For information on this, see Administer profiles within and across OUs.

High availability and disaster recovery with Profile Management

Aug 14, 2017

As a prerequisite, familiarize yourself with the structure of the user store and how to create it by reading Profile management architecture and Create the user store.

These topics describe the supported scenarios for high availability and disaster recovery as they apply to Citrix Profile management. It relates the scenarios to the relevant, underlying Microsoft technologies and identifies what is supported:

- Scenario 1: Basic setup of geographically adjacent user stores and failover clusters
- Scenario 2: Multiple folder targets and replication
- Scenario 3: Disaster recovery
- Scenario 4: The traveling user
- Scenario 5: Load-balancing user stores

Profile management assumes that it operates in an environment that is reliable. Principally, this reliability applies to the availability of Active Directory (AD) and a networked user store (NUS). When either of these is not available, Profile management cannot provide a profile, and hands over responsibility to Windows, which generally provides a default profile.

In disaster recovery and high availability scenarios, Citrix Profile management may be affected by the same issues as affect Microsoft roaming profiles, and unless stated to the contrary, Profile management does not resolve such issues.

In particular, note the following:

- Profile management support is limited to the scenarios where roaming profiles are also supported. For more information about this, see "Can I use DFS with Offline Files and redirected My Documents folders?" at http://technet.microsoft.com/en-us/library/hh341474(WS.10).aspx.
- The cache option for offline files must be disabled on roaming user profile shares. The same restriction applies to Profile management shares. For more information about this, see http://support.microsoft.com/kb/287566.
- A roaming profile is not loaded from a DFS share. The same restriction applies to Profile management shares. For more information about this, see http://support.microsoft.com/kb/830856.

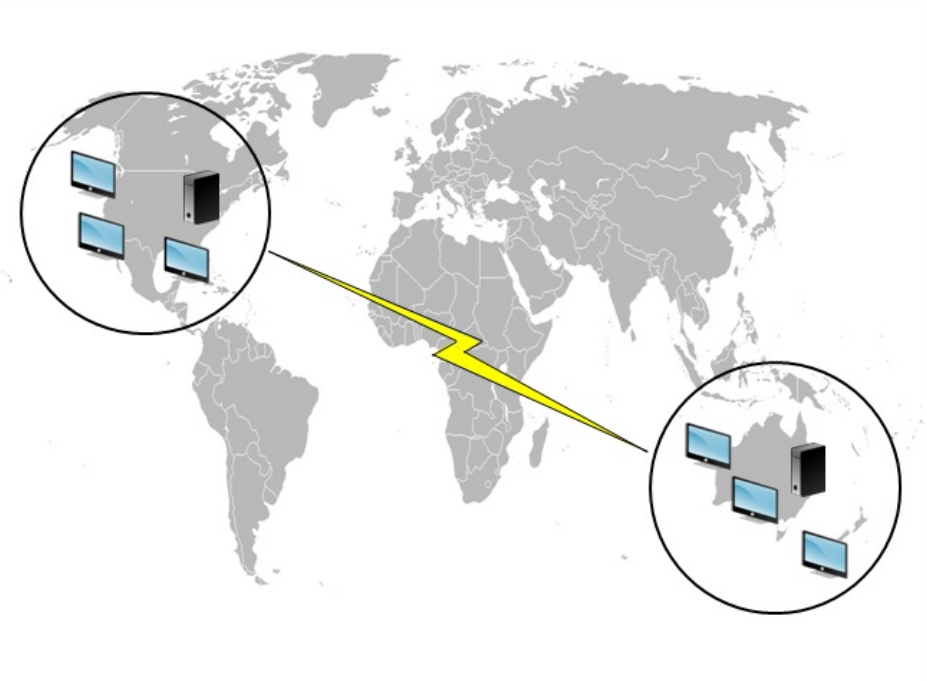
Scenario 1 - Basic setup of geographically adjacent user stores and failover clusters

Aug 14, 2017

“I want my users to always use a geographically adjacent, preferred networked user store (NUS) for their profiles.” Options 1 and 2 apply in this case.

“I want my NUS to be on a failover cluster, to give me high availability.” Option 2 applies in this case.

The following graphic illustrates this scenario. Users in North America (NA) want to use the NUS in New York rather than the NUS in Brisbane, to reduce latency and to minimize the traffic sent over the intercontinental link to Australia or New Zealand (ANZ).



Background reading

- For an overview of the Microsoft DFS Namespaces technology, see http://technet.microsoft.com/en-us/library/cc730736(WS.10).aspx.
- For advice on load balancing user stores, see the Citrix blog at http://community.citrix.com/display/ocb/2009/07/21/Profile+Management+-+Load+Balancing+User+Stores.

Implementing this option

DFS Namespaces can resolve some of the issues presented in the blog article.

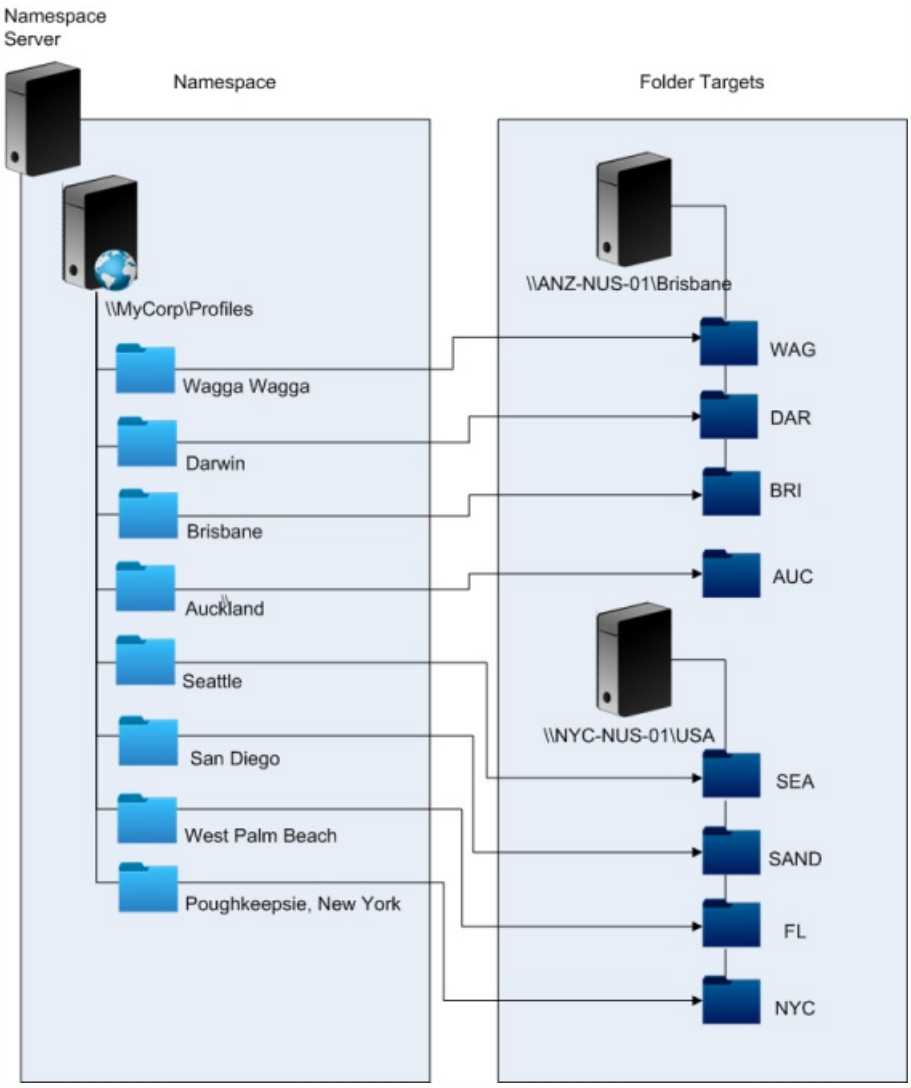
Let us set up a namespace for the NUS called \\MyCorp\Profiles; this is the namespace root. We set up namespace servers in New York and Brisbane (and any of the other sites). Each namespace server has folders corresponding to each Active

Directory location, which in turn have targets on a server in New York or Brisbane.

We might have the following locations configured in Active Directory (part of the user records).

AD Location Attribute (#l#)	Geographic Location
Wagga Wagga	ANZ
Darwin	ANZ
Brisbane	ANZ
Auckland	ANZ
Seattle	NA
San Diego	NA
West Palm Beach	NA
Poughkeepsie, New York	NA

The following graphic shows one way of setting this up using DFS Namespaces.



Once this is set up, we configure the Path to user store setting as:

\\MyCorp\Profiles\#l#

The profiles of users belonging to the eight sites will be distributed to just two servers, meeting the geographical constraints required of the scenario.

Alternatives

You can order namespace targets and use the ordering rules as follows. When DFS Namespaces resolves which target to use, it is possible to specify that only targets in the local site are chosen. This works well so long as you are sure that, for any given user, every desktop and server is guaranteed to belong to the same site.

This technique fails if, say, a user normally based at Poughkeepsie visits Wagga Wagga. Their laptop profile may come from Brisbane, but the profile used by their published applications may come from New York.

The recommended technique, using AD attributes, ensures that the same DFS Namespace choices are made for every session that the user initiates, because the #l# derives from the user's AD configuration rather than from machine configurations.

Background reading

- For a step-by-step guide to configuring a two-node file server failover cluster, see http://technet.microsoft.com/en-us/library/cc731844(WS.10).aspx.
- For information about choosing a namespace type, see http://technet.microsoft.com/en-us/library/cc770287(WS.10).aspx.

Implementing this option

Adding failover clustering allows you to provide basic high availability.

The key point in this option is to turn the file servers into failover clusters, so that folder targets are hosted on a failover cluster rather than a single server.

If you require the namespace server itself to have high availability, you must choose a standalone namespace, as domain-based namespaces do not support the use of failover clusters as namespace servers. Folder targets may be hosted on failover clusters, regardless of the type of namespace server.

Important: The state of file locks may not be preserved if a server in a failover cluster fails. Profile management takes out file locks on the NUS at certain points during profile processing, so it is possible that a failover at a critical point may result in profile corruption.

Scenario 2 - Multiple folder targets and replication

Aug 14, 2017

"If my local NUS is not available, I want my users to be able to get their profile data from a backup location somewhere else on the corporate network. If they make changes, those changes need to get back to their preferred NUS when it is available again."

The basic requirement in this scenario is to provide alternative locations for profiles on the network. The use case includes the partial failure of the network infrastructure or the complete unavailability of a folder target such as a failover cluster.

Options you should consider are the use of multiple folder targets and the use of DFS replication.

Background reading

For information about tuning DFS namespaces, see http://technet.microsoft.com/en-us/library/cc771083(WS.10).aspx.

About this option

A referral is an ordered list of targets that are tried in turn by a user device. It is designed for scenarios where the targets are read-only, such as software libraries. There is no linkage between targets, so using this technique with profiles may create multiple profiles that cannot be synchronized.

However, it is possible to define both an ordering method and a target priority for targets in referrals. Choosing a suitable ordering method appears to result in a consistent choice of target by all user sessions. But in practice, even when all of a user's devices are within the same site, intra-site routing problems can still result in different targets being chosen by different sessions. This problem can be compounded when devices cache referrals.

Important: This option is not suitable for Profile management deployments and is generally not supported. However, file replication has been used in some specialized deployments in which only a single session can be guaranteed and Active write back is disabled. For information on these special cases, contact Citrix Consulting.

Background reading

- For an overview of Distributed File System Replication (DFSR), see http://technet.microsoft.com/en-us/library/cc771058(WS.10).aspx.
- For a statement of support about replicated user profile data, see http://blogs.technet.com/b/askds/archive/2010/09/01/microsoft-s-support-statement-around-replicated-user-profile-data.aspx.
- To understand why DFSR does not support distributed file locking, see http://blogs.technet.com/b/askds/archive/2009/02/20/understanding-the-lack-of-distributed-file-locking-in-dfsr.aspx.

Implementing this option

DFS Replication provides folder synchronization across limited bandwidth network connections. This appears to solve the problems in Option 1 because it synchronizes multiple folder targets that a single namespace folder definition refers to. Indeed, when folders are added as targets to a folder definition, they can be specified as belonging to a replication group.

There are two forms of replication to consider:

- One-way replication (also known as active-passive replication) is designed for backing up critical data to a safe repository. This makes it suitable for maintaining a disaster recovery site, for example. This can be made to work with Profile management so long as the passive targets are disabled for referrals, and are only invoked when the disaster recovery plan is activated.
- Two-way replication (also known as active-active replication) is intended to provide local read-write access to global shared data. Instantaneous replication is not necessarily a requirement here. The shared data may be modified infrequently.
  Important: Active-active DFSR is not supported.

A schedule defines the frequency with which data is replicated. A frequent schedule is more intensive on both CPU and bandwidth, but will not guarantee instantaneous updates.

At various points in its operation, Profile management requires certain files to be locked in the NUS to coordinate updates to the (shared) user store. Typically these updates take place when a session starts and ends, and in the middle of a session if active write-back is enabled. Since distributed file locking is not supported by DFS Replication, Profile management can only select one target as an NUS. This effectively eliminates any value of two-way replication (active-active replication), which is therefore not suitable for Profile management and is not supported. One-way replication (active-passive replication) is suitable for Profile management only as part of a disaster recovery system. Other uses are not supported.

Scenario 3 - Disaster recovery

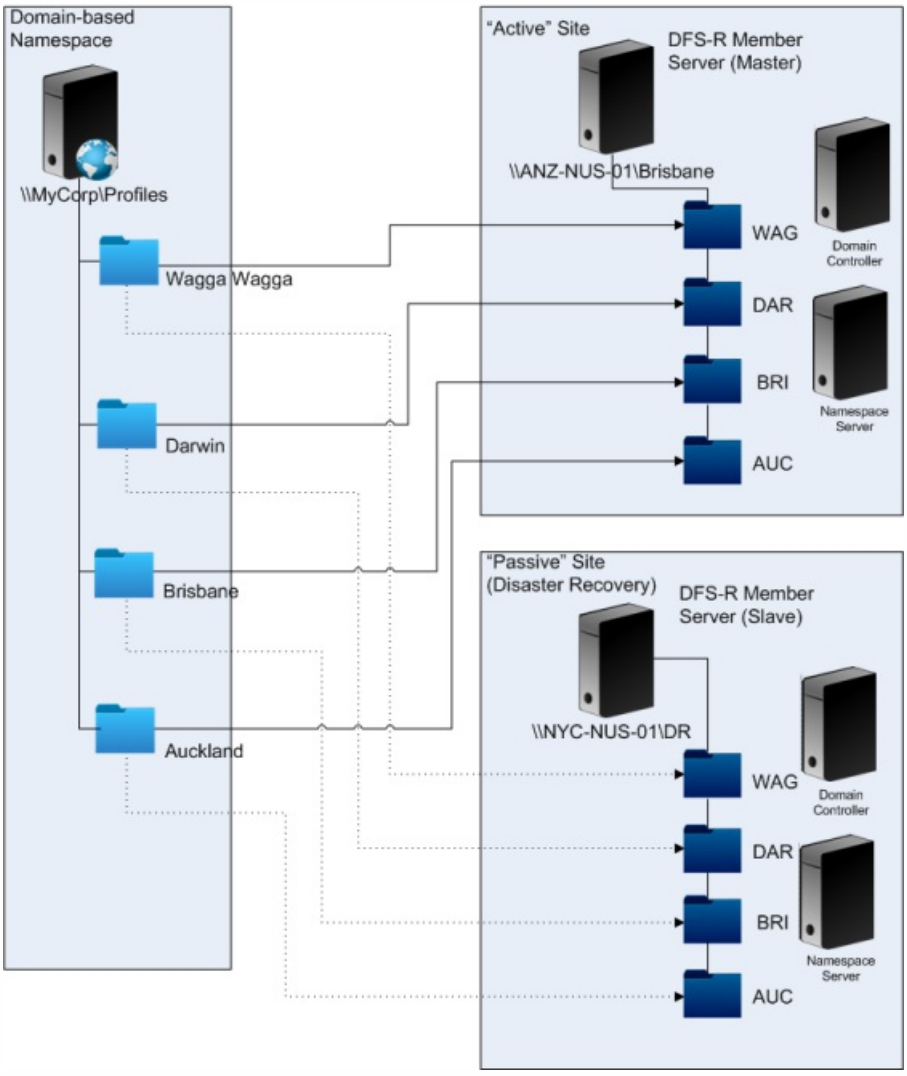
Aug 14, 2017

"How do I set up a full disaster recovery site to handle Citrix user profiles?"

The key features required for disaster recovery (DR) are supported by Profile management:

- **DFS namespaces**. Domain-based namespace servers are preferred in this scenario because they allow the DR site to have its own namespace server. (A standalone namespace server cannot be replicated, but it can be hosted on a failover cluster.)
- **Multiple folder targets and DFS Replication**. For each NUS, you provide at least two targets, but only enable one in normal operation. You set up one-way DFS Replication to ensure that the disabled targets (at the DR sites) are kept up-to-date.
- **Failover clusters for hosting individual folder targets**. This is optional. It might be wasteful of resources on the DR site.

In this diagram, a domain-based namespace manages the NUS. (The diagram in Scenario 1 deliberately did not include namespaces.) This means that we can include a namespace server in each site, including the DR site, and the servers all support the same view of the namespace.



If the DR plan is activated, the DR site's NUS is up-to-date with the changes replicated from the master NUS. However, the namespace server still reflects the wrong view of the namespace, so its configuration must be updated. For each folder, the folder target on the master site must be disabled and the folder target on the DR site enabled.

After AD updates have propagated, the namespace server correctly locates the DR folder targets and the DR site is ready to use by Profile management.

Note: The Path to user store setting refers to namespace folders, not real servers, so there is no need to update the Profile management configuration.
In practice, one-way or two-way replication is possible because the DR site is not normally used for profiles. Once the disaster is over, a connection from the DR site to the master site ensures that changes made to the NUS during the disaster are replicated on the master site.

Scenario 4 - The traveling user

Aug 14, 2017

“When my staff roam between different offices, I want their preferred NUS to change, so that they’re still using a geographically adjacent NUS.”

The difficulty with this scenario is that a user's logon session may be aggregated from multiple locations. They typically roam their desktop session from one site to another, but many of their applications are hosted on backend servers that have no awareness of the current location of the user's desktop.

Furthermore, the user may reconnect to disconnected sessions, probably hosted at their home location, so if the sessions were for some reason forced to switch to an NUS in the user's new location, their performance degrades.

For travelers who hot-desk, using the Profile streaming and Always cache settings is the best option. With a fixed machine, they still log on quickly, using Citrix streamed user profiles. Enabling Always cache loads the remainder of the profile in the background.

Scenario 5 - Load-balancing user stores

Aug 14, 2017

"I want to load-balance my users across several geographically adjacent networked user stores (NUSs)."

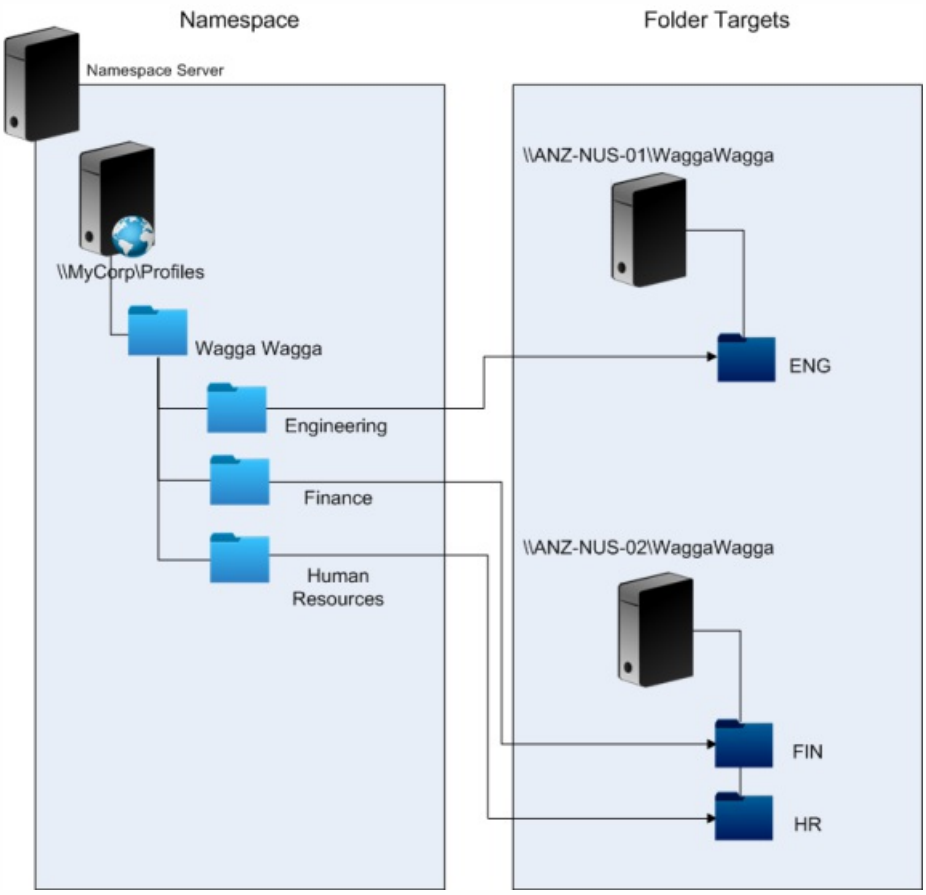
- For an overview of the Microsoft DFS Namespaces technology, http://technet.microsoft.com/en-us/library/cc730736(WS.10).aspx.
- For advice on load balancing user stores, see the Citrix blog at http://blogs.citrix.com/2009/07/21/profile-management-load-balancing-user-stores/.

Unlike Scenario 1, this scenario has a single site that is large enough to require multiple NUSs. Using DFS namespaces, we can improve on the solution in Scenario 1.

Scenario 1 (Option 1) used DFS Namespaces to map multiple sites to different folders on the same server. You can use a similar technique to map subfolders of a namespace to folders on different servers.

Ideally, you need an AD attribute that partitions user accounts into similarly sized chunks, such as #department#. As in Scenario 1, #department# must always be defined and must be guaranteed to contain a correct folder name.

As in Scenario 1, we set up a namespace for the NUS called \\MyCorp\Profiles.
This diagram shows how to set up the namespace.



Once this is set up, you configure the Path to user store setting as:

\\MyCorp\Profiles\#l#\#department#

With this configuration, the users in Wagga Wagga are distributed across two NUS servers, both local.

Plan folder redirection with Profile Management

Aug 14, 2017

Profile management works with folder redirection and its use is encouraged.

Active Directory (AD) allows folders, such as Application Data or Documents, to be saved (redirected) to a network location. The contents of the folders are stored in the redirected location and not included within the user profile, which therefore reduces in size. Depending on the version of AD, some folders can be redirected but not others. In addition, configuring folder redirection allows users with mandatory profiles to save some settings, files, and other data while still restricting profile usage.

As a general guideline, Citrix recommends enabling folder redirection for all user data that is not accessed regularly within a session if network bandwidth permits.

Not all folders which can be redirected are accessible with AD. The folders that can be redirected on a specific operating system are in the registry under HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders.

Note the following important points about using folder redirection with Profile management:

- In XenDesktop 7, you specify the folders to redirect in Studio using XenDesktop policies. For information on this, see the XenDesktop documentation.
- To configure folder direction successfully, be aware of the differences in folder structure between Version 1 and Version 2 profiles.
- For additional security considerations when using folder redirection, see Secure and the article Folder Redirection Overview on the Microsoft TechNet Web site.
- Treat the user store differently to the share used for redirected folders.
- Do not add redirected folders to exclusion lists.

Third-party directory, authentication, and file services

Aug 14, 2017

This topic describes support for directory, authentication, and file services other than those provided by Microsoft.

Important: Active Directory (AD) is critical to the operation of Profile management. Other directory services are not supported. These include:

- Novell eDirectory.
- Windows 2000 server or earlier operating systems (OSs). Windows 2000 server supports AD but not at the required level; for more information, see Domain and forest support in Profile management. Microsoft Windows NT 4.0 pre-dates AD.
- Samba 4 or earlier.

Other authentication services can co-exist with AD within a domain but are not supported by Profile management because, like the Profile Management Service, they can interact with winlogon.exe and cause problems with the user logon process. For example, the authentication service from Novell allows users to access Novell resources, such as printers and file shares, but is not supported.

Third-party file services can be used for the user store and folder redirection (if supported by the Windows operating system being used). File servers must be of the type Server Message Block (SMB) or Common Internet File System (CIFS) and must support the NTFS file system. For these reasons, the following are supported:

- Windows Server 2003 or later
- Samba 3

Important: Because it requires authentication against the Novell directory, the Novell file service is not supported.

Frequently asked questions about profiles on multiple platforms and Profile Management migration

Aug 14, 2017

This section contains questions and answers about using profiles in environments with multiple Windows operating systems, or multiple versions or bitnesses of a single operating system.

For answers to frequently asked questions about upgrades, see Frequently asked questions about upgrading Profile management.

This requires balancing the need to support heterogeneous environments with the need for personalization settings to track users and their devices. Typically, the balance between these two needs can only be determined by administrators and IT departments. This means managing the different systems by adjusting the user profiles as follows. When profiles roam, any issues should be handled properly or, if really necessary, settings should be completely ignored and not tracked at all. This is the basis of many third-party software solutions.

To minimize troubleshooting, try and roam profiles across exactly the same device setup (installed applications, OS version, and so on). In many scenarios in the modern world however, that is not easily achieved, which makes for an imperfect user experience. For example, a user should not need to replicate their Favorites or My Documents just because they use multiple operating systems. Administrators can enhance the user experience in this case by using Folder Redirection. The use of this Microsoft feature is also encouraged in other scenarios.

Citrix recommends having one base profile for each platform. This is not necessarily the same as one profile per operating system. For more information on this recommendation, see Plan for multiple platforms This minimizes the number of settings that may not work well together or that do not apply to any given OS. For example, desktop power settings are not applicable in a server scenario or one involving Remote Desktop Services (formerly Terminal Services).

As you try to simplify and reduce the number of profiles and they are used on more than one OS, there is greater risk of conflicting settings. This is further compounded when the systems are not the same. For example, Microsoft Office add-ins may not exist on every device. Fortunately, settings such as this one that are not applicable on a given device are often ignored. Support issues arise when they are not ignored. Microsoft Excel fails to start if an add-in is not present.

Citrix provides the ability to roam common settings across multiple base profiles. Citrix enables roaming of settings such as Microsoft Office, Internet Explorer, and wallpaper. The ability to support these types of scenarios is limited by the degree to which applications support the roaming of settings between platforms. The links in the next question cover Microsoft's position and best practices.

For best practices for roaming profiles, see http://technet.microsoft.com/en-us/library/cc784484.aspx.

For recommended strategies to roam Outlook, see http://office.microsoft.com/en-us/ork2003/HA011402691033.aspx.

For Office installation recommendations, see http://office.microsoft.com/en-us/ork2003/HA011402061033.aspx.

For Office 2007 toolbar settings, see http://support.microsoft.com/kb/926805/en-us.

Where the standard Microsoft Windows profile solutions do not fully address technical, custom, or business requirements, Profile management represents a viable solution.

Sharing one profile between Windows x86 and x64 might generally work, but some issues are possible.

There are several reasons for this. For example, one reason is that per-use file associations are stored in HKCU\Software\Classes. If a non-administrator sets Firefox as their default browser, the following is stored on a 32-bit system:

HKEY_CURRENT_USER\Software\Classes\FirefoxHTML\shell\open\command -> "C:\Program Files\Mozilla Firefox\firefox.exe" -requestPending -osint -url "%1"

If a profile containing this path is used on Windows x64, the OS looks for a 64-bit version of Firefox, but this does not exist. Instead, a 32-bit version is probably installed at C:\Program Files (x86)\Mozilla Firefox. This results in the browser not starting.

The reverse is also true; a path is set on an x64 platform but is used on an x86 one.

Testing and validating are key to experimenting with the use of one profile on more than one platform. The recommended approach is to have one profile per platform, but if you want to explore how a single profile behaves across multiple platforms, the following information may be helpful.

Start by identifying what might cause issues by answering the next question, and use the remaining questions in this topic for ideas for tackling and tracking the issues.

Items that will work across platforms:

- My Documents and Favorites
- Applications that store their configuration information (with defaults) completely within the profile

Items that might not work:

- Applications that store hard-coded data, path data, and so on
- Settings specific to x64 or x86 platforms
- Installations of applications that are not identical, such as Excel Add-ins that are not present on all systems. These might cause all types of error conditions that vary by application

Yes. Profile management can apply a profile based on the local desktop, XenApp, or XenDesktop, or any combination of these.

With the correct Profile management setting enabled, a Remote Desktop Services (formerly Terminal Services) profile is used only when a user has a Terminal Server or XenApp session. This setting overrides any existing profile (except for a Citrix user profile) when the user logs on through a Remote Desktop Services session.

On Windows 7, you can use a GPO computer setting to assign a profile based on the computer a user logs on to. Again, because this is based on GP, the profile assignment depends on the OU to which the GPO is applied.

It is very useful to assign a profile to the computer a user logs on to if a distinct user experience is desired. For example, administrators may decide that profiles used with Remote Desktop Services (formerly Terminal Server) sessions are kept separate from profiles used with desktops.

You can configure Profile management to automatically migrate existing roaming and local profiles when users log on. You can also use a template profile or the default Windows profile as the basis for new Citrix user profiles.

For information about planning and setting up your Profile management migration, see Migrate profiles? New profiles?. For details of how the software migrates Windows user profiles to Citrix user profiles, see Logon diagram.

Profile management can migrate Windows local profiles and Windows roaming profiles. Mandatory profiles (.man files) are ignored by Profile management but they can be used as templates for Citrix user profiles. To ensure Profile management works correctly, deactivate the assignment of mandatory profiles to all users.

To use your existing Windows mandatory profile as a template, see To specify a template or mandatory profile.

Profile management allows you to specify a template profile that is used as the basis for the creation of new Citrix user profiles. Typically, a user who is assigned a profile for the first time receives the default user profile of the Windows device they log on to. This may be acceptable, but it means any variation in different devices' default user profiles results in differences in the base profile created for the user. Therefore, you can regard the template profile feature as a global default user profile.

If you want to prevent users making any changes to their profile data, you can also identify a template profile as a Citrix mandatory profile.

For more information, see To specify a template or mandatory profile.

Install and set up

Aug 14, 2017

Deploying Profile Management consists of installing an .msi file and either an .adm or .admx file. For information on upgrades rather than installations, see Upgrade and migrate.

Install the Profile Management .msi file on each computer whose user profiles you want to manage. Typically, you install the .msi file on computers using a distribution tool, an imaging solution, or streaming technology. You can also install it directly on any computer using one of the installers in the download package. Unattended installations are supported.

Install the .adm or .admx file by adding it to Group Policy (GP).

Installing the .msi file and the .adm or .admx file alone does not enable Profile Management. You must enable it separately (using the procedure To enable Profile management) after performing all other setup tasks.

Citrix recommends that the same version of Profile Management is installed on all user devices and the same version's .adm or .admx file is added to each Group Policy Object on all domain controllers. This prevents corruption of profile data, which may result when different user store structures (from different versions) exist.

> **Note**
>
> In Profile Management 5.x releases, Citrix maintains the same user store structure, except that Citrix updates profile versions by following Microsoft operating system updates.

This procedure installs Profile management on a single computer.

1. Log on to the computer with administrator privileges.
2. Locate and run the appropriate installer from the download package. The installation wizard appears.
3. Follow the on-screen instructions in the wizard.
4. Restart the computer.

Important: In an earlier version of Profile Management, the following keys were removed from the registry exclusion list in the supplied .ini file:

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Group Policy
- HKEY_CURRENT_USER\Software\Policies
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies

If you use these exclusions in Group Policy and set OVERWRITEINIFILES=yes in this procedure, ensure you add all three of the keys or none of them (but not a subset) to the registry exclusion list. (The OVERWRITEINIFILES option is primarily intended for deployments using Group Policy rather than an .ini file, or for either deployment type in which configuration settings can be discarded and the default .ini file re-installed.) The option overwrites all of the changes you made throughout the .ini file including the keys. Citrix recommends running the installer without this option and then manually removing the key settings in the .ini file. Alternatively, if you use this option, ensure you add the exclusions as described. For more information on preserving exclusions during installation, see the Sepago blog at http://www.sepago.de/sepago-backstage/blogs/.

1. At a command line, run the following command:
   msiexec /i <path to the MSI file> /quiet [/norestart] [INSTALLDIR=<installation directory>] [OVERWRITEINIFILES=yes] [INSTALLPOLICYINIFILES=no]
   This command performs the installation without displaying a user interface and then performs a restart.

   If UAC is enabled, run the msiexec command with elevated rights, for example from an elevated command prompt.

   You can suppress the restart using the /norestart option, but, depending on the operating system, Profile management might not function until the computer has restarted. For example, you do not need to restart Windows 7 workstations.

   INSTALLDIR can be user specified.

   For information on the OVERWRITEINIFILES=yes option, see Upgrade Profile management.

Setting INSTALLPOLICYINIFILES to no prevents the installation of the Profile management .ini file. If you have used the .ini file with a previous version of the software and want to continue to use the settings contained in it with this version, after installation transfer each setting manually to the equivalent Profile management policy in Group Policy Editor.

If UAC is enabled, run the msiexec command with elevated rights, for example from an elevated command prompt.

2. If you are upgrading, a dialog box may advise you that some files are in use. You are given the option to close the application or continue without closing. Select the option to close the application.

Use this procedure if no earlier version of the Profile Management .adm file is present in Group Policy. If you are upgrading an .adm file, see Upgrade Profile management.

In production environments, configure Profile Management with Group Policy. For each OU containing the computers you want to manage, create and link a Group Policy Object (GPO), and then add the Profile Management .adm or .admx file to the GPO.

To configure Citrix user profiles, you can use any computer that runs Windows Group Policy Management Console. The computer does not have to be a domain controller. Domain controllers only store the .adm or .admx file.

Note: For small pilot projects and evaluations where no separate test deployment of Active Directory (AD) is available, you can also use the installed .ini file instead of the .adm or .admx file. If, after successful testing, you move from the .ini file to an AD deployment, be sure to add to the .adm or .admx file any required inclusions and exclusions in addition to the minimum defaults that are documented in Default inclusions and exclusions.

1. On the domain controller, do one of the following:
   - Import the .adm file. The file is located in the GPO folder in the download package.
   - Copy the .admx file from the GPO folder in the download package to the C:\Windows\PolicyDefinitions folder and copy the .adml file to the C:\Windows\PolicyDefinitions\<localized folder>. For example, on English language operating systems, <localized folder> is en-US. Proceed to Step 5.
2. On the computer you want to use to configure Profile management, open Active Directory Users and Computers.
3. Identify the OUs containing the computers that Profile management will be installed on. For information on how to configure Profile management to work in your existing OU structure, see Administer profiles within and across OUs.
4. In Group Policy Management, create a GPO and link it to each OU.
   Note: If you apply security filtering to the GPO, do so using either the Authenticated Users group or a computer group. Do not use a security group that only contains individual users.
5. Edit the GPO in Group Policy Editor:
   1. Expand Computer Configuration and right-click Administrative Templates under the GPO.
   2. Click Add/Remove Templates and click Add.
   3. Browse to the .adm or .admx file that you imported or copied earlier and click Open.
   4. Click Close. This creates a Citrix folder and a Profile Management subfolder that stores the settings from the .adm or .admx file.

> **Note**
>
> Profile Management 5.5 places the ADMX policies node under Citrix Components. To configure Profile Management 5.5:
>
> - Remove the existing .admx files in the [WindowsFolder]\PolicyDefinitions folder, and then copy the ctxprofile5.5.0.admx file and the CitrixBase.admx file to the folder.
> - Remove the existing .adml file in the [WindowsFolder]\PolicyDefinitions\<localized folder>, and then copy the ctxprofile5.5.0.adml file and the CitrixBase.adml file to the folder.

This procedure removes Profile Management from a single computer. You must be an administrator of the computer.

1. To avoid data loss, ensure all users are logged off.
2. From the list of installed programs in Programs and Features, select Profile management and click Uninstall.
3. Click Yes.
4. Restart the computer.

You can also remove Profile Management in unattended mode.

Files included in the download

Aug 14, 2017

The following files are included in this release.

File Name	Description
profilemgt_x86.msi	Installer for 32-bit systems
profilemgt_x64.msi	Installer for 64-bit systems
GPO\ctxprofile5.1.0.adm	.Adm file used in Group Policy
GPO\ctxprofile5.1.0.admx	.Admx file used in Group Policy
GPO\ctxprofile5.1.0.adml	.Adml file used with .admx file in Group Policy
welcome.html	List of documentation resources
CrossPlatform*.xml	Definition files for supported applications

In addition to DLLs and other files, you may need to be aware of the following files, which are created by the installer in the install location (by default, C:\Program Files\Citrix\User Profile Manager).

File Name	Description
UPMPolicyDefaults_all.ini	Profile management .ini file
UserProfileManager.exe	Windows service carrying out functions on computers managed by Profile management

Create the user store

Aug 14, 2017

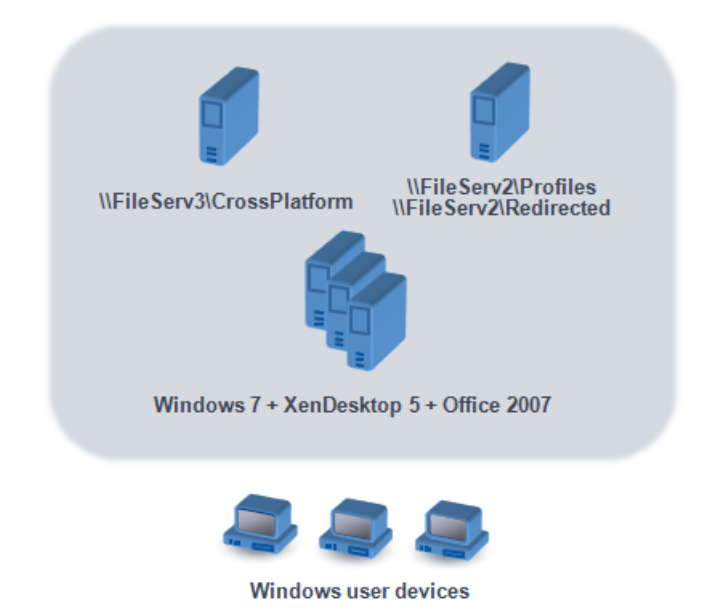
This topic helps you create the user store in a way that best suits your organization. In addition to reviewing the information here, be sure to configure the path to the user store as efficiently as possible (for example, by the sensible use of variables). For advice and examples on that subject, see To specify the path to the user store.

The user store is the central, network location for storing Citrix user profiles.

Any Server Message Block (SMB) or Common Internet File System (CIFS) file share can be used for the user store, but best practice is to ensure that the share:

- Can be accessed by the accounts used with Citrix user profiles
- Is large enough to store profile data
- Is robust in case of disk or network failure

This diagram illustrates an example user store in relation to storage for redirected folder items, the cross-platform settings store (on a separate file server), and Windows 7 virtual desktops published with XenDesktop and running Microsoft Office. User devices that access the virtual desktops are also shown for reference.



Recommendations on creating secure user stores are available in the article called Create a file share for roaming user profiles on the Microsoft TechNet Web site. These are minimum recommendations that ensure a high level of security for basic operation. Additionally, when configuring access to the user store include the Administrators group, which is required in order to modify or remove a Citrix user profile.

If your deployment includes multiple platforms, review the information on Version 1 and Version 2 profile types in Plan for multiple platforms The structure of the user store is described in Profile management architecture.

Note: If an application modifies the access control list (ACL) of a file in the user's profile, Profile management does not replicate those changes in the user store. This is consistent with the behavior of Windows roaming profiles.

Test Profile Management with a local GPO

Aug 14, 2017

Before deploying Profile management in a production environment, Citrix recommends using a test environment. You can create this setup on a local machine with the supplied .ini file, but a fully supported and easier means of transferring settings to the domain GPO is based on a local installation and configuration of the ADM file on a device. Test logon and logoff behaviors and make adjustments to the local GPO until satisfactory results are obtained. You can perform tests safely this way if the device is a member of a production OU because local policies are invoked where OU and domain policies do not exist or are not configured. When using local policies, ensure no Profile management GPOs are used anywhere else (for example, in the domain or sites).

In addition, where an administrator does not have access to or control of domain GPOs for the configuration of the Profile management ADM file, local GPOs can be used as a long-term solution. However, this introduces complexities into the environment, such as ensuring that the Profile management ADM file is installed and correctly configured on each device and the inability of domain users to maintain settings when accessing multiple devices.

Important: For these reasons Citrix does not recommend the use of local GPOs as a long-term, enterprise solution.
If you are testing on Windows 2008 domain controllers, consider using a Windows Management Instrumentation (WMI) filter to temporarily restrict your configuration to just one machine in an OU.

Minimizing differences in the end user experience when accessing resources from various devices is the ultimate goal when implementing a profile solution. Before Profile management, the contents of users' registry and files might vary depending on the physical device, profile configuration, and operating system. For this reason, Profile management should be configured to address the differences between system installations on computers the users will roam between.

You should therefore check user access to resources in ways that mimic your production environment. These may include:

- A client device with locally installed applications
- A virtual desktop created with Citrix XenDesktop and including streamed or locally installed applications
- A Citrix XenApp application, either published on or streamed from a XenApp server
- A Terminal Services client

Users may access applications from different operating systems, and the variation between them may create conflicting settings within a single user profile. You should understand the differences between Version 1 and Version 2 profiles and how they affect your deployment, since the variations are key to any profile solution. For more information on Version 1 and Version 2 profiles, see About profiles.

Upgrade and migrate

Aug 14, 2017

This section contains procedures for upgrading Profile Management software and information about transitioning your existing Windows user profiles to Citrix user profiles. For example, you can easily upgrade from Version 3.x to Version 5.x using those procedures.

Before upgrading, understand which Profile Management features and settings are available in the release you are upgrading from and to. To review this information, see Profile Management policies. To facilitate upgrades from .ini files to Group Policy, that topic also maps the setting names in the .ini file to those in the .adm and .admx files.

Do not configure Profile Management (either in Group Policy or with the .ini file) while upgrading. Separate these two tasks by upgrading your deployment first and then configuring settings as required, ideally by answering the questions in Decide on a configuration.

Tip: You can hotfix your deployment of Profile Management 2.1.1 or later by upgrading to the latest version. After upgrading, you can, if desired, enable any later feature.

For deployments in which different versions of Profile Management coexist, you should:

- Minimize the time that a mixed deployment exists
- Add the latest version's .adm or .admx file to each Group Policy Object on all domain controllers, ensuring all new features are disabled and allowing time for the new policies to propagate
- Upgrade all computers to the latest version of Profile Management before enabling any policy

Mixed deployments that contain Versions 5.x and 3.2 are supported. However, treat such deployments as a temporary state that exists during migration from the earlier version to the later one.

Important: Deployments that contain Version 5.x with Version 2.1.1 or any earlier version, including Citrix Technical Preview or beta releases, are unsupported. However, if you cannot upgrade, and those versions must coexist in your deployment, you may find the rest of this topic helpful.

The rest of this topic contains information on the coexistence of Profile Management 2.1.1 or earlier, and Profile Management 3.x, or 5.x. It tells you how to migrate from one version to the other. In this topic, the terms Version 2 and Version 5 are used as shorthand for these versions.

Isolate each version in a separate OU and maintain separate user stores for the computers running each version. Alternatively, if a single user store serves computers running both versions, ensure all Version 5 settings are disabled until all the computers have been upgraded to Version 5. After you enable any Version 4 setting in a "mixed" user store, users can still log on to a computer that runs Version 2, but they receive a temporary Windows user profile (not their network, Citrix user profile) and changes they make to that profile are not saved. This is why you should consider mixed deployments to be temporary, and minimize the time they exist before completing the upgrade.

Using separate OUs and user stores can be inconvenient. To avoid these constraints, you can use one of the following two strategies. You configure each group in the appropriate version of Profile Management using the Processed groups setting. Strategy 2 is more work than Strategy 1 because, with the former, you keep updating the Version 5 processed user groups and maintain two sets of applications and desktops (but you can automate by exporting application definitions from

XenApp). The advantage is that you can take your time over the migration.

Note: As an alternative to the following strategies, with Windows Server 2008 Active Directory you can use WMI filtering to apply a GPO to a subset of computers in an OU, and determine which version of Profile Management is installed. This allows you to automatically adjust which policy is applied, to match the version.

This scenario assumes that some downtime is acceptable. All computers are migrated at the same time.

The migration strategy is:

1. Replace the Version 2 ADM file with the Version 5 file. The latter is compatible with the earlier version, so Version 2 computers continue to operate normally.
2. Ensure all of the Version 5 settings are disabled. Do not rely on the default **Not enabled**.
3. Start upgrading all the computers from Version 2 to Version 5. Fit this in with your normal maintenance and update schedules. With one exception, Version 5 acts as Version 2 until you enable any Version 5 setting. The exception is as follows. It is rare but more likely to occur if this upgrade step is staggered over a long time. If a user accesses their Citrix user profile from multiple servers, multiple Version 4 sessions are created. For example, they first use a workstation to access a virtual desktop on one server and then a laptop to access a published application on another. Profile Management must use the pending area for the second, laptop session. At this point, the entire OU is treated as a Version 5 deployment (albeit one without any configured Version 5 features) and PmCompatibility.ini is updated to reflect this.
4. Optionally, set your Version 5 processed users group to include only the members of a small pilot group. Wait for the AD Group Policy changes to propagate throughout the network (for example, over a weekend). You do not need to prevent access for any other users while this is happening. Back up the profiles of the pilot group. Then let the pilot group test Profile Management.
5. When you are happy with the pilot group results, ensure that you have backed up the other users' profiles.
6. Use the next scheduled maintenance period to add the remaining users to the Version 5 processed users group. Allow sufficient time for the AD Group Policy changes to propagate, and let the remaining users log on.

This scenario assumes that you cannot move all your machines or your users to the new version in one go, so you select subsets of users that you migrate in batches. It suits deployments with several datacenters or geographically distributed users.

The migration strategy is:

1. Replace the Version 2 ADM file with the Version 5 file. The latter is compatible with the earlier version, so Version 2 computers continue to operate normally.
2. Ensure all of the Version 5 settings are disabled. Do not rely on the default Not enabled.
3. Upgrade a few computers (the first batch) to Version 5. Alternatively, install Version 5 on new computers. By default, your Version 5-processed users group contains an empty group, so no user is processed as a Version 5 user. Be aware of the exception described in Strategy 1, which may also apply when you upgrade computers in a phased migration.
4. Publish new applications (using XenApp) or virtual desktops (using XenApp or XenDesktop) from your Version 5 computers. These applications and desktops are identical to the ones previously published from your Version 2 computers, except for their names, which identify them as for use by Version 5 users.
5. The selected users in this batch log on to the applications or desktops (for example, using Web Interface). They choose the new applications. (Use Web Interface to enforce this, based on user name or group membership). As a result, their sessions run on the Version 4 computers but they are processed with Version 2 settings.
6. Ensure that you have backed up all users' profiles.

7. Move the users out of the Version 2 processed users group and into the Version 4 group. Wait for the AD Group Policy changes to propagate to the Version 5 computers. Next time they log on, the users' sessions are processed with Version 5 settings.
8. Upgrade the next batch of computers and migrate the next batch of users, as above.

Upgrade Profile Management

Aug 14, 2017

This topic provides guidance on upgrading your Profile Management deployment by using Active Directory.

Important: It is important that you follow the order of the steps in this upgrade process. Upgrade the software on all computers only after adding the new .adm or .admx file to Group Policy. If you upgrade beforehand, log files might be stored in two locations (one containing log files for the old version and the other for the new version). This consideration particularly affects XenDesktop deployments.

It is also important to perform upgrades during a scheduled maintenance period or at a time when Active Directory replication allows the changes to propagate through your deployment. Typically, this can take up to 24 hours.

The upgrade process involves:

1. Creating a new Group Policy Object (GPO) and adding the new .adm or .admx file to the new GPO

   - or -

   Upgrading an existing .adm or .admx file as described in Step 1 below

2. Upgrading the .msi file on all computers as described in Step 2 below
3. Applying the GPO.

If any earlier version of the Profile Management .adm file already exists in Group Policy, you can upgrade it by using this procedure. All policy settings in the earlier version are preserved when you upgrade. For more information, see A new .adm or .admx file is released with a new version of the software. What do I do?.

1. On the domain controller, do one of the following:
   - Import the existing .adm file. The file is located in the GPO_Templates folder in the download package.
   - Copy the .admx file from the GPO_Templates folder in the download package to the C:\Windows\PolicyDefinitions folder and copy the .adml file to the C:\Windows\PolicyDefinitions\<localized folder>. For example, on English operating systems, <localized folder> is en-US.
2. On the computer you use to configure Profile Management, open Active Directory Users and Computers.
3. In the Group Policy Object Editor, right-click Administrative Templates and select Add/Remove Templates.
4. Select the existing version of the Profile Management .adm file (for example, ctxprofile5.4.1), click Remove and then Close. The Administrative Templates\Citrix folder is deleted.
5. Right-click Administrative Templates and select Add/Remove Templates again.
6. Click Add, browse to the location of the new version of the .adm or .admx file (for example, ctxprofile5.5.0), select it, and click Close. The new file is imported but the old settings are retained.

Citrix recommends that you install the same version of Profile Management on all user devices and that you add the .adm or .admx file of that same version to each Group Policy Object on all domain controllers. Doing so prevents corruption of profile data, which might result when different user store structures (from different versions) exist.

Citrix recommends that you upgrade all computers to the latest version of Profile Management before enabling any new setting. To check whether a setting is new in the version you are using, see Profile Management Policies.

1. Ensure that all users are logged off from the computers you want to upgrade.
2. Install the new version of Profile Management over the existing version by running the .msi file on each computer. For more information, see Install and set up Profile Management.

If you edited the .ini file in an earlier version of Profile Management and upgrade to a newer version, the software detects that the file was edited and, by default, does not overwrite it. If you want to preserve your .ini file settings but also make use of the new settings in the newer version, you must do one of the following:

- Manually add the new settings from the .ini file of the newer version to your existing, edited .ini file.
- Save a copy of the existing, edited version's .ini file, use the OVERWRITEINIFILES=yes command-line option to force an overwrite of the file during the upgrade and add your saved settings to the upgraded .ini file. For example:

  msiexec /i <path to the MSI file> /quiet [INSTALLDIR=<installation directory>] [OVERWRITEINIFILES=yes] [INSTALLPOLICYINIFILES=no]

> ## Note
>
> To configure Profile Management policy through HDX, you must:
>
> - upgrade your Delivery Controller(s). The reason is that HDX reads the Profile Management policy settings from the UserProfileManager_PowerShellSnapIn.msi file present in the XenApp and XenDesktop layout image-full\x64\Citrix Desktop Delivery Controller.
> - upgrade your VDAs so as to get the latest version of Profile Management.

More Resources

- Frequently asked questions about upgrading Profile Management.
- Profile Management Policies.
- Install and set up Profile Management.

Frequently asked questions about upgrading Profile Management

Aug 14, 2017

This topic contains questions and answers about upgrading to Citrix Profile Management 5.0.

For more information on upgrading Profile Management and how different versions coexist, see the Citrix Profile Management blog.

Important: Do not upgrade from versions earlier than Version 3.0.

Test Profile Management before rolling out the software in a production environment. Your pilot must use a separate Organizational Unit (OU), and must not use the same accounts as users in the production environment. It must at least use a different user store.

For upgrades from Version 2.x, note that Version 5.0 marks profiles in the user store with Version 5.0 tags because it uses a schema newer than that used in Version 2.0. Version 2.1.1 can detect the new schema but cannot process it, so it tries to load a temporary profile to avoid overwriting data managed by Version 5.0. This is undesirable in a production environment. Citrix recommends using a different user store for testing Version 5.0.

The .adm and .admx files are designed so you can replace .adm files from earlier releases. The existing settings are preserved. You can replace the files in the same Group Policy Object (GPO). You do not have to create a GPO, but if you prefer to do so, see the instructions in Upgrade Profile Management.

For upgrades from Version 2.x, you must not enable any of the new features in Profile Management 5.0 while the upgrade is in progress. Version 5.0 has a different schema, which would be corrupted if Version 2.x wrote to it. A compatibility check was introduced in Profile Management 2.1.1 to help avoid the resulting corruption if this version runs in an environment that also includes a later version.

During the upgrade process, ensure that Profile Management is not running. Some machines have the old configuration and others have the new one, which can lead to inconsistencies or temporary profiles being assigned.

When all upgrades are completed and no Profile Management 2.x systems are present, it is safe to enable the desired version 5.0 features in the GPO. Do this during a scheduled maintenance period, and allow time (typically 24 hours) for the Active Directory (AD) changes to propagate.

This topic describes rolling back from Version 5.0 to any earlier version.

Important: Rolling back to an earlier version has not been officially tested and can be difficult.
The most important step is to revert the schema, which must be done for every user's profile while all users are logged off (during a scheduled downtime).

Each user's profile in the user store contains a file in the root directory called PmCompatibility.ini, which must be deleted. After all these files are deleted, you can revert to the earlier version and restart the deployment with that version's .adm file.

If the PmCompatibility.ini files are not deleted, the earlier version checks, finds that Version 5.0 systems also use the user store, gives the user a temporary profile, and asks them to alert their support desk. They can tell the user to log off and then manually delete the .ini file from the user store.

To migrate user profiles

Aug 14, 2017

This topic contains instructions on turning Citrix user profiles into Windows roaming profiles. It also describes how to remove Citrix user profiles from personal vDisks (a Citrix XenDesktop feature) so Profile management can process them. For more information on migration strategies, see Upgrading Profile Management and Migrating Profiles.

You can migrate Citrix user profiles to Windows roaming profiles at any time. This involves moving profile data to a network location where the roaming profiles will be stored. After migration, Profile management takes no part in processing user logons or application settings.

1. Ensure all users are logged off.
2. Remove the Profile Management Service from all of the computers that are managed by the software.
3. In the user store, move the contents of \UPM_Profile to your roaming profile location. You do not have to move the contents of the cross-platform settings store.
4. In addition, for Version 1 profiles only, remove the _upm_var suffix from all subfolders of \UPM_Profile.
   Note: You may find that scripting simplifies this step.

If you use the Personal vDisk feature in XenDesktop, by default user profiles are stored on the Personal vDisk's P: drive not the virtual desktop's C: drive. If instead you want Citrix Profile management (not the Personal vDisk) to process the profiles, you adjust this default when installing the Virtual Desktop Agent by modifying the Registry on the master image used for a new catalog. In this scenario, because the catalog is new, no users have logged on, so no profiles are stored on the P: drive.

Important: An alternative scenario occurs if you enable Profile management on machines in existing catalogs with Personal vDisks. Because the catalog is already in use, logons will already have taken place and profiles will be present on the P: drive (and will remain there after you modify the Registry). You must therefore adjust the default differently.
Issues that indicate the presence of profiles on P: drives while Profile management is enabled include users having to reset their wallpaper, having to reconfigure their applications, or receiving temporary profiles.

Follow these instructions to adjust the default in this alternative scenario.

1. Schedule a maintenance downtime for the virtual machines whose profiles you want to migrate.
2. Create a startup script (or edit your existing script) and include a command to run Delprof.exe, a profile deletion tool for Windows XP from Microsoft, or Delprof2.exe. a similar tool for later operating systems from Sepago. Follow the run command by a shutdown command:
   \\<share name>\delprof.exe /q /i
   shutdown /s /t 0
   You can download Delprof.exe from the Microsoft Web site. For information on this tool, see http://support.microsoft.com/kb/315411.
3. On the master image, change the following Registry setting from 1 to 0:
   Caution: Editing the registry incorrectly can cause serious problems that may require you to reinstall your operating system. Citrix cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk. Be sure to back up the registry before you edit it.
   HKLM\Software\Citrix\personal vDisk\Config\EnableUserProfileRedirection

4. Update the master image's inventory.
5. During the scheduled downtime, distribute the master image to the virtual machines, and ensure they restart. At that point, the script runs, deletes the profiles from the P: drives, and shuts down the machines.
6. When all of the machines are shutdown, delete the startup script (or the line you added to your existing script).
7. Start all of the machines or let users log on. From this point, profiles are stored on the virtual desktops' C: drives.

Note: To migrate profiles in the reverse direction so they are managed by the personal vDisk (not Profile management), follow these instructions but change the Registry setting of EnableUserProfileRedirection from 0 to 1. This loads the profiles on to the personal vDisk's P: drive.

Configure

Aug 14, 2017

This topic introduces how to configure Profile Management policies to meet your deployment requirements. For instructions on setting a policy, see Manage.

Manage

Aug 14, 2017

Important: The following policy generally does not require configuration. Unless instructed to by Citrix personnel, leave it in its default settings.

Policy: Number of retries when accessing locked files

It is most unlikely that you will need to enable this policy.

During logoff, if there are any locked files, the Profile Management Service tries the specified number of times to access the files and copy them back to the user store. But typically the Service only needs to read (not write to) the files for the copy operation to succeed. If any locked files exist, the Service does not delete the local profile and instead leaves it "stale" (as long as the appropriate policy was enabled).

Citrix recommends that you do not enable this policy.

To resolve conflicting profiles

Aug 14, 2017

Conflicts between local Windows user profiles and Citrix user profiles (in the user store) can occur when you add Profile management to an existing deployment. In this scenario, you must determine how the data in the local Windows profile is managed.

1. Under Profile Management, open the Profile handling folder.
2. Double-click the Local profile conflict handling policy.
3. Select Enabled.
4. Select one of the following options from the drop-down list:
   - Use local profile. Profile management processes the local Windows user profile but does not change it in any way.
   - Delete local profile. Profile management deletes the local Windows user profile and then imports the Citrix user profile from the user store.
   - Rename local profile. Profile management renames the local Windows user profile (for backup purposes) and then imports the Citrix user profile from the user store.

If Local profile conflict handling is not configured here, the value from the .ini file is used. If this setting is not configured here or in the .ini file, existing local profiles are used.

For your changes to take effect, run the gpupdate /force command from the command prompt as documented at http://technet.microsoft.com/en-us/library/bb490983.aspx.

To specify a template or mandatory profile

Aug 14, 2017

By default, new Citrix user profiles are created from the default user profile on the computer where a user first logs on. Profile management can alternatively use a centrally stored template when creating new profiles. The template can be a standard roaming, local, or mandatory profile that resides on any network file share.

Any variation in different devices' default user profiles results in differences in the base profile created for the user. This means you can regard your selection of a template profile as a Global Default User profile.

As prerequisites:

- Ensure the template profile does not contain any user-specific data
- Ensure users have read access to the template profile
- Convert a mandatory profile to a template profile by renaming the file NTUSER.MAN to NTUSER.DAT
- Remove SACLs from NTUSER.DAT in the template profile

For information on creating template profiles by customizing existing Microsoft profiles, see http://support.microsoft.com/kb/959753and http://support.microsoft.com/kb/973289.

1. Under Profile Management, open the Profile handling folder.
2. Double-click the Template profile policy.
3. Select Enabled.
4. In Path to the template profile, enter the location of the profile you want to use as a template or mandatory profile. This is the full path to the folder containing the NTUSER.DAT registry file and any other folders and files required for the template.
   Important: If the path consists only of NTUSER.DAT, ensure that you do not include the file name in the path. For example, with the file \\myservername\myprofiles\template\ntuser.dat, set the location as \\myservername\myprofiles\template.
   Use absolute paths, which can be UNC paths or paths on the local machine. You can use the latter, for example, to specify a template profile permanently on a Citrix Provisioning Services image. Relative paths are not supported.

   This policy does not support expansion of Active Directory attributes, system environment variables, or the %USERNAME% and %USERDOMAIN% variables.

5. Optionally, select a check box to override any existing Windows user profiles. If a user has no Citrix user profile, but a local or roaming Windows user profile exists, by default the local profile is used (and migrated to the user store, if this is not disabled). This can be changed by enabling the checkbox Template profile overrides local profile or Template profile overrides roaming profile. Additionally, identify the template as a Citrix mandatory profile. Like Windows mandatory profiles, changes cannot be saved to Citrix mandatory profiles.

If Template profile is not configured here, the value from the .ini file is used. If this setting is not configured here or in the .ini file, no template or mandatory profile is used.

For your changes to take effect, run the gpupdate /force command from the command prompt as documented at http://technet.microsoft.com/en-us/library/bb490983.aspx.

To choose a migration policy

Aug 14, 2017

When a user first logs on after Profile management is enabled, no Citrix user profile for them exists but you can migrate their existing Windows user profile "on the fly" during logon. Decide which existing profile (roaming, local, or both) is copied and used in all further processing.

For more information on planning a migration strategy, see Migrate profiles? New profiles?. In addition, review the system requirements for migrating existing profiles in System requirements.

1. Under Profile Management, open the Profile handling folder.
2. Double-click the Migration of existing profiles policy.
3. Select Enabled.
4. Select one of the following options from the drop-down list:
   - Local. Use this setting if you are migrating local profiles.
   - Local and Roaming. Use this setting if you are migrating local and roaming profiles (including Remote Desktop Services profiles, formerly known as Terminal Services profiles).
   - Roaming. Use this setting if you are migrating roaming profiles or Remote Desktop Services profiles.

If Migration of existing profiles is not configured here, the value from the .ini file is used. If this setting is not configured here or in the .ini file, existing local and roaming profiles are migrated. If this setting is disabled, no profile is migrated. If this setting is disabled and no Citrix user profile exists in the user store, the existing Windows mechanism for creating new profiles is used as in a setup without Profile management.
For your changes to take effect, run the gpupdate /force command from the command prompt as documented at http://technet.microsoft.com/en-us/library/bb490983.aspx.

To enable Profile Management

Aug 14, 2017

By default, to facilitate deployment, Profile management does not process logons or logoffs. Enable Profile management only after carrying out all other setup tasks and testing how Citrix user profiles perform in your environment.

1. Under Profile Management, double-click the Enable Profile management policy.
2. Select Enabled.

If this setting is not configured here, the value from the .ini file is used. If this setting is not configured here or in the .ini file, Profile management does not process Windows user profiles in any way.

For your changes to take effect, run the gpupdate /force command from the command prompt as documented at http://technet.microsoft.com/en-us/library/bb490983.aspx.

Configuration precedence

Aug 14, 2017

You can configure Profile management using Group Policies and the .ini file. Configuration settings are applied as follows:

1. Settings defined by Group Policies take precedence. The .ini file will only be queried if a policy setting is set to **Not Configured**.
   Note: If you apply a Group Policy Object selectively to sites and domains within an Organizational Unit, a further precedence applies. See *Defining the scope of application of Group Policy* documented at https://technet.microsoft.com/en-us/library/cc754948(v=ws.10).aspx. In addition, note that domain and OU Group Policies take precedence over local policies.
2. Where a setting is not defined by a policy, Profile management tries to read the setting from the .ini file.
3. If a setting is not configured by a group policy or in the .ini file, the default setting is used.

In XenDesktop 7 deployments, be aware of the additional precedence introduced by XenDesktop policies. For information on this, see the topic User profiles in the XenDesktop documentation.

There may be situations where you want to configure the same setting differently in Group Policy and the .ini file, for example when you want to activate default logging with a Group Policy setting but activate verbose logging using the .ini file on a computer that you use for troubleshooting.

About the Profile Management .ini file

Aug 14, 2017

Profile Management comes with a default configuration stored in an .ini file. This must be located in the installation folder so that the Profile Management Service can recognize it. The default configuration is suitable for most environments. It processes the profiles of all users in all groups.

If you have a non-English deployment of Profile management running on Windows XP or Windows Server 2003, you must create an appropriate language version of the .ini file using UPMPolicyDefaults_all.ini. Rename a copy of this file to reflect your language (for example, UPMPolicyDefaults_all_es.ini for Spanish) and localize the folder names. Use these file names:

- For French operating systems, UPMPolicyDefaults_all_fr.ini
- For German operating systems, UPMPolicyDefaults_all_de.ini
- For Spanish operating systems, UPMPolicyDefaults_all_es.ini
- For Japanese operating systems, UPMPolicyDefaults_all_ja.ini
- For Simplified Chinese operating systems, UPMPolicyDefaults_all_zh-CN.ini

If you add entries to the .ini file, ensure the variables and values have the correct format.

Flags (on/off indicators) must be of this form:
<variable>=<value>
A value of 1 enables a setting and any other value or no value disables it. For example, the following entry enables the ServiceActive setting:
ServiceActive=1
Any of the following entries disable the setting:
ServiceActive=ON
ServiceActive=OFF
ServiceActive=TRUE
ServiceActive=FALSE
ServiceActive=
List entries must be of this form:
<value>=
Do not append 1 after the equals sign. For example, the following entry specifies Microsoft Office files to be synchronized:
[SyncFileList]
AppData\Local\Microsoft\Office*.OfficeUI
Changes to Group Policy settings take effect when a manual or automatic policy refresh occurs on the target computers. Changes to the .ini file take effect when you issue the command gpupdate /force, which is recommended, or when you restart the Profile Management Service on the target computers.

Include and exclude items

Aug 14, 2017

This topic describes the process that Profile management uses to include and exclude items from users' profiles. You need to understand this process if you decide to modify the default inclusion or exclusion lists to improve the logon and logoff experience of your users. To help you determine whether this is required, see Which applications?

For example, you might include Microsoft Word because it is a highly customizable and frequently used application that should present the same experience to roaming users however it is accessed. Conversely, you might exclude an enterprise application because it is infrequently used by some groups so its profile data does not need to be downloaded at each logon and logoff.

By default, all files and folders in local profiles are synchronized with the user store. You can specify files and folders that you do not want to synchronize by adding them to an exclusion list. If you exclude a folder, you can specify subfolders of it that you do want to synchronize by adding them to an inclusion list.

You can include and exclude:

- Files and folders contained inside profiles.
- Files and folders that store personalization settings outside profiles.
- Registry entries in the HKCU hive that store personalization settings. Entries in the HKLM hive are not processed by default and cannot be configured to do so.

Before tuning the contents of your users' profiles, consider using the set of built-in Windows Performance Monitoring (Perfmon) counters. These provide insights into the behavior of your profiles. Available counters include measurements of the profile size and the time taken to create a Citrix user profile on the local computer.

You may need to decide whether to cache profiles locally (on the computers that run Profile management). Factors that affect the decision include the Citrix products in your deployment, the available space on the local computers, and the number of users in the deployment.

All included and excluded folder names are language specific. However, folder names in the user store are in a format independent of the operating system language.

You can synchronize files or folders on disks that are treated as local by the operating system. You cannot synchronize files or folders on network mapped drives.

For existing users, the entire HKCU hive is copied to the user store. For new users, the hive of their Microsoft local, roaming, default, or template profile is copied. Inclusions are added and exclusions are removed from the hive when changes are made to the user store.

Changes to registry key values are not preserved. This is by design and supports the typical use case in which an administrator provides users with a template profile containing a registry value that should not be changed (for example, in order to standardize the functioning of a particular application). If you have a template profile that contains unwanted

keys, use a tool such as Profile Nurse from Sepago to eliminate them from the user store.

Exclusions are processed at logoff not logon. They do not delete data from the user store but prevent new data from being written to it.

Other than the default exclusions, typically you do not need to exclude any items when you first roll out Profile management. Later, as you track application performance and gather feedback from users, you may need to exclude items if settings from multiple applications clash or if a user's NTUSER.DAT file grows very large as a result of collecting unneeded settings.

Do not add redirected folders as exclusions.

Important: Citrix recommends that you exclude the folder AppData\Local and AppData\LocalLow from synchronization. If you do not, a very large amount of data may be transferred over the network and users may experience logon delays. These folders are not synchronized by standard Windows roaming profiles. In the default configuration, the exclusion lists contain these folders.

The following rules are used when Profile management includes and excludes files, folders, and registry keys:

1. All items are included by default
2. If the same path is configured as both an inclusion and an exclusion, the inclusion takes precedence
3. An inclusion takes precedence over an exclusion in the same folder
4. An inclusion takes precedence over an exclusion higher up in the folder hierarchy
5. An exclusion takes precedence over an inclusion higher up in the folder hierarchy

These rules result in sensible and intuitive behavior; all items are included by default. From that starting point, you can configure top-level exceptions as exclusions, then configure deeper exceptions to the top-level exceptions as inclusions, and so on.

Default inclusions and exclusions

Aug 14, 2017

This topic describes the default items that Profile management includes in and excludes from its processing. Depending on the applications in your deployment, additional (non-default) items may be required. To help you determine which additional items you need to include or exclude, see Which applications?

Important: If you use Group Policy rather than the .ini file (or you are rolling out a Group Policy deployment after a successful test with the .ini file), note that, unlike the installed .ini file, no items are included or excluded by default in the .adm or .admx file. This means you must add the default items manually to the file. These are shown in the tables in this topic. Note the following:

- Use Profile Management Policies to map setting names in the .ini file and the .adm or .admx file, and to understand how the Profile management variables (for example, !ctx_internetcache!) expand
- When pasting inclusions and exclusions from the .ini file, remove the trailing = (equals sign) from each item
- Do not add an initial backslash to inclusions and exclusions

Default Value
<empty>

Default Value
Software\Microsoft\AppV\Client\Integration=
Software\Microsoft\AppV\Client\Publishing=
Software\Microsoft\Speech_OneCore=

Note: If you are using Microsoft App-V, this exclusion is not correct and different exclusions are required as documented at Profile management and App-V.

Default Value
<empty>

All folders in the profile are included by default.

Folders in this table are excluded from synchronization.

Default Value
!ctx_internetcache!=
!ctx_localappdata!\Google\Chrome\User Data\Default\Cache=
!ctx_localappdata!\Google\Chrome\User Data\Default\Cached Theme Images=
!ctx_localappdata!\Google\Chrome\User Data\Default\JumpListIcons=
!ctx_localappdata!\Google\Chrome\User Data\Default\JumpListIconsOld=
!ctx_localappdata!\GroupPolicy=
!ctx_localappdata!\Microsoft\AppV=
!ctx_localappdata!\Microsoft\Messenger=
!ctx_localappdata!\Microsoft\Office\15.0\Lync\Tracing=
!ctx_localappdata!\Microsoft\OneNote=
!ctx_localappdata!\Microsoft\Outlook=
!ctx_localappdata!\Microsoft\Terminal Server Client=
!ctx_localappdata!\Microsoft\UEV=
!ctx_localappdata!\Microsoft\Windows Live=
!ctx_localappdata!\Microsoft\Windows Live Contacts=
!ctx_localappdata!\Microsoft\Windows\Application Shortcuts=
!ctx_localappdata!\Microsoft\Windows\Burn=
!ctx_localappdata!\Microsoft\Windows\CD Burning=
!ctx_localappdata!\Microsoft\Windows\Notifications=

!ctx_localappdata!\Packages=
!ctx_localappdata!\Sun=
!ctx_localappdata!\Windows Live=
!ctx_localsettings!\Temp=
!ctx_roamingappdata!\Microsoft\AppV\Client\Catalog=
!ctx_roamingappdata!\Sun\Java\Deployment\cache=
!ctx_roamingappdata!\Sun\Java\Deployment\log=
!ctx_roamingappdata!\Sun\Java\Deployment\tmp=
$Recycle.Bin=
AppData\LocalLow=
Tracing=

Default Value
<empty>

All files in the profile are included by default.

Default Value
<empty>

No files in the profile are excluded by default.

To include and exclude items

Aug 14, 2017

As a prerequisite, ensure that you understand how inclusions and exclusions work. For information on this, see Include and exclude items. For information on the default included and excluded items, see Default inclusions and exclusions.

Use Enter to separate multiple entries when you include and exclude items.

Tips: If desired, you can include specific top-level folders. In a collaborative environment, this has the advantage of signaling critical folders to other administrators.

1. Under Profile Management > Registry, double-click the Inclusion list policy.
2. Select Enabled.
3. Add any profile-related registry keys in the HKCU hive that you want to be processed during logoff. Example: Software\Adobe.
4. Under Profile Management > File system > Synchronization, double-click the Directories to synchronize policy.
5. Select Enabled.
6. Add any folders that you want Profile Management to process but that are located in excluded folders.
   Profile Management synchronizes each user's entire profile between the system it is installed on and the user store. It is not necessary to include subfolders of the user profile by adding them to this list. Paths on this list can be absolute or relative. Relative paths are interpreted as being relative to the user profile. Example:

   - Desktop\exclude\include. Ensures that the subfolder called include is synchronized even if the folder called Desktop\exclude is not.
7. Under Profile Management > File system > Synchronization, double-click the Files to synchronize policy.
8. Select Enabled.
9. Profile Management synchronizes each user's entire profile between the system it is installed on and the user store. It is not necessary to include files in the user profile by adding them to this list.
   This setting allows for the inclusion of files below excluded folders. Paths on this list can be absolute or relative. Relative paths are interpreted as being relative to the user profile. Wildcards can be used but are only allowed for file names. Wildcards cannot be nested and are applied recursively. Examples:

   - AppData\Local\Microsoft\Office\Access.qat. Specifies a file below a folder that is excluded in the default configuration.
   - AppData\Local\MyApp*.cfg. Specifies all files with the extension .cfg in the profile folder AppData\Local\MyApp and its subfolders.

If Inclusion list is not configured here, the value from the .ini file is used. If this setting is not configured here or in the .ini file, all of the HKCU hive is processed.

If Directories to synchronize is not configured here, the value from the .ini file is used. If this setting is not configured here or in the .ini file, only non-excluded folders in the user profile are synchronized. Disabling this setting has the same effect as enabling it and configuring an empty list.

If Files to synchronize is not configured here, the value from the .ini file is used. If this setting is not configured here or in the .ini file, only non-excluded files in the user profile are synchronized. Disabling this setting has the same effect as enabling it and configuring an empty list.

For your changes to take effect, run the gpupdate /force command from the command prompt as documented at http://technet.microsoft.com/en-us/library/bb490983.aspx.

1. Under Profile Management > Registry, click the Exclusion list policy.
2. Select Enabled.
3. Click Show and add any registry keys in the HKCU hive that you do not want to be processed during logoff. Example: Software\Policies.
4. Under Profile Management > File system, double-click the Exclusion list - directories policy.
5. Select Enabled.
6. Add any folders that you do not want Profile Management to process. Folder names can be specified as absolute paths or as paths relative to the user profile (%USERPROFILE%). Use that variable to locate the profile but do not enter the variable itself in this policy. Omit initial backslashes from paths.
   Examples:
   - Desktop. Does not process the Desktop folder in the user profile.
   - MyApp\tmp. Does not process the folder %USERPROFILE%\MyApp\tmp.
7. Under Profile Management > File system, double-click the Exclusion list - files policy.
8. Select Enabled.
9. Add any files that you do not want Profile Management to process. File names can be specified as absolute paths or as paths relative to the user profile (%USERPROFILE%). Use that variable to locate the profile but do not enter the variable itself in this policy. Wildcards are allowed and are applied recursively.
   Examples:
   - *.tmp ignores all temp files in %USERPROFILE%.
   - appData\roaming\MyUnwantedApp*.tmp ignores all files with the extension .tmp in %USERPROFILE% for the specified application.

If Exclusion list is disabled, no registry keys are excluded. If this setting is not configured here, the value from the .ini file is used. If this setting is not configured here or in the .ini file, no registry keys are excluded.

If Exclusion list - directories is disabled, no folders are excluded. If this setting is not configured here, the value from the .ini file is used. If this setting is not configured here or in the .ini file, no folders are excluded.

If Exclusion list - files is disabled, no files are excluded. If this setting is not configured here, the value from the .ini file is used. If this setting is not configured here or in the .ini file, no files are excluded.

For your changes to take effect, run the gpupdate /force command from the command prompt as documented at http://technet.microsoft.com/en-us/library/bb490983.aspx.

Using wildcards

Aug 14, 2017

You can use DOS-style wildcard characters, such as ? (question mark) and * (asterisk), in policies that refer to files (for example, file inclusion and exclusion lists). The ? (question mark) matches a single character. The * (asterisk) matches zero or more characters.

As of Profile Management 7.15, you can use the vertical bar '|' for applying a policy to only the current folder without propagating it to the subfolders.

Wildcards work recursively. Ensure you specify a valid path when using wildcards.

Policies that support wildcards do not support any other type of processing, such as the use of environment variables or Active Directory attributes. You cannot use wildcards in policies that refer to folders or registry entries.

The wildcard <path name>\h*.txt matches house.txt, h.txt, and house.txt.txt, but does not match ah.txt.

The wildcard <path name>\a?c.txt matches abc.txt, but does not match ac.txt.

The wildcard <path name>\a?c*d.txt matches abcd.txt and abccd.txt, but does not match acd.txt.

Configuring policies in profile root folder:

*.txt specifies all files with the extension .txt in the root folder and subfolders.

*h.txt specifies all files that match this wildcard in the root folder and subfolders.

h*.txt specifies all files that match this wildcard in the root folder and its subfolders.

a?c.txt specifies all files that match this wildcard in the root folder and its subfolders.

*.txt| specifies all files with the extension .txt in the root folder without propagating it to the subfolders.

Configuring policies in profile non-root folders:

- Examples for a file name part starts with * or ?

  AppData*.txt specifies all files that match this wildcard in the directory AppData and its subfolders.

  AppData*h.txt specifies all files that match this wildcard in the directory AppData and its subfolders.

- Examples for a file name part not starting with * or ?

  AppData\h*.txt specifies all files that match this wildcard in the directory AppData without propagating it to the subfolders.

  AppData\a?c.txt specifies all files that match this wildcard in the directory AppData without propagating it to the

subfolders.

Note: As of Profile Management 7.15, such configuration is applied to not only the current folder but also the subfolders. For example, AppData\h*.txt specifies all files that match this wildcard in the directory AppData and its subfolders.

To enable logon exclusion check

Aug 14, 2017

When logon exclusion check is set to "1," Profile Management does not synchronize the files and folders specified in the logon exclusion list from the user store to the local profile when a user logs on. When logon exclusion check is set to “2,” Profile Management deletes the files and folders specified in the exclusion list from the user store when a user logs on. By default, logon exclusion check is disabled.

Warning: Setting logon exclusion check to “2” deletes your excluded files and folders from the user store permanently. When you include the excluded files and folders again, these files and folders are deleted from the cached local profile when you log on.

To enable logon exclusion check, follow the steps below:

1. Open the Profile Management .ini file. For more information about the .ini file, see About the Profile management .ini file.
2. Add the EnableLogonExclusionCheck item in the [General Settings] section.
3. To ignore files and folders specified in the exclusion list from the user store, set the value to 1.
   To delete files and folders specified in the exclusion list from the user store, set the value to 2.
   To disable the check, set the value to 0.
   EnableLogonExclusionCheck=1
   EnableLogonExclusionCheck=2
   EnableLogonExclusionCheck=0
4. Save and close the Profile Management .ini file.

For your changes to take effect, run the gpupdate /force command. For more information, see http://technet.microsoft.com/en-us/library/bb490983.aspx.

To define which groups' profiles are processed

Aug 14, 2017

You can define the users whose profiles are processed and those that are not. You can use both computer local groups and domain groups (local, global and universal). Specify domain groups in the format <DOMAIN NAME>\<GROUP NAME>. Specify local groups in the format GROUP NAME.

Note: Computer local groups must be newly created local groups and the members must be domain users.

1. Under Profile Management, double-click the Processed groups policy.
2. Select Enabled.
3. Click Show.
4. Add the groups containing the users whose profiles you want Profile Management to process. Use Enter to separate multiple entries.
   If this setting is not configured here, the value from the .ini file is used. If this setting is not configured here or in the .ini file, members of all user groups are processed unless you exclude them using the Excluded groups policy.

5. Under Profile Management, double-click the Excluded groups policy.
6. Select Enabled.
7. Click Show.
8. Add the groups containing the users you do not want Profile Management to process. Use Enter to separate multiple entries.
   If this setting is not configured here, the value from the .ini file is used. If this setting is not configured here or in the .ini file, no members of any groups are excluded.

9. To manage the profiles of local administrators, under Profile Management, double-click the Process logons of local administrators policy and click Enabled.
   Important: By default, Profile Management recognizes which operating system is in use, and processes the accounts of local administrators on desktop, not server, operating systems. This is because users are typically members of the Local Administrators group only on desktops, and excluding local administrators from processing in server environments assists with troubleshooting. You should therefore only enable this policy if you want to modify the default behavior.
   The Excluded groups policy takes precedence over the Process logons of local administrators policy; if an account appears in both policies, it is not processed by Profile Management.

   If this setting is not configured here, the value from the .ini file is used. If this setting is not configured here or in the .ini file, the profiles of local administrators are not processed.

For your changes to take effect, run the gpupdate /force command from the command prompt as documented at http://technet.microsoft.com/en-us/library/bb490983.aspx.

To specify the path to the user store

Aug 14, 2017

Before specifying the path to the user store, refer to Profile management architecture and, if relevant to your deployment, understand the effect of:

- Storing multilingual profiles
- Combining inclusions and exclusions

1. Under Profile Management, double-click the Path to user store policy.
2. Select Enabled and enter the path to the directory (the user store) in which the user settings (registry changes and synchronized files) are saved.

The path can be:

- **A relative path**. This must be relative to the home directory, which is typically configured as the #homeDirectory# attribute for a user in Active Directory (AD).
- **A UNC path**. This typically specifies a server share or a DFS namespace.
- **Disabled or unconfigured**. In this case, a value of #homeDirectory#\Windows is assumed.

The following types of variables can be used for this setting:

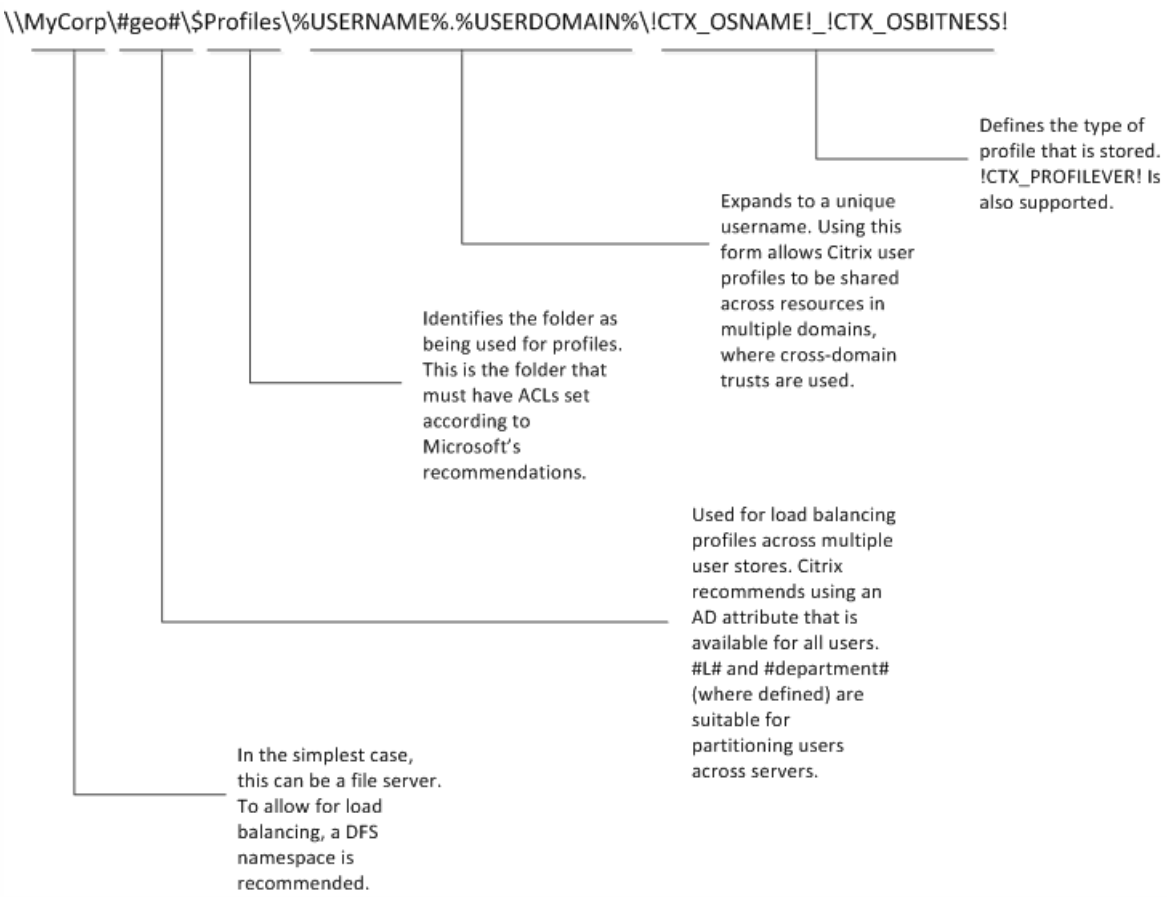
- System environment variables enclosed in percent signs (for example, %ProfVer%). Note that system environment variables generally require additional setup. For information on this, see Administer profiles within and across OUs.
- Attributes of the AD user object enclosed in hashes (for example, #sAMAccountName#).
- Profile management variables. For more information, see Profile management policies.

User environment variables cannot be used, except for %username% and %userdomain%. You can also create custom AD attributes to fully define organizational variables such as location or users. Attributes are case-sensitive.

Examples:

- \\server\share\#sAMAccountName# stores the user settings to the UNC path \\server\share\JohnSmith (if #sAMAccountName# resolves to JohnSmith for the current user)
- \\server\profiles$\%USERNAME%.%USERDOMAIN%\!CTX_OSNAME!!CTX_OSBITNESS! might expand to \\server\profiles$\JohnSmith.Finance\Win8x64

Important: Whichever attributes or variables you use, check that this setting expands to the folder one level higher than the folder containing NTUSER.DAT. For example, if this file is contained in \\server\profiles$\JohnSmith.Finance\Win8x64\UPM_Profile, set the path to the user store as \\server\profiles$\JohnSmith.Finance\Win8x64 (not the \UPM_Profile subfolder).
This diagram illustrates the components of a typical path to the user store that incorporates AD attributes, environment variables, and Profile management variables.



For more information on using variables when specifying the path to the user store, see the following topics:

- Share Citrix user profiles on multiple file servers
- Administer profiles within and across OUs
- High availability and disaster recovery with Profile management

If Path to user store is disabled, the user settings are saved in the Windows subdirectory of the home directory.

If this setting is not configured here, the setting from the .ini file is used. If this setting is not configured here or in the .ini file, the Windows directory on the home drive is used.

For your changes to take effect, run the gpupdate /force command from the command prompt as documented at http://technet.microsoft.com/en-us/library/bb490983.aspx.

To store certificates

Aug 14, 2017

Follow this procedure to save personal certificates that have been imported into the certificate store during a session. By default, certificates are automatically synchronized.

1. Add the path Application Data\Microsoft\SystemCertificates\My to the Directories to synchronize setting. The operating system language determines the Application Data folder in this location. If a policy is used to configure multi-language systems, add each language's location to the list.

On an English system, the path is Application Data\Microsoft\SystemCertificates\My. On a German system it is Anwendungsdaten\Microsoft\SystemCertificates\My.

For your changes to take effect, run the gpupdate /force command from the command prompt as documented at http://technet.microsoft.com/en-us/library/bb490983.aspx.

To stream user profiles

Aug 14, 2017

With the Citrix streamed user profiles feature, files and folders contained in a profile are fetched from the user store to the local computer only when they are accessed by users after they have logged on. Registry entries and any files in the pending area are exceptions. They are fetched immediately. For more information on the pending area, see Pending area. Streaming is not required and does not work with the personal vDisk feature of Citrix XenDesktop.

1. Under Profile Management, double-click Streamed user profiles.
2. Double-click Profile streaming.
3. Select Enabled and click OK.
4. Optionally, to enhance the streaming experience for users, double-click Always cache, select Enabled, and do one of the following:
   - To save network bandwidth by imposing a lower limit on the size of files or folders that are streamed, set a limit in megabytes. Any files and folders that exceed the limit are fetched as soon as possible after logon.
   - To turn on the cache entire profile feature, set the limit to zero. After logon, this fetches all files in the user store as a background system task, without any feedback to users.

   If large files are present, the Always cache policy can improve performance by reducing logon times.
5. Click OK.
6. Optionally, double-click Timeout for pending area lock files, select Enabled, and enter a timeout period (days) that frees up files so they are written back to the user store from the pending area in the event that the user store remains locked when a server becomes unresponsive. Use this setting to prevent bloat in the pending area and to ensure the user store always contains the most up-to-date files.
7. Click OK.
8. Optionally, if you want only a subset of user profiles in the OU to be streamed, double-click Streamed user profile groups, select Enabled, and enter a list of groups. Use Enter to separate multiple entries. The profiles of users in all other groups will not be streamed.
9. Click OK.

If Profile streaming is not configured in Policy or INI file, Profile Streaming is enabled.

If Always cache is not configured here, the value from the .ini file is used. If this setting is not configured here or in the .ini file, it is disabled.

If Timeout for pending area lock files is not configured here, the value from the .ini file is used. If this setting is not configured here or in the .ini file, the default value of one day is used.

If Streamed user profile groups is disabled, all user groups are processed. If this setting is not configured here, the value from the .ini file is used. If this setting is not configured here or in the .ini file, all users are processed.

For your changes to take effect, run the gpupdate /force command from the command prompt as documented at http://technet.microsoft.com/en-us/library/bb490983.aspx.

To enable profile streaming exclusion

When profile streaming exclusion is enabled, Profile Management does not stream folders in the exclusion list, and all the folder as are fetched immediately from the user store to the local computer when a user logs on.

To enable profile streaming exclusion, follow the steps below:

1. Under Profile Management, double-click Streamed user profiles.
2. Double-click the Profile Streaming Exclusion list - directories policy.
3. Select Enabled.
4. Click Show.
5. Add folders that you do not want Profile Management to stream. The folder names can be specified as absolute paths or as paths relative to the user profile (%USERPROFILE%). Use that variable to locate the profile but do not enter the variable itself in this policy. Omit initial backslashes from paths.

For example:

- Desktop. The Desktop folder is not processed in the user profile.
- MyApp\tmp. The %USERPROFILE%\MyApp\tmp folder is not processed.

If this setting is not configured here, the following folders in the .ini file are excluded by default:

- AppData\Local\Microsoft\Credentials
- Appdata\Roaming\Microsoft\Credentials
- Appdata\Roaming\Microsoft\Crypto
- Appdata\Roaming\Microsoft\Protect
- Appdata\Roaming\Microsoft\SystemCertificates

If this setting is not configured here or in the .ini file, all folders are streamed.

For your changes to take effect, run the gpupdate /force command. For more information, see http://technet.microsoft.com/en-us/library/bb490983.aspx.

Note:

- This policy only takes effect when Profile Streaming is enabled.
- The wildcard * and ? are not supported by this policy.
- Use Enter to separate multiple entries.
- When manually editing the profile streaming exclusion list, you must add the default excluded folders as shown above to avoid logons hanging.

To configure folder redirection

Aug 14, 2017

Folder redirection is a feature of Microsoft Windows and can be used in conjunction with Profile management.

Important: Configure folder redirection using only one of these methods: Microsoft Active Directory (AD) GPOs or Citrix policies. Using multiple methods to configure folder redirection may cause unpredictable results. Using Microsoft AD GPOs provides the most comprehensive configuration options, so it is recommended.

1. Move the required users to the OU that is managed by Profile management.
2. Create a GPO and open it for edit.
3. In User Configuration > Policies > Administrative Templates > Citrix > Profile Management > Folder Redirection, select the folder you want to redirect.
4. Enable the Redirect the <folder name> folder policy and provide the path to this shared folder. Do not add exclusions for redirected folders. Do not add usernames or folder names to this path. For example, if you set this path to the Desktop folder as \\server\share\, to the user this is redirected as \\server\share\<user name>\Desktop.
5. For your changes to take effect, run the gpupdate /force command from the command prompt as documented at http://technet.microsoft.com/en-us/library/bb490983.aspx.

All folders can be redirected, including:

- The Documents folder, which you can redirect to the user's home directory
- The Music, Pictures, and Videos folders, which you can redirect relative to the Documents folder

To manage cookie folders and other transactional folders

Aug 14, 2017

This topic applies to Profile Management 3.1 and later.

The two procedures, mirroring folders and deleting stale cookies, are related. If you manage the Internet Explorer Cookies folder, use both procedures. This ensures transactional integrity while also reducing profile bloat involving Index.dat and browser cookies.

Mirroring can also be applied more widely because it can help solve similar issues involving any transactional folder (also known as a referential folder), that is a folder containing interdependent files, where one file references others. Mirroring folders allows Profile Management to process a transactional folder and its contents as a single entity, thereby avoiding profile bloat.

For example, consider how Index.dat references cookies while a user browses the Internet. If a user has two Internet Explorer sessions, each on a different server, and they visit different sites in each session, cookies from each site are added to the appropriate server. When the user logs off from the first session (or in the middle of a session, if the active write back feature is configured), the cookies from the second session should replace those from the first session. However, instead they are merged, and the references to the cookies in Index.dat become out of date. Further browsing in new sessions results in repeated merging and a bloated cookie folder.

Mirroring the cookie folder solves the issue by overwriting the cookies with those from the last session each time the user logs off so Index.dat stays up to date.

The cookie folder can become bloated not only when multiple sessions are involved but also when Web sites are revisited and stale cookies build up. The second procedure in this topic solves the latter issue by removing the stale cookies from all profiles.

Settings required for Internet Explorer 10 and later versions for browser compatibility

CONFIGURE: The following folders need to be added under Mirroring:

- AppData\Local\Microsoft\Windows\INetCookies (Cookies location for Windows 8.1 platform)
- AppData\Roaming\Microsoft\Windows\Cookies (Cookies location for Windows 7 and Windows 8 platforms)
- AppData\Local\Microsoft\Windows\WebCache (Cookies database is maintained at Webcache01.dat)

Note:

- History: Browsing history from Version 5.1 of UPM or older profiles is not persisted.
- Cookies: Cookies created using Version 5.1 of UPM or older profiles are persisted.
- Stale cookies: In Version 5.1 & older of UPM, these cookies are not handled and remain as a part of the profile until deleted manually. In Version 5.2 of UPM, when using Internet Explorer 10 and later, these cookies are handled in Protected and Normal modes.

The cookies and browsing history information in versions of Internet Explorer 9 and earlier are not compatible with the cookies and browsing history information in Internet Explorer 10 and later. Users are advised to not move across multiple systems that have different versions of Internet Explorer installed. [#474200]

Use this procedure for any transactional folders not just those that store cookies.

Caution: Mirroring transactional folders can mean that the "last write wins"; files that are modified in more than one session are overwritten by the last update. This might result in the loss of users' profile changes.

1. Under Profile Management > File system > Synchronization, double-click the Folders to mirror policy.
2. Select Enabled.
3. Add the list of folders, relative to the root folder in the user store, that you want to mirror. Use Enter to separate multiple entries. This policy works recursively, so do not add subfolders to the list. For example, add AppData\Roaming\Microsoft\Windows\Cookies but not AppData\Roaming\Microsoft\Windows\Cookies\Low as well.

If Folders to mirror is not configured here, the value from the .ini file is used. If this setting is not configured here or in the .ini file, no folders are mirrored.

For your changes to take effect, run the gpupdate /force command from the command prompt as documented at http://technet.microsoft.com/en-us/library/bb490983.aspx.

If you are using Internet Explorer 10 or later, this procedure is not required.

1. Under Profile Management > Advanced Settings, double-click the Process Internet cookie files on logoff policy.
2. Select Enabled.
3. Click OK.

If Process Internet cookie files on logoff is not configured here, the value from the .ini file is used. If this setting is not configured here or in the .ini file, no processing of Index.dat takes place.
For your changes to take effect, run the gpupdate /force command from the command prompt as documented at http://technet.microsoft.com/en-us/library/bb490983.aspx.

Be aware that enabling Process Internet cookie files on logoff increases logoff times. Nevertheless, in order to maintain the integrity of the cookie folder, the supported configuration is to set both Folders to mirror and Process Internet cookie files on logoff, as the following best practice demonstrates:

1. Under Profile Management > File system > Synchronization, double-click the Folders to mirror policy.
2. Select Enabled.
3. Add the list of folders, relative to the root folder in the user store, that you want to mirror. Add the folder Cookies for Version 1 profiles and AppData\Roaming\Microsoft\Windows\Cookies for Version 2 profiles.
4. Under Profile Management > Advanced Settings, double-click the Process Internet cookie files on logoff policy. This step deletes the stale cookies referenced by Index.dat.
5. Select Enabled.
6. Click OK.

For your changes to take effect, run the gpupdate /force command from the command prompt as documented at http://technet.microsoft.com/en-us/library/bb490983.aspx.

To configure offline profiles

Aug 14, 2017

Citrix offline profiles are intended for laptop users or mobile-device users who roam with intermittent access to a network. This feature allows profiles to synchronize with the user store at the earliest possible opportunity. When a network disconnection occurs, profiles remain intact on the laptop or device even after restarting or hibernating. As mobile users work, their profiles are updated locally and are eventually synchronized with the user store when the network connection is re-established.

This feature works only with domain-joined computers (including ones running Citrix XenClient) and is not intended for use with servers or desktop computers, whose network connections tend to be permanent.

Typically, you don't enable both offline profiles and streamed user profiles. For this reason, offline profiles takes precedence over and disables streamed user profiles and the Delete locally cached profiles on logoff setting. This ensures users always have a complete profile on their laptop or mobile device when they first log on.

You can configure offline profiles in these ways:

- **Using Group Policy**. This gives you centralized administrative control of the feature but you must create a separate OU containing the laptops or devices that will use offline profiles.
- **Using the .ini file**. This is an easier option if you prefer not to create a special OU just for laptops and mobile devices, but it effectively hands control of this feature to individual device owners. This option requires a once-only configuration of each laptop or mobile device.

If Offline profile support is not configured using Group Policy, the value from the .ini file is used. If this setting is not configured in Group Policy or in the .ini file, offline profiles are disabled.

1. Create an OU containing all computers managed by Profile management, including the laptops and mobile devices that will be using offline profiles, your XenApp servers, and your virtual desktops.
2. Create a child OU containing only the laptops and mobile devices.
3. In Group Policy Management, create a baseline Group Policy Object (GPO) that enforces your site-wide policies, and link it to both OUs.
4. Configure the baseline GPO with the Profile management settings common to all computers.
5. Create a second, offline GPO and link it to the child OU.
6. Configure the offline GPO as follows:
    1. Under Profile Management, double-click Offline profile support.
    2. Select Enabled and click OK.
    3. Configure any other settings that you want to apply only to laptops and mobile devices.

For your changes to take effect, run the gpupdate /force command from the command prompt as documented at http://technet.microsoft.com/en-us/library/bb490983.aspx.

As a prerequisite, ensure that Offline profile support is unconfigured (the default) in both the baseline and offline GPO. If these settings are configured, the .ini file setting is overridden.

1. On each laptop or mobile device, locate the .ini file that was created by the Profile management installer. To locate the .ini file, see Files included in the download.
2. Uncomment this line (by removing the semi-colon from it):
   ;OfflineSupport=
3. Save the .ini file.
   For your changes to take effect, run the gpupdate /force command from the command prompt as documented at http://technet.microsoft.com/en-us/library/bb490983.aspx.

To configure the Customer Experience Improvement Program (CEIP)

Aug 14, 2017

To configure the Customer Experience Improvement Program (CEIP), follow these steps:

1. Open the Group Policy Management Editor.
2. Under **Policies** > **Administrative Templates: Policy definitions (ADM)** > **Classic Administrative Templates (ADM)** > **Citrix** > **Profile Management** > **Advanced settings**, double-click **Customer Experience Improvement Program**.
3. Select **Enabled** or **Disabled**, then click **OK**.
4. For your changes to take effect, run the **gpupdate /force** command from the command prompt as documented at Gpupdate.

Note: If **Customer Experience Improvement Program** is not configured in Group Policy objects and HDX, the value from the .ini file is used. If this setting is not configured anywhere, it is enabled by default.

For more information about CEIP, see About the Citrix Customer Experience Improvement Program (CEIP).

To configure active write back

Aug 14, 2017

To ensure profile integrity, files and folders that are modified on the local computer can be backed up to the user store during a session, before logoff.

Note that if a user starts a second session (started at a second computer, for example) modifications made to a file in the first session will be available in the second if it was started before logging off the first.

1. Under Profile Management, double-click Active write back.
2. Select Enabled and click OK.

If Active write back is not configured in Group Policy objects and HDX, the value from the .ini file is used. If this setting is not configured anywhere, it will be configured by Profile management dynamically. For more information, see Advanced troubleshooting checklist.

For your changes to take effect, run the gpupdate /force command from the command prompt as documented at http://technet.microsoft.com/en-us/library/bb490983.aspx.

> ## Note
>
> Active write back for registry entries is disabled by default. You can enable this feature under **Profile Management** > **Active write back Registry** when active write back has been enabled. If it is not configured in Group Policy objects and HDX, the value from the .ini file is used.

To configure cross-platform settings

Aug 14, 2017

Important: Note the following important information for this feature:

- Cross-platform settings in Profile management work with a set of supported operating systems (OSs) and applications. Only configure this feature in a production environment if your organization uses one or more of these.
- Microsoft Office settings do not roam between versions of that application. For more information, see Operating systems and applications supported By cross-platform settings.
- This feature is suitable for registry and application settings, but not for files or folders, or objects typically used with folder redirection (for example, browser favorites, and desktop and Start menu settings).
- If you use this feature to migrate user profiles between systems with different profile versions, disable it after the migration has been completed for all users. There is some performance impact, primarily to logoffs, when using this feature so it is best to leave it disabled unless you support roaming between profile versions.

This topic contains an example of the steps you can take to configure cross-platform settings. For a more detailed case study, see Cross-platform settings - Case study.

Tip: Citrix recommends restricting this feature to a small, test set of users before putting it into production. Use the Cross-platform settings user groups option to achieve this. If this setting is configured, the cross-platform settings feature of Profile management processes only members of these user groups. If this setting is disabled, the feature processes all of the users specified by the Processed groups setting. If Cross-platform settings user groups is not configured in Group Policy or the .ini file, all user groups are processed.

1. For the settings that are common to all platforms, create a common Group Policy Object (common GPO), link it to the Profile management .adm or .admx file, and configure the settings as required. This is best practice because it minimizes duplicate settings that can make any later troubleshooting awkward. Depending on your requirements, all Profile management settings work on multiple platforms except Path to user store, which you must configure separately for each platform due to the different user store structures of Version 1 and Version 2 profiles. In the common GPO, leave this setting unconfigured.
2. Create separate OUs for your different platforms (for example, if you are migrating from Windows 7 to Windows 8, create separate OUs for these operating systems), and set Path to user store appropriately in each OU.
3. Locate the definition (.xml) files for the supported applications whose personalizations you want to work across the platforms. These files are located in the CrossPlatform folder in the download package.
4. Copy the .xml files to a suitable location on your network.
5. Edit the common GPO in Group Policy Management Editor. Under Profile Management open the Cross-platform settings folder and configure these settings:
   - Cross-platform settings user groups. Restricts the users who experience cross-platform settings. This setting is optional. It is useful when testing this feature or rolling it out in stages.
   - Path to cross-platform definitions. Identifies the network location of the definition files that you copied from the download package. This must be a UNC path. Users must have read access to this location, and administrators must have write access to it. The location must be a Server Message Block (SMB) or Common Internet File System (CIFS) file share.
   - Path to cross-platform settings store. This is the common area of the user store where profile data shared by multiple platforms is located. Users must have write access to this area. The path can be an absolute UNC path or a path relative to the home directory. You can use the same variables as for Path to user store.
6. Specify a base platform by ensuring Source for creating cross-platform settings is set to Enabled in that platform's OU. This setting migrates data from the base platform's profiles to the cross-platform settings store. In the other platforms'

OUs, set this policy to Disabled or Unconfigured. Each platform's own set of profiles are stored in a separate OU. This means you must decide which platform's profile data to use to seed the cross-platform settings store. This is referred to as the base platform. If the cross-platform settings store contains a definition file with no data, or the cached data in a single-platform profile is newer than the definition's data in the store, Profile management migrates the data from the single-platform profile to the store unless you disable this setting.
Important: If Source for creating cross-platform settings is enabled in multiple OUs, the platform that the first user logs on to becomes the base profile.

7. Set Enable cross-platform settings to Enabled. By default, to facilitate deployment, cross-platform settings is disabled until you turn on this setting.
8. Run a Group Policy update.
9. If you are migrating profiles across platforms but not supporting roaming of them, when the migration is complete, set Enable cross-platform settings to Disabled .

If Path to cross-platform definitions is not configured here, the value from the .ini file is used. If this setting is not configured here or in the .ini file, no cross-platform settings are applied.

If Path to cross-platform settings store is disabled, the default path Windows\PM_CP is used. If this setting is not configured here, the value from the .ini file is used. If this setting is not configured here or in the .ini file, the default path is used.

If Enable cross-platform settings is not configured here, the value from the .ini file is used. If this setting is not configured here or in the .ini file, no cross-platform settings are applied.

This example describes the major steps involved in allowing users' application settings to roam between two operating systems that create Version 2 profiles. Microsoft Office 2010 is the example application, and roaming takes places between Citrix XenApp 6.5 on Windows Server 2008 and Windows 7. Both OSs are 64-bit.

1. Users are accustomed to accessing Office 2010 and Internet Explorer 9 as published applications on XenApp servers, and change several settings in these applications (for example, they modify their email signature in Office and choose a new home page in Internet Explorer).
2. At a future date, virtual desktops (created with Citrix XenDesktop) are created but not yet released to users. The desktops run Windows 7 and are preconfigured with Office 2010 and Internet Explorer 9.
3. The users will expect their settings to be the same on their new desktops. To achieve this, you configure the cross-platform settings feature according to the procedure in this topic. This includes enabling Source for creating cross-platform settings in the OU for Windows Server 2008.
4. When users next run the published versions of the applications (not the new, virtual desktops), their settings are copied to the cross-platform settings store.
5. The new desktops are then released to users. When they log on and run the local versions of Office and Internet Explorer, the settings from the earlier Windows Server 2008 sessions are used; users' modified email signatures and home pages are available on their Windows 7 machines.
6. Users browse in Internet Explorer from their virtual desktop, and decide to change their home page again.
7. Users log off and leave work. They don't have access to their virtual desktop at home, but they can run the published version of Internet Explorer 9 remotely. They find their most recent home page, created on Windows 7 in the previous step, has been preserved.

Operating systems and applications supported by cross-platform settings

Aug 14, 2017

This topic describes the applications and operating systems (OSs) supported by the cross-platform settings feature in this release of Profile management.

Definition files contain common personalizations for selected Windows applications. Each file and the definitions within it allow users to connect to the same application on multiple OSs, presenting essentially identical profiles on each platform. For example, users might access two instances of Microsoft Office: one that is installed on a Windows 7 virtual desktop and the other that is published with Citrix XenApp on Windows Server 2003; whichever instance is accessed, users' experience of Office is consistent.

Preconfigured definition files are a key aspect of the cross-platform settings feature. There is a definition file for each supported application. Definition files are in an XML format.

Important: Without a thorough analysis of an application's behavior across all OSs and a full understanding of this feature's operation, editing of definition files can result in unexpected changes to users' profiles that can be difficult to troubleshoot. For this reason, Citrix does not support the editing of the supplied definition files or the creation of new ones. In addition, note that some application settings cannot be duplicated across OSs due to the nature of Windows user profiles.
In addition note that, although this feature is suitable for registry and application settings, it is not suitable for files or folders, or objects typically used with folder redirection (for example, browser favorites, and desktop and Start menu settings).

You can roam profiles between any of the supported client OSs, and between any of the supported server OSs.

The following are supported (x86 and x64 versions as applicable):

- **Client OSs**. Windows XP, Windows 7, and Windows Vista.
- **Server OSs**. Windows Server 2003, Windows Server 2008, and Windows Server 2008 R2.

The following Citrix products are supported by the cross-platform settings feature:

- XenApp 5 Feature Pack for Windows Server 2003 or later
- XenDesktop 4 or later

The following definition files are available in this release. The XML file name indicates the supported application and versions.

- **Internet Explorer 7 Plus.xml**. This file supports the roaming of Versions 7, 8, and 9 of Internet Explorer (except favorites) across platforms. The roaming of favorites and feeds is not supported.

- Office 2007.xml.
- Office 2010.xml.
- Wallpaper.xml. This file supports the roaming of desktop wallpaper across platforms. The roaming of themes across platforms is not supported.

Important: Use the definition files for each application only in the above supported scenarios. For example, Internet Explorer 7 Plus.xml roams settings between multiple versions of that browser, but you cannot use Office 2007.xml or Office 2010.xml to roam settings between versions of Office.

Cross-platform settings - Case study

Aug 14, 2017

The primary use case for the cross-platform settings feature is the migration from Windows 7 and Windows Server 2008 to Windows 8 and Windows Server 2012. It is likely that this is accompanied by a move from Microsoft Office 2003 or Office 2007 to Office 2010. Given the typical investment in Windows 2003 systems, a significant coexistence phase is expected, so the feature is expected to support both migration and sustained coexistence.

This case study starts with an existing Windows 7 and Windows 2008 environment running Office 2007 and adds Windows 8 shared, provisioned virtual desktops.

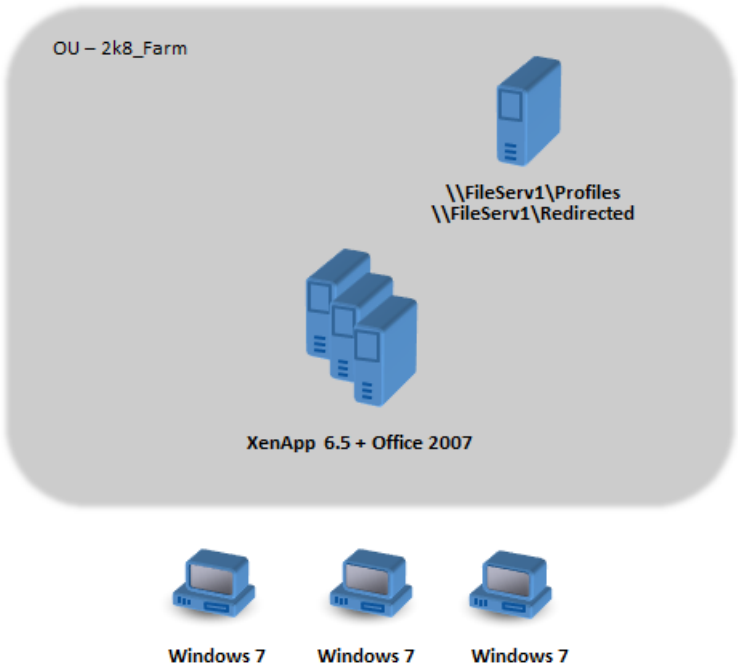
The case study consists of:

- Initial configuration
- Plan the new site
- Execute the plan
- Other considerations

Initial configuration

Aug 14, 2017

The following graphic illustrates the environment configuration in this case study.



Windows 7 machines are configured to use Office 2007 published on Citrix XenApp 6.5.

The domain includes Windows 2008 domain controllers running Active Directory at Windows 2008 level. All of the machines belong to an OU called 2k8_Farm and the Profile management 5.0 .adm file is added to a GPO called 2k8_Farm_PO. The following policies are configured.

Policy	Value
Path to user store	\\FileServ1\Profiles\#sAMAccountName#\%ProfVer%
Profile streaming	Enabled
Active write back	Enabled

A machine logon script, which sets the system environment variable %ProfVer%, runs on all of the machines in the OU.

Machine Type	%ProfVer%
XenApp server on Windows 2008	Win2008
Windows 7 desktops	Win7

So, for example, user john.smith has his profile at \\FileServ1\Profiles\john.smith\Win7 for the Windows 7 desktop and at

\\FileServ1\Profiles\john.smith\Win2008 for the XenApp servers. Note that separate profiles are maintained for desktops and servers. The administrator is aware that issues exist when profiles roam between workstation and server operating systems and is being cautious.

Folder redirection is set up using Group Policy in User Configuration > Policies > Windows Settings > Folder Redirection.

Plan the new site

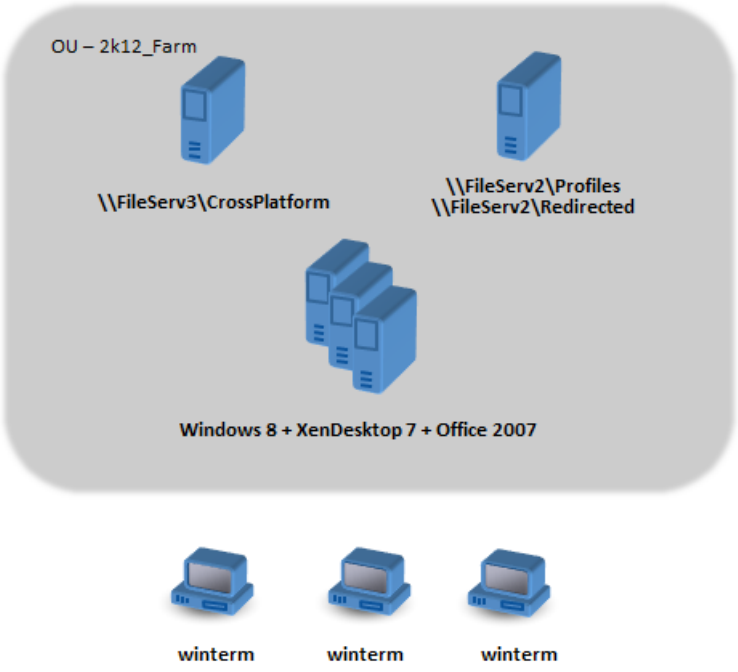
Aug 14, 2017

The network administrators have decided to set up a new domain for the new environment, based on Windows Server 2012 domain controllers and Active Directory 2012. Ultimately, a new XenApp farm is planned, based on Windows Server 2012 running XenApp, but for now, the new domain is used only for the Windows 7 XenDesktop site.

The site is based on a shared Windows 7 base image hosted in a XenServer environment and accessed by Windows terminals. Office 2007 is included in the base image.

Because users from both domains are expected to make use of the new domain, a two-way trust is set up between OldDomain and NewDomain, both of which must belong to the same AD forest.

The following graphic illustrates the configuration of the new XenDesktop site.



Execute the plan

Aug 14, 2017

You set up file servers in NewDomain for managing cross-platform settings (\\FileServ3) and for storing profiles for 2k12_Farm (\\FileServ2).

In this case, we choose to set up separate file servers for the profiles and for the cross-platform settings. This is not strictly necessary, but it is an easy way of making the cross-platform settings server available; the profile server might be designed differently, using DFS namespaces for example, and so take longer to implement.

In both cases, the server shares should be set up according to the security recommendations for roaming user profiles on shared folders. For information on this, see http://technet.microsoft.com/en-us/library/cc757013(WS.10).aspx.

For instructions on this, see Upgrade Profile management.

A number of configuration files (called definition files) are supplied for Microsoft Office, Internet Explorer and Windows wallpaper.

Important: Do not update these files unless instructed to by Citrix personnel.
Choose the configuration files that are relevant to your deployment, and copy only these files to \\FileServ3\CrossPlatform\Definitions. In this example, copy just Office 2007.xml.

Once the upgrade is complete, make the following configuration changes to (partially) enable the cross-platform settings feature. Note that, at this stage, only \\FileServ3\CrossPlatform needs to be available.

Policy	Value	Notes
Path to user store	\\FileServ1\Profiles\#sAMAccountName#\%ProfVer%	No change. This path is only used by OldDomain users, so there is no need to change it to support NewDomain users.
Enable cross-platform settings	Enabled	
Cross-platform settings user groups	Disabled	All user groups are processed.
Path to cross-platform definitions	\\FileServ3\CrossPlatform\Definitions	This is where the definition files are located.

Policy	Value	Notes
Path to cross-platform settings store	\\FileServ3\CrossPlatform\Store\%USERNAME%.%USERDOMAIN%	The cross-platform settings store is shared by users of both domains, so both %USERNAME% and %USERDOMAIN% must be specified in the path.
Source for creating cross-platform settings	Enabled	This ensures that cross-platform settings from OldDomain are used to initialize the cross-platform settings store, before giving users access to NewDomain resources.

No changes are required to the machine logon script.

No changes are required to the folder redirection policy.

The OU 2k8_Farm can now be left to run. As users log on, Profile management copies the settings identified in the definition file Office 2007.xml to the cross-platform settings store.

Now that the file servers are set up in 2k8_Farm, it is time to build the XenDesktop site. Install Profile management 5.0 when the Windows 7 XenDesktop virtual desktops are running. Here is a suitable configuration.

Policy	Value	Notes
Path to user store	\\FileServ2\Profiles\%USERNAME%.%USERDOMAIN%\%ProfVer%	As this file share is used by users from both domains, it is important also to include domain information.
Active write back	Disabled	
Enable cross-platform settings	Enabled	
Cross-platform settings user groups	Disabled	All user groups are processed.
Path to cross-platform definitions	\\FileServ3\CrossPlatform\Definitions	This is where the definition files are located. This setting must match the setting in 2k8_Farm.
Path to cross-platform	\\FileServ3\CrossPlatform\Store\%USERNAME%.%USERDOMAIN%	The cross-platform settings store is shared by users of both

Policy	Value	Notes
settings store		domains, so both %USERNAME% and %USERDOMAIN% must be specified in the path. This setting must match the setting in 2k8_Farm.
Source for creating cross-platform settings	Disabled	This prevents settings from NewDomain being used for the initial setup of the profile data in the cross-platform settings store. It ensures that settings from OldDomain take precedence.

A machine logon script, which sets the system environment variable %ProfVer%, runs on all machines in the OU.

Machine Type	%ProfVer%	Notes
XenApp server on Windows 2012	Win2012x64	This is not needed yet, but it will be when your planned 64-bit servers become available. See Other considerations for more information.
Windows 7 desktops	Win7	If both 32- and 64-bit versions of Windows 7 are deployed, it is recommended that they have separate profiles, so %ProfVer% should be configured differently on each platform.

So the OldDomain user john.smith has his profile at \\FileServ2\Profiles\ john.smith.OldDomain\Win7 for the Windows 7 desktop and at \\FileServ2\Profiles\ john.smith.OldDomain\Win2012x64 for the XenApp servers.

And a NewDomain user william.brown has his profile at \\FileServ2\Profiles\ william.brown.NewDomain\Win7 for the Windows 7 desktop and at \\FileServ2\Profiles\william.brown.NewDomain\Win2012x64 for the XenApp servers.

Again, you set up folder redirection using Group Policy. Because the domain is based on Windows Server 2012, set folder redirection from<Group Policy Object Name> > User Configuration > Policies > Windows Settings > Folder Redirection.

Policy	Value
Favorites	\\FileServ2\Redirected\%USERNAME%.%USERDOMAIN%\Favorites
My Documents	\\FileServ2\Redirected\%USERNAME%.%USERDOMAIN%\Documents

Note that %USERDOMAIN% has been added to the folder redirection path. This is not necessary because this policy only applies to NewDomain users, but it may be useful if in the future, you decide to migrate OldDomain users to the same server. For now, OldDomain users continue to use the Folder Redirection policy from OldDomain which redirects their folders to \\FileServ1.

You perform testing in two stages:

1. You test that the profile data for users from NewDomain operates correctly. These users have no data set up in the cross-platform settings store. As the policy Source for creating cross-platform settings is set to disabled, their profile changes do not propagate to OldDomain.
2. You test with a small number of users from OldDomain. When they first log on, the cross-platform settings data is copied to their profile. For later logons, changes from either domain are copied to the other. Note that if a user from OldDomain logs on to NewDomain and no profile data is present (because the user has not used their profile in OldDomain since OldDomain was upgraded to Profile management 5.0), the cross-platform settings store is not updated. With the configuration described in this topic, a user must log on to OldDomain before their settings roam between the domains. This ensures that user settings (possibly created over many years) are not overwritten by default settings from NewDomain.

Other considerations

Aug 14, 2017

As configured in this case study, Profile management does not use the settings from NewDomain to initialize the cross-platform settings store. Only settings from OldDomain can be used to initialize the store. This is acceptable until NewDomain contains more than one type of profile (such as Windows 7 32-bit and Windows 7 64-bit). Alternatively, users from NewDomain may need to access resources in OldDomain. In these cases, you must enable the policy Source for creating cross-platform settings on further types of machine appropriately.

Caution: If Source for creating cross-platform settings is set incorrectly, it is entirely possible that a new profile will obliterate an existing profile with many accumulated and treasured settings. To avoid this, Citrix recommends that this policy is set on only one platform type at a time. This is generally the older (more mature) platform, where settings that users most likely want to keep have accumulated.

In this case study, separate domains are used to illustrate a number of points. Additionally, the cross-platform settings feature can manage the roaming of settings between two OUs, or even between machines of different types in a single OU. In this case, you might have to set the policy Source for creating cross-platform settings differently for the different machine types. This can be achieved in a number of ways:

- Use the setting CPMigrationsFromBaseProfileToCPStore in the .ini file to set the policy differently on each machine type. Do not set the policy Source for creating cross-platform settings.
- Use Windows Management Instrumentation (WMI) filtering to manage different GPOs on the same OU. You can configure the common settings in a GPO that applies to all machines in the OU, but only add the policy Source for creating cross-platform settings to additional GPOs and filter using a WMI query.

To force user logoffs

Aug 14, 2017

By default, users are given a temporary profile if a problem is encountered (for example, the user store is unavailable). However, you can instead configure Profile management to display an error message and then log users off. This can help with troubleshooting.

1. Under Profile Management, open the Advanced settings folder.
2. Double-click the Log off user if a problem is encountered policy.
3. Select Enabled.

Policies

Aug 14, 2017

This topic provides:

Profile Management policies - describing some important aspects of the policies in the .adm and .admx files, and the templates used to configure Profile Management.

Profile Management policy descriptions and defaults - providing reference information on each policy, including policy default settings.

Profile Management policies

Aug 14, 2017

This topic describes some important aspects of the policies in the .adm and .admx files, the templates used to configure Profile Management.

For reference information on each policy, including its default setting, see Profile Management policy descriptions and defaults. For instructions on setting a policy, see Manage.

To deactivate any Profile Management policy that you enter as lists (for example, exclusion lists and inclusion lists), set the policy to Disabled. Do not set the policy to Not Configured.

For your changes to take effect, run the gpupdate /force command from the command prompt as documented at http://technet.microsoft.com/en-us/library/bb490983.aspx.

In this version of Profile Management, the following variables are available for use in both Group Policy and the .ini file.

For policies that define files and registry entries, the following variables expand as follows.

Variable	Expansion for Version 1 profiles	Expansion for Version 2 profiles
!ctx_localsettings!	Local Settings\Application Data	AppData\Local
!ctx_roamingappdata!	Application Data	AppData\Roaming
!ctx_startmenu!	Start Menu	AppData\Roaming\Microsoft\Windows\Start Menu
!ctx_internetcache!	Local Settings\Temporary Internet Files	AppData\Local\Microsoft\Windows\Temporary Internet Files
!ctx_localappdata!	Local Settings\Application Data	AppData\Local

For policies that are used to build paths, the following variables expand as follows.

Variable	Expansion for Version 1 profiles	Expansion for Version 2 profiles
!ctx_profilever!	v1	v2
!ctx_osbitness!	x86	x64

Additionally for policies that are used to build paths, !ctx_osname! expands to the short name as follows depending on the

operating system. The long name is written to the log files when the Profile Management Service starts.

Long Name	Short Name
Windows 10 Redstone 1	Win10RS1
Windows 10	Win10
Windows 8.1	Win8.1
Windows 8	Win8
Windows 7	Win7
Windows Server 2016	Win2016
Windows Server 2012 R2	Win2012R2
Windows Server 2012	Win2012
Windows Server 2008 R2	Win2008
Windows Server 2008	Win2008

As an aid to migration, the following tables show the policies that are available in different versions of Profile Management, the location of each policy in the .adm (or .admx) file and the .ini file, and the feature each policy is designed for (or whether it is part of the base configuration of all deployments). The location in the .adm or .admx file is relative to the folder Citrix > Profile Management. Where no location in the .ini file is shown, the policy is not included there.

As a further aid, the tables also relate policies to the configuration decisions that you make when planning your Profile Management deployment. For more information on these, see Decide on a configuration. Where no decision is shown, do not set the policy unless asked to by Citrix Technical Support.

To simplify upgrades, in Profile Management 5.x all policies in the .adm or .admx file are set to Not Configured by default.

Policies available from Version 5.5

Policy in .adm or .admx file	Location in .adm or .admx file	Location in .ini file	Feature

Default Exclusion list	\Registry	DefaultExclusionListRegistry	
NTUSER.DAT	\Registry	LastKnownGoodRegistry	
Default Exclusion list - directories	\File system	DefaultSyncExclusionListDir	

Policy in .adm or .admx file	Configuration decision
Default Exclusion list	
Default Exclusion list - directories	
NTUSER.DAT	

Policies available from Version 5.0 to 5.4

Policy in .adm or .admx file	Location in .adm or .admx file	Location in .ini file	Feature
Excluded groups		ExcludedGroups	Excluded Groups
Disable automatic configuration	\Advanced Settings	DisableDynamicConfig	Automatic Configuration
Redirect the AppData(Roaming) folder, Redirect the Desktop folder, ...	\Folder Redirection (in User Configuration)		Integration with XenDesktop
Delay before deleting cached profiles	\Profile handling	ProfileDeleteDelay	Base

Policy in .adm or .admx file	Configuration decision
Excluded groups	
Disable automatic configuration	
Redirect the AppData(Roaming) folder, Redirect the Desktop folder, ...	
Delay before deleting cached profiles	

Policy in .adm or .admx file	Configuration decision

Folder redirection policies are absent from the .ini file for the following reason. Policies in this file apply to computers and can only be filtered for users in basic ways, for example using the ProcessedGroups policy. In contrast, policies in the .adm or .admx file can be filtered in more complex ways that are ideally suited to, and normally required by, folder redirection.

Policies available from Version 4.x

Policy in .adm or .admx file	Location in .adm or .admx file	Location in .ini file	Feature
Cross-platform settings user groups	\Cross-platform settings	CPUserGroupList	Cross-platform settings
Enable cross-platform settings		CPEnabled	
Source for creating cross-platform settings		CPMigrationFromBaseProfileToCPStore	
Path to cross-platform definitions		CPSchemaPath	
Path to cross-platform settings store		CPPath	
Offline profile support		OfflineSupport	Offline profiles
Log off user if a problem is encountered	\Advanced Settings	LogoffRatherThanTempProfile	Improved Troubleshooting

Policy in .adm or .admx file	Configuration decision
Cross-platform settings user groups	
Enable cross-platform settings	
Source for creating cross-platform settings	
Path to cross-platform definitions	
Path to cross-platform settings store	
Offline profile support	Mobile? Static?
Log off user if a problem is encountered	

Policy in .adm or .admx file	Configuration decision

Policies available from Version 3.x

Policy in .adm or .admx file	Location in .adm or .admx file	Location in .ini file	Feature
Active write back		PSMidSessionWriteBack	Active profile write back (in Version 4.0, renamed Active write back)
Folders to mirror (available from Version 3.1)	\File system\Synchronization	MirrorFoldersList	Folder mirroring
Process Internet cookie files on logoff (available from Version 3.1)	\Advanced settings	ProcessCookieFiles	
Delete Redirected Folders (available in Versions 3.2, 3.2.2, and 4.0)		DeleteRedirectedFolders	Support for folder redirection
Always cache	\Streamed user profiles	PSAlwaysCache	Streamed user profiles
Profile streaming		PSEnabled	
Timeout for pending area lock files		PSPendingLockTimeout	
Streamed user profile groups		PSUserGroupsList	

Policy in .adm or .admx file	Configuration decision
Active write back	Persistent? Provisioned? Dedicated? Shared?
Folders to mirror (available from Version 3.1)	Which applications?
Process Internet cookie files on logoff (available from Version 3.1)	
Delete Redirected Folders (available in Versions 3.2, 3.2.2, and 4.0)	Mobile? Static?
Always cache	
Profile streaming	
Timeout for pending area lock files	

Policy in .adm or .admx file	Configuration decision
Streamed user profile groups	

Policies available from Version 2.x

Policy in .adm or .admx file	Location in .adm or .admx file	Location in .ini file	Feature
Path to user store		PathToUserStore	Base
Processed groups		ProcessedGroups	
Local profile conflict handling	\Profile handling	LocalProfileConflictHandling	
Migration of existing profiles		MigrateWindowsProfilesToUserStore	
Template profile		TemplateProfilePath, TemplateProfileOverridesRoamingProfile, TemplateProfileOverridesLocalProfile,	
Delete locally cached profiles on logoff		DeleteCachedProfilesOnLogoff	
Directory of the MFT cache file (removed in Version 5.0)	\Advanced settings	USNDBPath	
Directories to synchronize	\File system\Synchronization	SyncDirList	
Exclusion list	\Registry	ExclusionListRegistry	
Files to synchronize	\File system\Synchronization	SyncFileList	
Inclusion list	\Registry	InclusionListRegistry	
Exclusion list - directories	\File system	SyncExclusionListDir	
Exclusion list - files		SyncExclusionListFiles	
Number of retries when accessing locked files	\Advanced settings	LoadRetries	

Policy in .adm or .admx file	Location in .adm or .admx file	Location in .ini file	Feature
Process logons of local administrators		ProcessAdmins	
Enable Profile management		ServiceActive	
Enable logging	\Log settings	LoggingEnabled	Logging
Log settings		LogLevel...	
Maximum size of the log file		MaxLogSize	
Path to log file(available from Version 2.1)		PathToLogFile	

Policy in .adm or .admx file	Configuration decision
Path to user store	Pilot? Production?
Processed groups	
Local profile conflict handling	Migrate Profiles? New Profiles?
Migration of existing profiles	
Template profile	
Delete locally cached profiles on logoff	Persistent? Provisioned? Dedicated? Shared?
Directory of the MFT cache file (removed in Version 5.0)	
Directories to synchronize	Which applications?
Exclusion list	
Files to synchronize	
Inclusion list	
Exclusion list - directories	

Policy in .adm or .admx file	Configuration decision
Exclusion list - files	
Number of retries when accessing locked files	
Process logons of local administrators	
Enable Profile management	
Enable logging	
Log settings	
Maximum size of the log file	
Path to log file(available from Version 2.1)	

Profile Management policy descriptions and defaults

Aug 14, 2017

This topic describes the policies in the Profile Management .adm and .admx files, and the structure of the files. In addition, it lists the default setting of each policy.

Other information, such as the names of the equivalent .ini file settings and which version of Profile Management is required for any particular policy, is available in Profile Management policies.

In the Group Policy Object Editor, most of the policies appear under Computer Configuration > Administrative Templates > Classic Administrative Templates > Citrix. Redirected folder policies appear under User Configuration > Administrative Templates > Classic Administrative Templates > Citrix.

All Profile Management policies are contained in the following sections, located in the Citrix folder. The policies are located under Computer Configuration in Group Policy Editor unless a section is labeled User Configuration:

Profile Management

Profile Management\Folder Redirection (User Configuration)

Profile Management\Profile handling

Profile Management\Advanced settings

Profile Management\Log settings

Profile Management\Registry

Profile Management\File system

Profile Management\File system\Synchronization

Profile Management\Streamed user profiles

Profile Management\Cross-platform settings

Enable Profile Management
By default, to facilitate deployment, Profile Management does not process logons or logoffs. Enable Profile Management only after carrying out all other setup tasks and testing how Citrix user profiles perform in your environment. If this policy is not configured here, the value from the .ini file is used. If this policy is not configured here or in the .ini file, Profile Management does not process Windows user profiles in any way.
Processed groups

Both computer local groups and domain groups (local, global and universal) can be used. Domain groups should be specified in the format: <DOMAIN NAME>\<GROUP NAME>.

If this policy is configured here, Profile Management processes only members of these user groups. If this policy is disabled, Profile Management processes all users. If this policy is not configured here, the value from the .ini file is used. If this policy is not configured here or in the .ini file, members of all user groups are processed.

Excluded groups

You can use computer local groups and domain groups (local, global, and universal) to prevent particular user profiles from being processed. Specify domain groups in the form <DOMAIN NAME>\<GROUP NAME>.

If this setting is configured here, Profile Management excludes members of these user groups. If this setting is disabled, Profile Management does not exclude any users. If this setting is not configured here, the value from the .ini file is used. If this setting is not configured here or in the .ini file, no members of any groups are excluded.

Process logons of local administrators

Specifies whether logons of members of the BUILTIN\Administrators group are processed. If this policy is disabled or not configured on server operating systems (such as XenApp environments), Profile Management assumes that logons by domain users, but not local administrators, must be processed. On desktop operating systems (such as XenDesktop environments), local administrator logons are processed. This policy allows domain users with local administrator rights, typically XenDesktop users with assigned virtual desktops, to bypass any processing, log on, and troubleshoot the desktop experiencing problems with Profile Management.

Note: Domain users' logons may be subject to restrictions imposed by group membership, typically to ensure compliance with product licensing.
If this policy is disabled, logons by local administrators are not processed by Profile Management. If this policy is not configured here, the value from the .ini file is used. If this policy is not configured here or in the .ini file, administrators will not be processed.

Path to user store

Sets the path to the directory (the user store) in which the user settings (registry changes and synchronized files) are saved.

The path can be:

- **A relative path**. This must be relative to the home directory (which is typically configured as the #homeDirectory# attribute for a user in Active Directory).
- **A UNC path**. This typically specifies a server share or a DFS namespace.
- **Disabled or unconfigured**. In this case, a value of #homeDirectory#\Windows is assumed.

The following types of variables can be used for this policy:

- System environment variables enclosed in percent signs (for example, %ProfVer%). Note that system environment variables generally require additional setup.
- Attributes of the Active Directory user object enclosed in hashes (for example, #sAMAccountName#).
- Profile Management variables. For more information on these, see Profile Management variables.

User environment variables cannot be used, except for %username% and %userdomain%. You can also create custom attributes to fully define organizational variables such as location or users. Attributes are case-sensitive.

Examples:

- \\server\share\#sAMAccountName# stores the user settings to the UNC path \\server\share\JohnSmith (if #sAMAccountName# resolves to JohnSmith for the current user)
- \\server\profiles$\%USERNAME%.%USERDOMAIN%\!CTX_OSNAME!!CTX_OSBITNESS! might expand to \\server\profiles$\JohnSmith.DOMAINCONTROLLER1\Win8x64

Important: Whichever attributes or variables you use, check that this policy expands to the folder one level higher than the folder containing NTUSER.DAT. For example, if this file is contained in \\server\profiles$\JohnSmith.Finance\Win8x64\UPM_Profile, set the path to the user store as \\server\profiles$\JohnSmith.Finance\Win8x64 (not the \UPM_Profile subfolder).
For more information on using variables when specifying the path to the user store, see the following topics:

- Share Citrix user profiles on multiple file servers
- Administer profiles within and across OUs
- High availability and disaster recovery with Profile Management

If Path to user store is disabled, the user settings are saved in the Windows subdirectory of the home directory.

If this policy is disabled, the user settings are saved in the Windows subdirectory of the home directory. If this policy is not configured here, the value from the .ini file is used. If this policy is not configured here or in the .ini file, the Windows directory on the home drive is used.

Active write back

With this policy, files and folders (but not registry entries) that are modified can be synchronized to the user store in the middle of a session, before logoff.

If this policy is not configured here, the value from the .ini file is used. If this policy is not configured here or in the .ini file, it is enabled.

Offline profile support

This policy allows profiles to synchronize with the user store at the earliest possible opportunity. It is aimed at laptop or mobile device users who roam. When a network disconnection occurs, profiles remain intact on the laptop or device even after rebooting or hibernating. As mobile users work, their profiles are updated locally and are eventually synchronized with the user store when the network connection is re-established.

If this policy is not configured here, the value from the .ini file is used. If this policy is not configured here or in the .ini file, offline profiles are disabled.

Back to top

The policies in this section (for example, Redirect the AppData(Roaming) folder) specify whether to redirect folders that commonly appear in profiles, and the redirection target. Specify targets as UNC paths (for server shares or DFS namespaces) or as paths relative to users' home directory. This is typically configured with the #homeDirectory# attribute in Active Directory.

If a policy is not configured here, Profile Management does not redirect the specified folder.

Note: When you use UNC paths for folder redirection, the #homedirectory# variable is not supported. After you choose the Redirect to the user's home directory policy, you do not need to specify the path.

Back to top

Delay before deleting cached profiles

Sets an optional extension to the delay before locally cached profiles are deleted at logoff. A value of 0 deletes the profiles immediately, at the end of the logoff process. Profile Management checks for logoffs every minute, so a value of 60 ensures that profiles are deleted between one and two minutes after users have logged off (depending on when the last check took place). Extending the delay is useful if you know that a process keeps files or the user registry hive open during logoff. With large profiles, this can also speed up logoff.

Important: This policy works only if Delete locally cached profiles on logoff is enabled.
If this policy is not configured here, the value from the .ini file is used. If this policy is not configured here or in the .ini file, profiles are deleted immediately.

Delete locally cached profiles on logoff

Specifies whether locally cached profiles are deleted after logoff.

If this policy is enabled, a user's local profile cache is deleted after they have logged off. This is recommended for terminal servers. If this policy is disabled cached profiles are not deleted.

Note: You can control when profiles are deleted at logoff using Delay before deleting cached profiles.
If **Delete locally cached profiles on logoff** is not configured here, the value from the .ini file is used. If this policy is not configured here or in the .ini file, cached profiles are not deleted.

Local profile conflict handling

This policy configures how Profile Management behaves if both a profile in the user store and a local Windows user profile (not a Citrix user profile) exist.

If this policy is disabled or set to the default value of Use local profile, Profile Management uses the local profile, but does not change it in any way. If this policy is set to Delete local profile, Profile Management deletes the local Windows user profile, and then imports the Citrix user profile from the user store. If this policy is set to Rename local profile, Profile Management renames the local Windows user profile (for backup purposes) and then imports the Citrix user profile from the user store.

If this policy is not configured here, the value from the .ini file is used. If this policy is not configured here or in the .ini file, existing local profiles are used.

Migration of existing profiles

Profile Management can migrate existing profiles "on the fly" during logon if the user has no profile in the user store. Select Roaming if you are migrating roaming profiles or Remote Desktop Services profiles.

The following event takes place during logon: if an existing Windows profile is found and the user does not yet have a Citrix user profile in the user store, the Windows profile is migrated (copied) to the user store on the fly. After this process, the user store profile is used by Profile Management in the current and any other session configured with the path to the same user store.

If this setting is enabled, profile migration can be activated for roaming and local profiles (the default), roaming profiles only, local profiles only, or profile migration can be disabled altogether. If profile migration is disabled and no Citrix user profile exists in the user store, the existing Windows mechanism for creating new profiles is used as in a setup without Profile Management.

If this policy is not configured here, the value from the .ini file is used. If this policy is not configured here or in the .ini file, existing local and roaming profiles are migrated. If this policy is disabled, no profile is migrated. If this policy is disabled and no Citrix user profile exists in the user store, the existing Windows mechanism for creating new profiles is used as in a setup without Profile Management.

Template profile

Specifies the path to any profile you want to use as a template. This is the full path to the folder containing the NTUSER.DAT registry file and any other folders and files required for the template profile.

Important: Ensure that you do not include NTUSER.DAT in the path. For example, with the file \\myservername\myprofiles\template\ntuser.dat, set the location as \\myservername\myprofiles\template.
Use absolute paths, which can be UNC ones or paths on the local machine. You can use the latter, for example, to specify a template profile permanently on a Citrix Provisioning Services image). Relative paths are not supported.

Note that this policy does not support expansion of Active Directory attributes, system environment variables, or the %USERNAME% and %USERDOMAIN% variables.

If this policy is disabled, templates are not used. If this policy is enabled, Profile Management uses the template instead of the local default profile when creating new user profiles. If a user has no Citrix user profile, but a local or roaming Windows user profile exists, by default the local profile is used (and migrated to the user store, if this is not disabled). This can be changed by enabling the checkbox Template profile overrides local profile or Template profile overrides roaming profile. Additionally, identifying the template as a Citrix mandatory profile means that, like Windows mandatory profiles, changes are not saved.

If this policy is not configured here, the value from the .ini file is used. If this policy is not configured here or in the .ini file, no template is used.

Back to top

Number of retries when accessing locked files

Sets the number of retries when accessing locked files.

If this policy is disabled the default value of five retries is used. If this policy is not configured here, the value from the .ini file is used. If this policy is not configured here or in the .ini file, the default value is used.

Process Internet cookie files on logoff

Some deployments leave extra Internet cookies that are not referenced by the file Index.dat. The extra cookies left in the file system after sustained browsing can lead to profile bloat. Enable this policy to force processing of Index.dat and remove the extra cookies. The policy increases logoff times, so only enable it if you experience this issue.

If this policy is not configured here, the value from the .ini file is used. If this policy is not configured here or in the .ini file, no processing of Index.dat takes place.

Disable automatic configuration

Profile Management examines any XenDesktop environment, for example for the presence of personal vDisks, and configures Group Policy accordingly. Only Profile Management policies in the Not Configured state are adjusted, so any customizations you have made are preserved. This feature speeds up deployment and simplifies optimization. No configuration of the feature is necessary, but you can disable automatic configuration when upgrading (to retain settings from earlier versions) or when troubleshooting. Automatic configuration does not work in XenApp or other environments.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, automatic configuration is turned on so Profile Management settings might change if the environment changes.

Log off user if a problem is encountered

If this policy is disabled or not configured, users are given a temporary profile if a problem is encountered (for example, the user store is unavailable). If it is enabled, an error message is displayed and users are logged off. This can simplify troubleshooting of the problem.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, a temporary profile is provided.

Back to top

Enable logging

This policy enables or disables logging. Only enable this policy if you are troubleshooting Profile Management.

If this policy is disabled only errors are logged. If this policy is not configured here, the value from the .ini file is used. If this policy is not configured here or in the .ini file, only errors are logged.

Log settings

This is a set of policies that you can use to focus on specific activities. Only set these policies if you are troubleshooting, and set them all unless you are requested to do otherwise by Citrix personnel.

If these policies are not configured here, Profile Management uses the values from the .ini file. If these policies are not configured here or in the .ini file, errors and general information are logged.

The check boxes for these policies correspond to the following settings in the .ini file: LogLevelWarnings, LogLevelInformation, LogLevelFileSystemNotification, LogLevelFileSystemActions, LogLevelRegistryActions, LogLevelRegistryDifference, LogLevelActiveDirectoryActions, LogLevelPolicyUserLogon, LogLevelLogon, LogLevelLogoff, and LogLevelUserName.

Maximum size of the log file

The default value for the maximum size of the Profile Management log file is small. If you have sufficient disk space, increase it to 5 or 10 MB, or more. If the log file grows beyond the maximum size, an existing backup of the file (.bak) is deleted, the log file is renamed to .bak, and a new log file is created. The log file is created in %SystemRoot%\System32\Logfiles\UserProfileManager.

If this policy is disabled, the default value of 1 MB is used. If this policy is not configured here, the value from the .ini file is used. If this policy is not configured here or in the .ini file, the default value is used.

Path to log file

Sets an alternative path to which the log files are saved.

The path can point to a local drive or a remote, network-based one (a UNC path). Remote paths can be useful in large, distributed environments but they can create significant network traffic, which may be inappropriate for log files. For provisioned, virtual machines with a persistent hard drive, set a local path to that drive. This ensures log files are preserved when the machine restarts. For virtual machines without a persistent hard drive, setting a UNC path allows you to retain the log files but the system account for the machines must have write access to the UNC share. Use a local path for any laptops managed by the offline profiles feature.

If a UNC path is used for log files, Citrix recommends that an appropriate access control list is applied to the log file folder to ensure that only authorized user or computer accounts can access the stored files.

Examples:

- D:\LogFiles\ProfileManagement.
- \\server\LogFiles\ProfileManagement

If this policy is not configured here, the value from the .ini file is used. If this policy is not configured here or in the .ini file, the default location %SystemRoot%\System32\Logfiles\UserProfileManager is used.

Back to top

Exclusion list

List of registry keys in the HKCU hive which are ignored during logoff.

Example: Software\Policies

If this policy is disabled, no registry keys are excluded. If this policy is not configured here, the value from the .ini file is used. If this policy is not configured here or in the .ini file, no registry keys are excluded.

Inclusion list

List of registry keys in the HKCU hive that are processed during logoff.

Example: Software\Adobe.

If this policy is enabled, only keys on this list are processed. If this policy is disabled, the complete HKCU hive is processed. If this policy is not configured here, the value from the .ini file is used. If this policy is not configured here or in the .ini file, all of HKCU is processed.

Enable Default Exclusion List - Profile Management 5.5

Default list of registry keys in the HKCU hive that are not synchronized to the user's profile. Use this policy to specify GPO exclusion files without having to fill them in manually.

If you disable this policy, Profile Management does not exclude any registry keys by default. If you do not configure this policy here, Profile Management uses the value from the .ini file. If you do not configure this policy here or in the .ini file, Profile Management does not exclude any registry keys by default.

NTUSER.DAT backup

Enables a backup of the last known good copy of NTUSER.DAT and rollback in case of corruption.

If you do not configure this policy here, Profile Management uses the value from the .ini file. If you do not configure this policy here or in the .ini file, Profile Management does not back up NTUSER.DAT.

Back to top

Exclusion list - files

List of files that are ignored during synchronization. File names must be paths relative to the user profile (%USERPROFILE%). Wildcards are allowed and are applied recursively.

Examples:

- Desktop\Desktop.ini ignores the file Desktop.ini in the Desktop folder
- %USERPROFILE%*.tmp ignores all files with the extension .tmp in the entire profile
- AppData\Roaming\MyApp*.tmp ignores all files with the extension .tmp in one part of the profile

If this policy is disabled, no files are excluded. If this policy is not configured here, the value from the .ini file is used. If this policy is not configured here or in the .ini file, no files are excluded.

Exclusion list - directories

List of folders that are ignored during synchronization. Folder names must be specified as paths relative to the user profile (%USERPROFILE%).

Example:

- Desktop ignores the Desktop folder in the user profile

If this policy is disabled, no folders are excluded. If this policy is not configured here, the value from the .ini file is used. If this policy is not configured here or in the .ini file, no folders are excluded.

Enable Default Exclusion List - directories - Profile Management 5.5

Default list of directories ignored during synchronization. Use this policy to specify GPO exclusion directories without having to fill them in manually.

If you disable this policy, Profile Management does not exclude any directories by default. If you do not configure this policy here, Profile Management uses the value from the .ini file. If you do not configure this policy here or in the .ini file, Profile Management does not exclude any directories by default.

Back to top

Directories to synchronize

Profile Management synchronizes each user's entire profile between the system it is installed on and the user store. It is not necessary to include subfolders of the user profile by adding them to this list.

Paths on this list must be relative to the user profile.

Example:

- Desktop\exclude\include ensures that the subfolder called include is synchronized even if the folder called Desktop\exclude is not

Disabling this policy has the same effect as enabling it and configuring an empty list.

If this policy is not configured here, the value from the .ini file is used. If this policy is not configured here or in the .ini file, only non-excluded folders in the user profile are synchronized.

Files to synchronize

Profile Management synchronizes each user's entire profile between the system it is installed on and the user store. It is not necessary to include files in the user profile by adding them to this list.

This policy can be used to include files below excluded folders. Paths on this list must be relative to the user profile. Wildcards can be used but are only allowed for file names. Wildcards cannot be nested and are applied recursively.

Examples:

- AppData\Local\Microsoft\Office\Access.qat specifies a file below a folder that is excluded in the default configuration
- AppData\Local\MyApp*.cfg specifies all files with the extension .cfg in the profile folder AppData\Local\MyApp and its subfolders

Disabling this policy has the same effect as enabling it and configuring an empty list.

If this policy is not configured here, the value from the .ini file is used. If this policy is not configured here or in the .ini file, only non-excluded files in the user profile are synchronized.

Folders to mirror

This policy can help solve issues involving any transactional folder (also known as a referential folder), that is a folder containing interdependent files, where one file references others. Mirroring folders allows Profile Management to process a transactional folder and its contents as a single entity, thereby avoiding profile bloat. For example, you can mirror the Internet Explorer cookies folder so that Index.dat is synchronized with the cookies that it indexes. Be aware that, in these situations the "last write wins" so files in mirrored folders that have been modified in more than one session will be overwritten by the last update, resulting in loss of profile changes.

For example, consider how Index.dat references cookies while a user browses the Internet. If a user has two Internet Explorer sessions, each on a different server, and they visit different sites in each session, cookies from each site are added to the appropriate server. When the user logs off from the first session (or in the middle of a session, if the active write back feature is configured), the cookies from the second session should replace those from the first session. However, instead they are merged, and the references to the cookies in Index.dat become out of date. Further browsing in new sessions results in repeated merging and a bloated cookie folder.

Mirroring the cookie folder solves the issue by overwriting the cookies with those from the last session each time the user logs off so Index.dat stays up to date.

If this policy is not configured here, the value from the .ini file is used. If this policy is not configured here or in the .ini file, no folders are mirrored.

Back to top

Profile streaming

With the Citrix streamed user profiles feature, files and folders contained in a profile are fetched from the user store to the local computer only when they are accessed by users after they have logged on. Registry entries and any files in the pending area are exceptions. They are fetched immediately.

If this policy is not configured here, the value from the .ini file is used. If this policy is not configured here or in the .ini file, it is disabled.

Always cache

Optionally, to enhance the user experience, use this policy with the Profile streaming policy.

This imposes a lower limit on the size of files that are streamed. Any file this size or larger is cached locally as soon as possible after logon. To use the cache entire profile feature, set this limit to zero (which fetches all of the profile contents as a background task).

If this policy is not configured here, the value from the .ini file is used. If this policy is not configured here or in the .ini file, it is disabled.

Timeout for pending area lock files

You can set a timeout period (days) that frees up users' files so they are written back to the user store from the pending area in the event that the user store remains locked when a server becomes unresponsive. Use this policy to prevent bloat in the pending area and to ensure the user store always contains the most up-to-date files.

If this policy is not configured here, the value from the .ini file is used. If this policy is not configured here or in the .ini file, the default value of one day is used.

Streamed user profile groups

This policy streams the profiles of a subset of Windows user groups in the OU. The profiles of users in all other groups are not streamed.

If this policy is disabled, all user groups are processed. If this policy is not configured here, the value from the .ini file is used. If this policy is not configured here or in the .ini file, all users are processed.

Back to top

Enable cross-platform settings

By default, to facilitate deployment, cross-platform settings are disabled. Turn on processing by enabling this policy but only after thorough planning and testing of this feature.

If this policy is not configured here, the value from the .ini file is used. If this policy is not configured here or in the .ini file, no cross-platform settings are applied.

Cross-platform settings user groups

Enter one or more Windows user groups. For example, you might use this policy to process only the profiles from a test user group. If this policy is configured, the cross-platform settings feature of Profile Management processes only members of these user groups. If this policy is disabled, the feature processes all of the users specified by the Processed groups policy.

If this policy is not configured here, the value from the .ini file is used. If this policy is not configured here or in the .ini file,

all user groups are processed.

Path to cross-platform definitions

Identifies the network location of the definition files that you copied from the download package. This must be a UNC path. Users must have read access to this location, and administrators must have write access to it. The location must be a Server Message Block (SMB) or Common Internet File System (CIFS) file share.
If this policy is not configured here, the value from the .ini file is used. If this policy is not configured here or in the .ini file, no cross-platform settings are applied.

Path to cross-platform settings store

Sets the path to the cross-platform settings store, the folder in which users' cross-platform settings are saved. Users must have write access to this area. The path can be an absolute UNC path or a path relative to the home directory.

This is the common area of the user store where profile data shared by multiple platforms is located. Users must have write access to this area. The path can be an absolute UNC path or a path relative to the home directory. You can use the same variables as for Path to user store.
If this policy is disabled, the path Windows\PM_CP is used. If this policy is not configured here, the value from the .ini file is used. If this policy is not configured here or in the .ini file, the default value is used.

Source for creating cross-platform settings

Specifies a platform as the base platform if this policy is enabled in that platform's OU. This policy migrates data from the base platform's profiles to the cross-platform settings store.

Each platform's own set of profiles are stored in a separate OU. This means you must decide which platform's profile data to use to seed the cross-platform settings store. This is referred to as the base platform. If the cross-platform settings store contains a definition file with no data, or the cached data in a single-platform profile is newer than the definition's data in the store, Profile Management migrates the data from the single-platform profile to the store unless you disable this policy.

Important: If this policy is enabled in multiple OUs, or multiple user or machine objects, the platform that the first user logs on to becomes the base profile.
By default this policy is Enabled.

Back to top

Integrate

Aug 14, 2017

This section contains information for Citrix administrators deploying Profile management with other Citrix products or components. Use this information in addition to, not instead of, the other topics in the Profile management documentation. For example, for solutions to common issues with Profile management in such deployments see Troubleshoot.

This section also contains information about how some third-party products interact with Profile management or profiles in general.

Profile Management and XenApp

Aug 14, 2017

Use of this version of Profile management on XenApp servers is subject to the Profile management end-user license agreement (EULA). You can also install Profile management on local desktops, allowing users to share their local profile with published resources.

Note: Profile management automatically configures itself in XenDesktop but not XenApp environments. You must use Group Policy or the .ini file to adjust Profile management settings for your XenApp deployment.
Profile management works in XenApp environments that employ Remote Desktop Services (formerly known as Terminal Services). In these environments, you must set up an OU for each supported operating system. For more information, see your Microsoft documentation.

In farms that contain different versions of XenApp or that run different operating systems, Citrix recommends using a separate OU for each server that runs each version or operating system.

Important: Including and excluding folders that are shared by multiple users (for example, folders containing shared application data published with XenApp) is not supported.

Profile management can be used in environments where applications are streamed to either user devices directly or streamed to XenApp servers and, from there, published to users.

Client-side application virtualization technology in XenApp is based on application streaming which automatically isolates the application. The application streaming feature enables applications to be delivered to XenApp servers and client devices, and run in a protected virtual environment. There are many reasons to isolate the applications that are being streamed to users, such as the ability to control how applications interact on the user device to prevent application conflicts. For example, isolation of user settings is required if different versions of the same application are present; Microsoft Office 2003 may be installed locally and Office 2007 may be streamed to users' devices. Failure to isolate user settings creates conflicts, and might severely affect the functionality of both applications (local and streamed).

For requirements relating to the use of Profile management with streamed applications, see System requirements.

Profile Management and XenDesktop

Aug 14, 2017

Important: Citrix recommends using the profile management capabilities integrated into XenDesktop. For information on this, see the XenDesktop documentation. The information in this topic applies to a different deployment - the use of XenDesktop with the Profile management component that has been separately installed and configured.

Use of this version of Profile management with XenDesktop is subject to the Profile management end-user license agreement (EULA). Subject to the terms in the EULA, you can also use Profile management with XenApp in a XenDesktop environment.

If you upgrade Profile management in a XenDesktop deployment, consider the effect on the log file locations as described in Upgrade Profile management.

For XenDesktop in Quick Deploy setups, see the recommendations in Decide on a configuration.

If Profile management has not been configured correctly on the images before they are rolled out, the Profile Management Service starts before Group Policy is applied. To avoid this, perform the configuration using the documented procedures before you put the images into a production environment.

Important: Including and excluding folders that are shared by multiple users (for example, folders containing data that can be shared by multiple virtual desktops) is not supported.

If you use the personal vDisk feature of XenDesktop, Citrix user profiles are stored on virtual desktops' personal vDisks by default, typically the P: drives. The profiles are not stored on users' C: drives. However, this is where Profile management expects to find the profiles so you must modify the Registry on the master image while installing or upgrading the Virtual Desktop Agent. In addition, because you have freed up space on the personal vDisk, it is also good practice to increase the default allocation of disk space for applications on the master image. For instructions on these modifications, see Managing XenDesktop documentation.

Do not delete the copy of a profile in the user store while a copy remains on the personal vDisk. Doing so creates a Profile management error, and causes a temporary profile to be used for logons to the virtual desktop. For more information on this, see
— Users Receive New or Temporary Profiles
in Troubleshooting common issues.

In XenDesktop environments, Windows Store applications (also known as Metro apps) are supported on dedicated desktops and on desktops with personal vDisks, but not on other desktop types.

Metro apps are intended for use by single users on dedicated devices. They are not designed to work with any type of roaming profile, including Citrix user profiles. If a user requires Metro apps on their desktops, Citrix recommends creating their profile on a dedicated desktop, and preserving the profile at logoff. The user should access the apps on this desktop only. Metro apps on any other desktops that create profiles in the user store will be unusable.

Metro apps do not work if:

1. A user accesses a pooled machine (pooled-random, static, or RDS) containing any type of roaming profile (including a Citrix user profile)
2. A user accesses a dedicated desktop with a personal vDisk (the recommended solution) but their profile was already created on another desktop

In these cases, there is a temporary fix that allows the user to install the apps in their current session. This is to follow the Microsoft recommendation of enabling the Allow deployment operations in special profiles policy. In Group Policy Management Editor, this is located in Computer Configuration > Policies > Administrative Templates > Windows Components > App Package Deployment. However, this fix requires users to install the apps each time they log on.

This topic lists Profile management policy settings used in a typical XenDesktop deployment. Windows 7 virtual desktops are created with Citrix Provisioning Services and are shared by multiple users. In this example, the desktops, which are created from a pooled-random catalog and are deleted at logoff, are intended for use on static workstations (not mobile laptops) and personal vDisks are not used.

Where no policy is listed, no selection or entry was made in Group Policy, and the default setting applies.

Note the following:

- **Path to user store** - You can incorporate Profile management variables into the path to the user store. This example uses !CTX_OSNAME! and !CTX_OSBITNESS!, which expand to Win7 and x86 respectively when the path is interpreted. The AD attribute #sAMAccountName# is also used to specify user names.
- **Delete locally cached profiles on logoff** - Disabling this policy is safe because the desktops do not include personal vDisks and get deleted when users log off. Preserving locally cached profiles is therefore unnecessary. (If the desktops were not discarded at logoff, this policy should be enabled.)
- **Profile streaming** - Enabling this setting improves logon times in this deployment.
- **Active write back** - This policy is enabled because the pooled desktops in this deployment are only temporarily allocated to users, who might therefore make changes to their profile but might forget (or not bother) to close their desktop session. With this setting enabled, local file changes in the profile are mirrored in the user store before logoff.

Note: If you enable the Active write back policy, performing a significant number of file operations in a session - such as file creation, file copy, and file deletion – can cause high system I/O activity and result in temporary performance issues while Profile management syncs the file changes to the user store.

- **Process logons of local administrators** - Enabling this setting is recommended for XenDesktop deployments, in which most users will be local administrators.
- **Processed groups** - All domain users' profiles are managed by Profile management.
- **Exclusion list - directories** (file system) and **Exclusion list** (registry) - These settings prevent the listed temporary or cached files, and the listed registry entries, from being processed. These files and entries are commonly stored in user profiles.
- **Directories to synchronize** and **Files to synchronize** - Knowledge of where users' application data is stored helped define these settings.

Important: XenDesktop deployments vary, so the Profile management policy settings you decide on will probably be different to those in this example. To plan your settings, follow the advice in Decide on a configuration.

Citrix/Profile Management

Enable Profile management

Enabled

Processed groups

MyDomainName\Domain Users

Path to user store

\\MyServer.MyDomain\MyUserStore\#sAMAccountName#\!CTX_OSNAME!_!CTX_OSBITNESS!

Active write back

Enabled

Process logons of local administrators

Enabled

Citrix/Profile Management/Profile handling

Delete locally cached profiles on logoff

Disabled

Citrix/Profile Management/Advanced settings

Process Internet cookie files on logoff

Enabled

Citrix/Profile Management/File system

Exclusion list - directories

$Recycle.Bin

AppData\Local\Microsoft\Windows\Temporary Internet Files

AppData\Local\Microsoft\Outlook

AppData\Local\Temp

AppData\LocalLow

AppData\Roaming\Microsoft\Windows\Start Menu

AppData\Roaming\Sun\Java\Deployment\cache

AppData\Roaming\Sun\Java\Deployment\log

AppData\Roaming\Sun\Java\Deployment\tmp

Citrix/Profile Management/File system/Synchronization

Directories to synchronize

AppData\Microsoft\Windows\Start Menu\Programs\Dazzle Apps

Folders to mirror

AppData\Roaming\Microsoft\Windows\Cookies

Citrix/Profile Management/Streamed user profiles
Profile streaming
Enabled

Profile Management and VDI-in-a-Box

Aug 14, 2017

You can use Profile management on desktops created with Citrix VDI-in-a-Box. For more information on this, see Configuring User Profile Management with VDI-in-a-Box.

Use of this version of Profile management with VDI-in-a-Box is subject to the Profile management end-user license agreement (EULA). Subject to the terms in the EULA, you can also use Profile management with XenApp in a VDI-in-a-Box environment. For more information, see Profile Management and XenApp.

Profile Management and UE-V

Aug 14, 2017

Profile management 5.x and Microsoft User Experience Virtualization (UE-V) 2.0 can co-exist in the same environment. UE-V is particularly useful when multiple profile versions are present (for example, Version 1 and Version 2 profiles). For this reason, do not use the cross-platform settings feature of Citrix Profile management when UE-V is present. In fact, UE-V may be preferred over that feature because it supports more applications, synchronization during user sessions, and XML configuration and generation for applications.

When Profile management co-exists with UE-V, whether or not the cross-platform settings feature is enabled:

- Exclude the AppData\Local\Microsoft\UEV folder. Profile settings captured by UE-V then overwrite those captured by Profile management.
- Do not share profiles controlled by UE-V with those controlled by Profile management alone. If you do, the "last write wins". In other words, the last component to synchronize the profile (UE-V or Profile management) determines which data is saved; this can lead to data loss.

Note: UE-V requires the Microsoft Desktop Optimization Pack (MDOP).

Profile Management and ShareFile

Aug 14, 2017

The information in this topic applies to the use of Profile management in Citrix ShareFile deployments. Some of it may also be useful for other Internet-based file-sharing systems.

You can use ShareFile with Profile management 4.1.2 and later. ShareFile is only supported in On-Demand mode.

If you use ShareFile 2.7, to avoid a compatibility issue install this version first before installing Profile management. This installation dependency does not exist with ShareFile 2.6.

ShareFile stores configuration data locally in the \AppData\Roaming\ShareFile folder. For users with Citrix user profiles, this data must roam with the user profile so that the user-specific ShareFile configuration is persisted. Since this ShareFile folder is part of the profile, no Profile management configuration is required; the configuration data roams by default.

However, user data that is managed by ShareFile is contained in the ShareFile folder that is in the root of the profile (%USERPROFILE%\ShareFile). This data must not roam with the profile because it is managed by, and synchronizes with, the ShareFile server. You must therefore add this folder as a Profile management exclusion. For instructions on setting exclusions, see To include and exclude items.

If you create virtual desktops with Personal vDisks (using Citrix XenDesktop), configure ShareFile with the location of the user data on the vDisks. This ensures that file synchronization can take place between the desktops and the ShareFile server. By default, Personal vDisks are mapped as P: drives on the desktops so the data might be located in P:\Users\<user name>. In this case, you would set the location using the LocalSyncFolder policy in ShareFile.

Important: To prevent unnecessary synchronizations, which can adversely affect the performance of Profile management and Personal vDisks, Citrix recommends using the Folder-ID setting on folders that contain large files unless they need to be synchronized on the virtual desktop. This is a ShareFile setting.

Profile Management and App-V

Aug 14, 2017

You can use Profile Management 5.x in the same environment as Microsoft Application Virtualization 5.0 (App-V 5.0).

Note: Profile Management supports only globally published App-V.

You must exclude the following item using Profile management exclusions:

- Profile Management\File system\Exclusion list\directories:
  - AppData\Local\Microsoft\AppV

You must add the following Profile Management policies:

- Profile Management\File system\Exclusion list\directories:
  - AppData\Local\Microsoft\AppV
  - AppData\Roaming\Microsoft\AppV\Client\Catalog
- Profile Management\registry\Exclusion list:
  Software\Microsoft\AppV\Client\Integration
  Software\Microsoft\AppV\Client\Publishing

For instructions on setting exclusions, see To include and exclude items.

If the UserLogonRefresh setting is enabled in App-V, disable the Profile streaming policy in Profile Management.

For an example of how to sequence an App-V application, see http://support.microsoft.com/kb/2830069.

For information on configuring third-party Profile management solutions with App-V enabled, see https://technet.microsoft.com/en-us/library/dn659478.aspx. Do not include Software\Classes on Microsoft Windows 10 systems.

Profile Management and Provisioning Services

Aug 14, 2017

This topic contains advice on maintaining Citrix user profiles on virtual disks (vDisks) created with Citrix Provisioning Services. Before following this advice, you should understand how your vDisk configuration affects your Profile management configuration as described in Persistent? Provisioned? Dedicated? Shared?

You can use Profile management on vDisks running in Standard Image and Private Image modes but not Difference Disk Image mode.

To prevent any non-essential, locally cached profiles being stored, ensure these are removed from vDisks running in Standard Image mode before taking the Master Target Device image, but do not remove the currently logged-on local administrator's profile. A good way of achieving this is as follows. During this procedure, error messages may be displayed.

1. Right-click Computer.
2. Select Properties.
3. Click Advanced system settings.
4. On the Advanced tab, click Settings in User Profiles.
5. Highlight each profile you want to remove and click Delete.

This topic provides guidance on using log files that reside on shared (vDisk) images created with Citrix Provisioning Services. Profile management saves the files at logoff, but, if you use vDisk images, you should take account of the fact that base images can be reset, which results in log files being deleted. You therefore need to take some action in order to retrieve the files. The action you take depends on whether the log files are being deleted at logon or logoff.

Use of vDisk images is common in XenDesktop deployments, so the guidance in this topic uses that product as an example.

To retrieve a log file that is deleted at logoff

If entire profiles or parts of them are not saved back to the user store on the network, the log file will also not be saved there.

If the Provisioning Services write-cache is stored on the computer running Provisioning Services, this issue should not arise and the log file should be saved back to the user store.

If the write-cache is stored locally, in this procedure you may have to log on from the same device as the user. However, even this may fail if the write-cache is stored locally in RAM.

If the write cache is not on the computer running Provisioning Services, you may have to create a copy of the vDisk image, assign it to the new virtual machine, and change the write-cache on the image so it is stored on that computer.

1. In XenDesktop, create a new desktop group, add one virtual machine to it, and point it to your vDisk image.
2. Grant access to the virtual machine to one test user and the administrator.
3. Modify the desktop group's idle pool count to 1 for all times of the day (to stop power management turning the

machine off), and set its logoff behavior to Do nothing (to prevent the machine restarting and resetting the image).
4. Log on as the test user to the virtual desktop and then log off from it.
5. Log on as administrator from the XenCenter or VMware console, and retrieve the log file.

Consult the XenDesktop documentation for more information on creating desktop groups and modifying their properties.

To retrieve a log file that is deleted at logon

If a profile is current in the user store on the network but does not load correctly when the user logs on, log file entries will be lost.

1. Map a drive to \\<vmhostname>\C$ and, before the user logs off the session, locate the log file. The log file will not be complete (some entries will be missing) but if the problem you are troubleshooting is at logon, it may provide enough information for you to isolate the cause of the issue.

To relocate Provisioning Services log files

Using Standard Image mode, the Provisioning Services event log files are lost when the system shuts down. For instructions on changing the default location of the files to prevent this, see CTX115601.

To preconfigure Profile Management on provisioned images

Aug 14, 2017

Using provisioning software such as Citrix Provisioning Services, Citrix XenServer, or VMware ESX you can build images that have Profile management pre-installed. When doing so, you will likely capture some Group Policy settings in the registry while you set up the image (for example, while it is in Private Image mode with Provisioning Services). The settings will still be present when you deploy the image (for example, when you switch back to Standard Image mode with Provisioning Services). Ideally, you should choose defaults that suit the state of the virtual machine when it starts running and your users requirements when they log on. At a minimum, you should ensure you have suitable defaults for those policies described in Persistent? Provisioned? Dedicated? Shared?

The defaults are used if gpupdate is not run before the Citrix Profile Management Service starts, so it is best to make sure they are sensible defaults for the majority of cases. Use this procedure to preconfigure these and other settings you want to preserve in the image.

Note: If you use Provisioning Services, Citrix recommends that you preconfigure images with the Profile management .ini file first and that you transfer the settings to the .adm or .admx file only once your testing proves successful.

1. If you use the .adm or .admx file, change the desired settings using the file in the appropriate GPO. If you use the .ini file, omit this step; you will make the changes in a later step.
2. Make the same changes to the log level.
3. Do one of the following:
   - Switch the image to Private Image mode (Citrix Provisioning Services) and start the operating system on it.
   - Start the operating system (Citrix XenServer or VMware ESX).
4. Log on using an Administrator account (not any test user account you may have set up), and run gpupdate /force. This step ensures the registry is correctly configured.
5. If you use the .ini file, change the desired settings in the file.
6. Stop the Profile Management Service.
7. To avoid confusion with the new log files that will be created, delete the old Profile management log file and the configuration log file. These have file names that use the name of the old image. They are redundant because the updated image has new files (with the name of the new image).
8. Do one of the following:
   - Switch the image back to Standard Image mode (Citrix Provisioning Services).
   - Save the updated image (Citrix XenServer or VMware ESX).
9. Start the operating system on the image.

Profile Management and Self-service Plug-in

Aug 14, 2017

By default, Profile management excludes the Windows Start menu folder. This means that Citrix Self-service Plug-in users cannot see their subscribed applications in the Start menu. Adjust this default behavior by removing the folder %APPDATA%\Microsoft\Windows\Start Menu from the **Exclusion list - directories** policy. In addition, when using GPOs for configuration, it is best practice to delete the Profile management .ini file. These actions ensure that the Start menu folder containing subscribed applications (and any user-created subfolders) are processed by Profile management.

Note: If you are using the Profile management .ini file rather than Group Policy, remove this entry from the default exclusion list in that file.

Profile Management and VMware

Aug 14, 2017

This topic applies to Citrix user profiles on virtual machines created with VMware software such as VMware ESX. It addresses an issue where local profile caches become locked.

If you have set up Profile management to delete cached local profiles when users log off from their virtual machines created with VMware (in your XenDesktop or XenApp deployment, say) but the profiles are not deleted, you can use this workaround to overcome the issue.

This issue has been shown to occur when roaming profiles are used on virtual machines created with VMware ESX 3.5 and the Profile management setting Delete locally cached profiles on logoff is enabled.

The issue occurs because the Shared Folders option in VMware Tools adds a file to the profiles, and the file is locked by a running process thereby preventing profiles being deleted at logoff. The file is C:\Documents and Settings\userid\Application Data\VMware\hgfs.dat.

If you have verbose logging enabled in Profile management, the log file may detect this problem with an entry such as:

2009-06-03;11:44:31.456;ERROR;PCNAME;JohnSmith4;3;3640;DeleteDirectory: Deleting the directory <C:\Documents and Settings\<user name>\Local Settings\Application Data\VMware> failed with: The directory is not empty.

To work around this issue in a XenApp deployment on Windows Server 2008:

1. Log on as Administrator to the XenApp server.
2. In XenApp deployments, log off all users from the server.
3. In Control Panel, go to Add/Remove Programs.
4. Locate VMware Tools and choose the Change option.
5. Change Shared Folders to This feature will not be available.
6. Click Next > Modify > Finish.
7. Restart the server.
8. Clean up the half-deleted profiles. Use My Computer > Properties > Advanced > User Profiles, select the profiles and delete them. Windows informs you of any errors trying to delete the profiles.

Note: A separate issue in environments running Profile management on VMware can result in the creation of multiple sequential profiles. For information about this issue and how to resolve it, see CTX122501.

Profile Management and Outlook

Aug 14, 2017

This topic describes best practice for integrating Microsoft Outlook with roaming profiles.

It is good practice to ensure that users store Outlook data on a server rather than on a network share or locally.

With roaming profiles, files and folders in the location defined by the environment variable %UserProfile% (on the local computer) roam with users, with the exception of one folder, %UserProfile%\Local Settings. This exception affects Outlook users because a Microsoft recommendation means that, by default, some Outlook data (for example, .ost, .pst, and .pab files) is created in this non-roaming folder.

Important: Files in this location are typically large and hinder the performance of roaming profiles.
The following practices can reduce troubleshooting of roaming profiles with Outlook and encourage good email management by users and administrators:

- If possible, use an ADM template for Microsoft Office that prohibits the use of .pst files.
- If users need more space, increase storage on your Microsoft Exchange servers rather than a network share.
- Define and enforce an email retention policy for the entire company (one that involves a company-wide email storage server) rather than granting exceptions for .pst files to individual users or increasing their personal storage capacity. The policy should also discourage reliance on .pst files by allowing users easily to request email restores to their inbox.
- If .pst files cannot be prohibited, do not configure Profile management or roaming profiles on your Exchange servers.

Using Windows profiles with Password Manager and Single Sign-on

Aug 14, 2017

This topic does not contain any information specific to Profile management. It tells you how to configure certain Windows options so that Citrix Single Sign-on operates optimally with local profiles, roaming profiles, mandatory profiles, or hybrid profiles. This topic applies to Citrix Single Sign-on 4.8 or 5.0.

Local profiles are stored on the local server to which the user has logged on. Password Manager and Single Sign-on save registry information in the HKCU\Software\Citrix\MetaFrame Password Manager hive of the User Registry located at:

%SystemDrive%\Documents and Settings\%username%\NTUSER.DAT.

Files are also saved in:

%SystemDrive%\Documents and Settings\%username%\Application Data\Citrix\MetaFrame Password Manager.

On Windows 7, Single Sign-on uses:

%APPDATA%\Roaming\Citrix\MetaFrame Password Manager

Important: It is critical that Single Sign-on has Full Control Access to the following files:

File Name	Description
%username%.mmf	User's credential information file with pointers to aelist.ini.
entlist.ini	Application definition file created at enterprise level in the synchronization point or Active Directory.
aelist.ini	Application definition file created by merging user's local application definition file (applist.ini) and the enterprise application definitions (entlist.ini).

Roaming profiles are saved on a network share and synchronized to a local server copy each time the user logs on. Characteristics of a successful roaming profile deployment include high-speed network connectivity such as a SAN (System Area Network) or NAS (Network Area Storage). Other common deployments include clustering solutions where the profiles are stored on high-availability servers.

Two issues affect roaming and mandatory profile deployments:

- A single roaming profile can only be used with one file synchronization point. When multiple synchronization points are used, data in the Memory Mapped File (MMF) may become corrupted.
- When roaming profiles are used with multiple concurrent sessions, they share the same backend MMF. This means that

all active sessions share some common session data such as retry lock counters, last used data counters, and event log entries.

Mandatory profiles are by definition user read-only profiles. Single Sign-on needs write permission to the profile folder under Application Data. With mandatory profiles, a user may make changes but the changes are not saved back to the profile at logoff. For Single Sign-on to work correctly with mandatory profiles, the Application Data Folder must be redirected.

The registry changes are written each time the user logs on. Credential information is synchronized with the synchronization point but the changes are not saved back to the profile.

Beginning with Windows 2000, Microsoft provides a mechanism for redirecting the Application Data folder. However, using Windows NT4 domains requires logon scripts capable of modifying the location of the Application Data folder. You can achieve this using tools such as Kix or VBScript to define a writeable location for the Application Data folder.

The following example uses Kix to redirect the Application Data folder during user logon:

Important: This sample script is for informational purposes only and should not be used in your environment without first testing it.

```
$LogonServer = "%LOGONSERVER%"
$HKCU = "HKEY_CURRENT_USER"
$ShellFolders_Key =
"$HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell
Folders"
$UserShellFolders_Key =
"$HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\User
Shell Folders"
$UserProfFolder =
"$LogonServer\profiles\@userID"
$UserAppData =
"$LogonServer\profiles\@userID\Application Data"
$UserDesktop =
"$LogonServer\profiles\@userID\Desktop"
$UserFavorites =
"$LogonServer\profiles\@userID\Favorites"
$UserPersonal = "X:\My Documents"
$UserRecent =
"$LogonServer\profiles\@userID\Recent"
if (exist("$UserAppData") = 0)
shell '%ComSpec% /c md "$UserAppData"'
endif
if (exist("$UserDesktop") = 0)
shell '%ComSpec% /c md "$UserDesktop"'
endif
if (exist("$UserRecent") = 0)
shell '%ComSpec% /c md "$UserRecent"'
endif
if (exist("$UserFavorites") = 0)
```

```
shell '%ComSpec% /c md "$UserFavorites"'
endif
```

The hybrid profile is another solution for the mandatory profile issue. When the user logs on, the mandatory profile loads and a custom application loads and unloads user registry hives based on applications available to the user. As with mandatory profiles, the user can modify those parts of the registry during a session. The difference compared with mandatory profiles is that changes are saved when the user logs off and are reloaded when they log on again.

If a hybrid profile is used, the HKEY_CURRENT_USER\Software\Citrix\MetaFrame Password registry keys must be imported and exported as part of the logon and logoff process.

Folder redirection is implemented using Group Policy Objects and Active Directory. It uses Group Policies to define a location for folders that are part of the user profile.

Four folders can be redirected:

- My Documents
- Application Data
- Desktop
- Start Menu

Two modes of redirection can be configured using Group Policies: basic redirection and advanced redirection. Both are supported by Single Sign-on. In Windows 2000, you must reference the share that stores application data using the username variable, (for example \\servername\sharename\%username%).

Folder redirection is global for the user and it affects all of their applications. This means all applications that use the Application Data folder must support it.

Read the following Microsoft articles to learn more about folder redirection:

HOW TO: Dynamically Create Secure Redirected Folders By Using Folder Redirections

Folder Redirection Feature in Windows

Enabling the Administrator to Have Access to Redirected Folders

- Redirect the Application Data folders where possible. This improves network performance, eliminating the need to copy the data in those folders each time users log on.
- When troubleshooting Password Manager Agent, always verify that the logged-on user has Full Control permission on their Application Data folder.

Google Chrome browser

Aug 14, 2017

Google Chrome users are advised to exclude the following folders from synchronizing:

- Appdata\Local\Google\Chrome\User Data\Default\JumpListIcons
- Appdata\Local\Google\Chrome\User Data\Default\JumpListIconsOld
- Appdata\Local\Google\Chrome\User Data\Default\Cache=
- Appdata\Local\Google\Chrome\User Data\Default\Cached Theme Images=

Firefox browser

Aug 14, 2017

Firefox users are advised to exclude the following file from synchronizing:

Appdata\roaming\mozilla\Firefox\profiles*\sessionstore.bak

Secure

Aug 14, 2017

This topic contains recommended best practice for securing Profile Management. In general, secure the servers on which the user store is located to prevent unwanted access to Citrix user profile data.

Recommendations on creating secure user stores are available in the article called Create a file share for roaming user profiles on the Microsoft TechNet Web site. These are minimum recommendations that ensure a high level of security for basic operation. Additionally, when configuring access to the user store include the Administrators group, which is required in order to modify or remove a Citrix user profile.

Citrix tests and recommends the following permissions for the user store and the cross-platform settings store:

- Share Permissions: Full control of the user store root folder
- The following NTFS permissions, as currently recommended by Microsoft:

Group or User Name	Permission	Apply To
Creator Owner	Full Control	Subfolders and files only
<The group of accounts under Profile management control>	List Folder / Read Data and Create Folders / Append Data	This folder only
Local System	Full Control	This folder, subfolders and files

Assuming inheritance is not disabled, these permissions allow the accounts to access the stores, create subfolders for users' profiles, and perform the necessary read and write operations.

Beyond this minimum, you can also simplify administration by creating a group of administrators with full control of subfolders and files only. This makes deleting profiles (a common troubleshooting task) easier for members of that group.

If you use a template profile, users need read access to it.

If you use the cross-platform settings feature, set ACLs on the folder that stores the definition files as follows: read access for authenticated users, and read-write access for administrators.

Windows roaming profiles automatically removes administrator privileges from the folders containing profile data on the network. Profile Management does not automatically remove these privileges from folders in the user store but, depending on your organization's security policies, you can do so manually.

Note: If an application modifies the ACL of a file in the user's profile, Profile Management does not replicate those changes in the user store. This is consistent with the behavior of Windows roaming profiles.

The streamed user profiles feature of Citrix Profile Management makes use of advanced NTFS features to simulate the presence of files missing from users' profiles. In that respect, the feature is very similar to a class of products known as Hierarchical Storage Managers (HSMs), which are typically used to archive infrequently used files on to slow mass-storage devices such as magnetic tape or rewritable optical storage. When such files are required, HSM drivers intercept the first file request, suspend the process making the request, fetch the file from the archive storage, and then allow the file request to continue. Given this similarity, the streamed user profiles driver, upmjit.sys, is in fact defined as an HSM driver.

In such an environment, it is very important to configure antivirus products to be aware of HSM drivers, and the streamed user profiles driver is no different. In order to defend against the most sophisticated threats, antivirus products must perform some of their functions at the device driver level and, like HSM drivers, they work by intercepting file requests, suspending the originating process, scanning the file, and resuming.

It is relatively easy to misconfigure an antivirus program to interrupt an HSM such as the streamed user profiles driver, preventing it from fetching files from the user store, and causing the logon to hang.

Fortunately, enterprise antivirus products are usually written with the possibility of sophisticated storage products, such as HSMs, in mind and can be configured to delay their scanning until the HSM has done its work. Note that home antivirus products are generally less sophisticated in this respect, so the use of home and SoHo (small office/home office) antivirus products is not supported with streamed user profiles.

To configure your antivirus product for use with streamed user profiles, look for one of the following product features. Feature names are indicative only:

- **Trusted process list**. This identifies HSMs to the antivirus product, which allows the HSM to complete the file retrieval process. The antivirus product scans the file when it is first accessed by a non-trusted process.
- **Do not scan on open or status-check operations**. This configures the antivirus product to only scan a file when data is accessed (for example, when a file is executed or created). Other types of file access (for example, when a file is opened or its status checked) are ignored by the antivirus product. HSMs generally activate in response to file-open and file-status-check operations, so disabling virus scans on these operations eliminates potential conflicts.

Citrix tests streamed user profiles with versions of the leading enterprise antivirus products to ensure that they are compatible with Profile Management. These versions include:

- McAfee Virus Scan Enterprise 8.7
- Symantec Endpoint Protection 11.0
- Trend Micro OfficeScan 10

Earlier versions of these products are not tested.

If you are using an enterprise antivirus product from other vendors, ensure that it is HSM-aware, that is, it can be configured to allow HSM operations to complete before performing scans.

Some antivirus products allow administrators to choose to only scan-on-read or scan-on-write. This choice balances performance against security. The streamed user profiles feature is unaffected by the choice.

Troubleshoot Profile Management in streaming and antivirus deployments

If you encounter issues, such as logons hanging or taking a very long time, there may be a misconfiguration between Profile Management and your enterprise antivirus product. Try the following procedures, in this order:

1. Check that you have the latest version of Profile Management. Your issue may already have been found and fixed.
2. Add the Profile Management service (UserProfileManager.exe) to the list of trusted processes for your enterprise antivirus product.
3. Turn off virus checking on HSM operations such as open, create, restore, or status check. Only perform virus checks on read or write operations.
4. Turn off other sophisticated virus checking features. For example, antivirus products may perform a quick scan of the first few blocks of a file to determine the actual file type. These checks match the file contents with the declared file type but can interfere with HSM operations.
5. Turn off the Windows search-indexing service, at least for the folders where profiles are stored on local drives. This service causes unnecessary HSM retrievals, and has been observed to provoke contention between streamed user profiles and enterprise antivirus products.

If none of these steps work, turn off streamed user profiles (by disabling the Profile streaming setting). If this works, re-enable the feature and disable your enterprise antivirus product. If this also works, gather Profile Management diagnostics for the non-working case and contact Citrix Technical Support. They will need to know the exact version of enterprise antivirus product.

To continue using Profile Management, do not forget to re-enable the enterprise antivirus and turn off streamed user profiles. Other features of Profile Management continue to function in this configuration; only the streaming of profiles is disabled.

Troubleshoot

Aug 14, 2017

As a first step in troubleshooting any issue that you or your users experience, follow these basic steps:

1. If you are using XenDesktop 7, start troubleshooting in Desktop Director. This console displays properties of profiles that can help you diagnose and correct problems.
2. Use UPMConfigCheck. This is a PowerShell script that examines a live Profile Management deployment and determines whether it is optimally configured. For more information on this tool, see CTX132805.
3. If a Profile Management .ini file is in use, check its configuration on the affected computer.
4. Check the settings in Group Policy (GP) against the recommended configurations that are described in Decide on a configuration. To deactivate any Profile Management policy that you enter as lists (for example, exclusion lists and inclusion lists), set the policy to Disabled. Do not set the policy to Not Configured.
5. Check the HKLM\Software\Policies registry entry on the affected computer to see if there are any stale policies due to GP tattooing issues, and delete them. Tattooing occurs when policies are deleted from GP but remain in the registry.
6. Check the file UPMSettings.ini, which contains all of the Profile Management settings that have been applied for each user. This file is located in the root folder of each Citrix user profile in the user store.

If these steps do not correct the issue, consult the remaining topics in this section of eDocs.

Enable logging for troubleshooting

Aug 14, 2017

Only enable logging if you experience an issue in your Profile management deployment and want to troubleshoot it. In addition, disable logging when the issue is resolved and delete the log files, which may contain sensitive information.

This policy enables or disables logging. Only enable this policy if you are troubleshooting Profile management.

If Enable logging is disabled, only errors are logged. If this policy is not configured in GP, the value from the .ini file is used. If this policy is not configured in GP or the .ini file, only errors are logged.

This policy is a set of options that you can use to focus on specific actions and events. Only set these options if you are troubleshooting, and set them all unless you are requested to do otherwise by Citrix personnel.

If Log settings is not configured in GP, Profile management uses the settings from the .ini file. If this policy is not configured in GP or the .ini file, errors and general information are logged.

The default value for the maximum size of the Profile management log file is 10 MB (10485760 bytes). If you have sufficient disk space, increase it to 20 MB (20971520 bytes), or more. If the log file grows beyond the maximum size, an existing backup of the file (.bak) is deleted, the log file is renamed to .bak, and a new log file is created. The log file is created in %SystemRoot%\System32\Logfiles\UserProfileManager.

In XenDesktop deployments that use Machine Creation Services a persistent folder imposes a 15 MB (15728640 bytes) limit on log files (not just Profile management ones). You can store your log files on a system disk, where this limitation does not apply, or use this policy to restrict the log file size to a maximum of 7 MB (7864320 bytes); Profile management can then store, on the persistent folder, the current log file and the previous one as a .bak file.

If this policy is disabled, the default value of 10 MB (10485760 bytes) is used. If this setting is not configured in GP, the value from the .ini file is used. If this setting is not configured in GP or the .ini file, the default value is used.

You can set an alternative path to which the log files are saved. The path can be to a local drive or a remote, network-based one (a UNC path). Remote paths can be useful in large, distributed environments, but they can create significant network traffic, which may be inappropriate for log files.

For profiles on virtual machines, consider whether drives on the desktops are persistent because this affects logging. If a desktop has a persistent drive (for example, if it was created with a personal vDisk using Citrix XenDesktop), set a local path to it; the log files are preserved when the machine restarts. If a desktop does not have a persistent drive (for example, it was created without a personal vDisk using XenDesktop), set a UNC path; this allows you to retain the log files but the system account for the machines must have write access to the UNC share. Use a local path for any laptops managed by the offline profiles feature.

If a UNC path is used for log files:

- Citrix recommends that an access control list is applied to the log file folder to ensure that only authorized user or computer accounts can access the stored files.
- Duplicate log files remain locally. These can be left on the computer, but if you want to remove them, first stop the Profile Management Service, delete the log file and the configuration log file, and restart the computer.
- Set NTFS and SMB share level permissions to Domain computers Read/Write.

Examples:

- D:\LogFiles\ProfileManagement
- \\servername\LogFiles\ProfileManagement

If Path to log file is not configured in GP, the value from the .ini file is used. If this policy is not configured in GP or the .ini file, the default location %SystemRoot%\System32\Logfiles\UserProfileManager is used.

For the special case of XenDesktop Machine Creation Services, a local, persistent folder is mapped to the C drive at C:\Program Files\Citrix\PvsVM\Service\PersistedData. This is a good location to store up to 15 MB of log data, but, if you use it, note the limit on Maximum size of the log file.

Profile Management log files

Aug 14, 2017

The following logs can be useful when troubleshooting Profile management.

Informal Name	Log Name	Location	Type of Log Information
Windows event log	<None>	%SystemRoot%\system32\LogFiles	The Windows event log, which you view with Microsoft Event Viewer, is used primarily for the purpose of error reporting. Only errors are written to it.
Profile management log file	<domainname># <computername>_pm.log	%SystemRoot%\system32\LogFiles\UserProfileManager	Informational messages and warnings, including errors, are written to the Profile management log file. <domainname> is the computer's domain and <computername> is its name. If the domain cannot be determined, this log file is called UserProfileManager.log.
Profile management configuration log file	<domainname># <computername>_pm_config.log	%SystemRoot%\system32\LogFiles\UserProfileManager	The configuration log file captures the GPO and .ini file settings even if logging is turned off. If the domain cannot be determined it is called UserProfileManager_pm_config.

If requested by Citrix Technical Support, you may also need to examine the log files created with Citrix Diagnostic Facility.

The rest of this topic describes the contents of the Profile management log file.

- **Common warnings**. All common warnings.
- **Common information**. All common information.
- **File system notifications**. One log entry is created each time a processed file or folder is changed.
- **File system actions**. File system operations performed by Profile management.
- **Registry actions**. Registry actions performed by Profile management.
- **Registry differences at logoff**. All registry keys in the hive HKCU that have been changed in a session.
  Important: This setting produces large amounts of output in the log file.
- **Active Directory actions**. Each time Profile management queries the Active Directory, an entry is written to the log file.
- **Policy values**. When the Profile management service starts or a policy refresh occurs, policy values are written to the log file.
- **Logon**. The series of actions during logon are written to the log file.
- **Logoff**. The series of actions during logoff are written to the log file.
- **Personalized user information**. Where applicable, user and domain names are logged to dedicated columns of the log file.

When the Citrix policy setting for each entry type is enabled, that entry type is logged.

Each line in the log file has several fields, separated by semicolons.

Field	Description
Date	Date of the log entry
Time	Time of the log entry (including milliseconds)
Severity	Either INFORMATION, WARNING, or ERROR
Domain	The domain of the user (where applicable)
User name	The name of the user (where applicable)
Session ID	The session ID (where applicable)
Thread ID	The ID of the thread that created this line
Function and description	The name of the Profile management function executing at the time, and the log message

Events logged by Profile Management

Aug 14, 2017

Events logged by Profile management can be used by Citrix EdgeSight or third-party monitoring and reporting tools. View the events in Windows Event Viewer. Select the Applications node in the left pane; the Source of the events in the right pane is Citrix Profile management.

Events are not all sequentially numbered and not all are used in this version of Profile management. However, they might be logged if you upgrade from an earlier version.

Event ID	Description	Cause	Action
6	The Citrix Profile management service has started.	The Citrix Profile management service has started. This may be the result of an automatic start, a manual start, or a restart.	If the start or restart was not planned, check the event log for errors and take any corrective action indicated, including Profile management troubleshooting procedures.
7	The Citrix Profile management service has stopped.	The Citrix Profile management service has stopped. This may be the result of a manual stop or as part of shutdown processing.	If the service stop was not planned, check the event log for errors and take any corrective action indicated, including Profile management troubleshooting procedures.
8	The profile for user <user name> has been modified by a later version of Citrix Profile management and can no longer be used by this version...	The Citrix Profile management service on this machine has detected that a later version of Profile management has modified the user's profile in the user store. To prevent possible data loss, earlier versions of Profile management revert to using a temporary profile.	Upgrade this computer (and all other computers sharing the same user store and using earlier versions of Profile management) to use the latest version.
9	The logon hook detection encountered a problem...	The Citrix Profile management service detected a problem while setting up logon notification. The Citrix Profile management service requires either that: • The installation path contains no spaces • 8.3 filename support is enabled on the volume where the service is installed	Reinstall Citrix Profile management to a path with no spaces or enable 8.3 filename support on the volume where Profile management is installed.

Event ID	Description	Cause	Action
10	User <user name> path to the user store is...	A valid Citrix user profile has been found at the location indicated.	None. This message is for information only.
11	spsMain: CreateNamedPipe failed with...	(This event is no longer used.)	None.
12	StartMonitoringProfile: A problem was detected in the Windows change journal management during logon...	The Citrix Profile Management Service was unable to monitor the profile or a folder configured for extended synchronization. A problem was detected in the Windows change journal event management, preventing the Service from monitoring changes. Citrix Profile Management will not process this folder. A Windows user profile will be used instead.	Ensure that change journal processing is configured and operational for all volumes managed by Profile management. Ensure that the computer has adequate system resources. Check the event log for errors and take any corrective action indicated, including Profile management troubleshooting procedures.
13	StopMonitoringProfile: A problem was detected in the Windows change journal management during logoff...	The Citrix Profile Management Service was unable to stop monitoring the profile or a folder configured for extended synchronization. A problem was detected in the Windows change journal management, preventing the Service from monitoring changes. Citrix Profile management will not process this folder. File and registry changes will not be synchronized for the user.	Ensure that change journal processing is configured and operational for all volumes managed by Profile management. Ensure that the computer has adequate system resources. Check the event log for errors and take any corrective action indicated, including Profile management troubleshooting procedures.
14	CJIncreaseSizeIfNecessary: Creating/resizing the change journal failed...	The Citrix Profile management service was unable to monitor the profile or a folder configured for extended synchronization. A problem was detected while attempting to create or resize the NTFS change journal on a volume, preventing the service from monitoring changes. Citrix Profile Management will not process this folder. A Windows user profile will be used instead.	Ensure that change journal processing is configured and operational for all volumes managed by Profile management. Ensure that the computer has adequate system resources. Check the event log for errors and take any corrective action indicated, including Profile management troubleshooting procedures.
15	CJInitializeForMonitoring:	The Citrix Profile management service	Ensure that change journal processing

Event ID	Description	Cause	Action
	Unable to query the journal...	was unable to monitor the profile or a folder configured for extended synchronization. A problem was detected while querying the NTFS change journal on a volume, preventing the service from monitoring changes. Citrix Profile Management will not process this folder. A Windows user profile will be used instead.	is configured and operational for all volumes managed by Profile management. Ensure that the computer has adequate system resources. Check the event log for errors and take any corrective action indicated, including Profile management troubleshooting procedures.
16	CJInitializeForMonitoring: Initial MFT scan finished with errors.	The Citrix Profile management service was unable to monitor the profile or a folder configured for extended synchronization. A problem was detected while performing an initial scan of the NTFS change journal on a volume, preventing the service from monitoring changes. Citrix Profile Management will not process this folder. A Windows user profile will be used instead.	Ensure that change journal processing is configured and operational for all volumes managed by Profile management. Ensure that the computer has adequate system resources. Check the event log for errors and take any corrective action indicated, including Profile management troubleshooting procedures.
17	CJInitializeForMonitoring: Processing FS changes since service start failed.	The Citrix Profile management service was unable to monitor the profile or a folder configured for extended synchronization. A problem was detected while performing an update scan of the NTFS change journal on a volume. This error does not prevent the service from monitoring changes. Citrix Profile management will process this directory as normal.	Although this error does not prevent the operation of Profile management, check for errors anyway. Ensure that change journal processing is configured and operational for all volumes managed by Profile management. Ensure that the computer has adequate system resources. Check the event log for errors and take any corrective action indicated, including Profile management troubleshooting procedures.
18	CJProcessAvailableRecords: Internal Error...	A failure occurred in the Citrix Profile management service while monitoring the profile or a folder configured for extended synchronization. A problem was detected while performing an update scan of the NTFS change journal on a volume, preventing the service from monitoring recent changes. Citrix Profile management	The Citrix Profile Management Service was unable to monitor the profile or a folder configured for extended synchronization. A problem was detected in the Windows change journal event management, preventing the Service from monitoring changes. Citrix Profile Management will not process this folder. A Windows user

Event ID	Description	Cause	Action
		will not complete processing on this folder. Back up critical data manually.	profile will be used instead.
19	USNChangeMonitor: Initialization of change journal failed...	A failure occurred in the Citrix Profile management service while monitoring the profile or a folder configured for extended synchronization. A problem was detected while preparing the initial scan of the NTFS change journal on a volume, preventing the service from monitoring changes. Citrix Profile management will not complete processing on this directory. Back up critical data manually.	The Citrix Profile Management Service was unable to monitor the profile or a folder configured for extended synchronization. A problem was detected in the Windows change journal event management, preventing the Service from monitoring changes. Citrix Profile Management will not process this folder. A Windows user profile will be used instead.
20	CADUser::Init: Determining the DNS domain and ADsPath failed...	A problem occurred while querying Active Directory for information about the logged-on user. Citrix Profile management will not process this folder. A Windows user profile will be used instead.	Ensure that the computer has a functioning network path to a domain controller. Ensure that the computer has adequate system resources. Check the event log for errors and take any corrective action indicated, including Profile management troubleshooting procedures.
21	Determining the DNS domain and ADsPath failed...	This issue can be caused by a limit on memory allocation, as described in the Microsoft TechNet article 263693.	The resolution for this issue is described in the Citrix Knowledge Center article CTX124953.
22	File access was slow. User <user name> experienced a delay while file <file name> was fetched from the user store.	The user tried to access the file but Profile management detected a delay in this operation. The user received a warning message. This may be due to antivirus software preventing access to the file in the user store.	Consult the Profile management documentation for troubleshooting and configuration advice on enterprise antivirus products.
23	File access may be denied. User <user name> experienced a long delay while file <file name> was fetched from the user store.	The user tried to access the file but Profile management detected such a significant delay in this operation that access may be denied. The user received an error message. This may be due to antivirus software preventing access to the file in the user store.	Consult the Profile management documentation for troubleshooting and configuration advice on enterprise antivirus products.

Event ID	Description	Cause	Action
24	RevertToSelf failed with error code <error code number> and Profile management was shut down.	Some logon and logoff processing is performed using impersonation. The RevertToSelf function is normally invoked when impersonation is complete. On this occasion, the function could not be called so, for security reasons, Profile management software was shut down. The user received an error message.	If you suspect a security breach, follow your organization's procedures to address it, and then restart Profile management.
25	The profile for user <user name> is managed by Citrix Profile management, but the user store <user store name> could not be reached...	The Citrix Profile Management Service on this computer could not reach the specified user store. This is normally because of a network issue or because the server hosting the user store is unavailable.	Ensure the server hosting the user store is available and the network between this computer and the server is operational.
26	The default profile location <location name> is invalid. Profiles in this location cannot be monitored correctly...	Profiles on this computer must be located on a disk mounted on a drive letter (for example, C:).	Move the profiles on this computer to a disk mounted on a drive letter, and restart Profile management.
27	The profile folder for user <user name> is not present under the default profile location <location name>...	In the registry, the location of this user's profile and of the default profile do not match. This can occur, for example, if profiles are moved between different volumes on the machine running the Profile Management Service.	Ensure this user's profile is located under the default folder location, using appropriate tools if necessary so that the profile data in the file system matches the profile's registry settings.
28	An error occurred while trying to reset security permissions on the registry hive for user <user name>.	It is likely that there are permission issues with the registry in the default or template profile used to create this Citrix user profile.	If appropriate, reset the security permissions on the user's registry hive in the Profile management user store using a third-party utility such as SetAcl.
29	A template profile path is configured but no profile was found...	The specified folder cannot be used in the Template profile setting because it does not contain the file NTUSER.DAT. This issue commonly occurs when the full path of the NTUSER.DAT file is configured instead	Check that you have configured a valid path to the folder containing the template profile. Check that the path contains NTUSER.DAT, that this is a valid file, and that access rights are set correctly on the folder to allow read

Event ID	Description	Cause	Action
		of the folder containing NTUSER.DAT. Note that the Template profile setting does not support expansion of Active Directory attributes, system environment variables, or the %USERNAME% and %USERDOMAIN% variables.	access to all files.
33	Citrix Profile Management created a profile in the user store from a local profile at <location>	A profile was created in the user store from the location indicated.	None. This message is for information only.
34	Citrix Profile Management created a profile in the user store from a roaming profile at <location>	A profile was created in the user store from the location indicated.	None. This message is for information only.
35	Citrix Profile Management created a profile in the user store from a template profile at <location>	A profile was created in the user store from the location indicated.	None. This message is for information only
36	The existing profile folder for <user> could not be prepared for this user's new Citrix mandatory profile. The user will be given a temporary profile if possible.	Citrix mandatory profiles use copies of a template profile for each logon. Any existing profiles are deleted and the Citrix mandatory profiles are copied from the specified template location. This process failed.	Delete any existing profile folder manually. You may have to restart the computer if files are locked by another process that causes the deletion to fail. Ensure the template folder exists and the user has permissions to read its contents.
37	The user store <user store path> for user <user name> could not be reached. A temporary profile will be created for this user and no changes will be saved to their profile in this user store.	The Citrix Profile Management Service on this computer could not reach the specified user store. This is normally because of a network issue or because the server hosting the user store is unavailable.	Ensure the server hosting the user store is available and the network between this computer and the server is operational.
38	The profile for user <user name> is managed by	The Citrix Profile Management Service on this computer could not find the	Ensure the server hosting the user store is available, the network

Event ID	Description	Cause	Action
	Citrix Profile management, but the user store <user store path> could not be found. A temporary profile will be created for this user and no changes will be saved to their profile in this user store.	profile in the specified user store. This may be because of a network issue or because the server hosting the user store is unavailable, but it may also be because the profile in the user store has been deleted or moved, or the path to the user store has changed and no longer correctly points to an existing profile in the user store.	between this computer and the server is operational and the path to the user store points to an existing profile. If the profile in the user store has been deleted, delete the profile on the local machine.

Log file checklist

Aug 14, 2017

After working through the basic troubleshooting checklist, examine the Profile management log file as follows.

1. Make sure that logging is enabled.
2. Check the log file for errors. Locate these by searching for the word ERROR.
3. Check the log file for warnings. Locate these by searching for the word WARNING.
4. Run the command gpupdate /force on the computer on which the error occurs, and check the log file again. Review which settings are active and from where the configuration has been read (either Group Policy or an .ini file).
5. Check the path to the user store is correct.
6. Check all information from Active Directory was read correctly.
7. Check the time stamps. Is there an action that took too long?

If the log file does not help you identify the issue, see Advanced troubleshooting checklist.

Troubleshoot without logging

Aug 14, 2017

If no logging at all is taking place, try the troubleshooting approach used in the following example. It is designed to help you work out which configuration settings are being read, establish where they are being read from (when multiple ADM files are present), and check that the log file correctly tracks changes made to profiles. The strategy creates a small test OU to which a test user logs on, allowing you to create profile modifications that you then track in the log file and Resultant Set of Policies (RSoP) report.

The deployment in this example has XenApp servers running on Windows Server 2003 with users connecting to their published resources using the Plug-in for Hosted Apps for Windows. The deployment uses OU-based GPOs. INI file-based configuration is not used.

Caution: Editing the registry incorrectly can cause serious problems that may require you to reinstall your operating system. Citrix cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk. Be sure to back up the registry before you edit it.

1. Remove from the production environment one of the XenApp servers that hosts the Citrix user profiles, and add it to a new OU containing just this server.
2. Remove and reinstall Profile management on the server. When reinstalling, check that short file names (also known as 8.3 file names) are activated. As this example uses Windows Server 2003, you do this as follows:
   - If the following registry entry is set to 1 (DWORD value), set it to 0 and reinstall Profile management: HKLM\System\CurrentControlSet\Control\FileSystem\NtfsDisable8Dot3NameCreation. This enables support for short file names.
   - If the entry is not set to 1, reinstall Profile management to a location where each subfolder name is eight characters or less, for example c:\prof-man

   For later operating systems, you do not need to adjust this registry entry.
3. Log on as a domain administrator to the server.
4. Examine the local policy and remove the ADM file at this level.
5. Delete any links to GPOs assigned to your new OU.
6. On the server, delete the key and all subkeys from Registry Editor: HKLM\Software\Policies\Citrix\UserProfileManager\
7. Remove any Profile management .ini file.
8. Using My Computer > Properties > Advanced, delete all profiles except those you want to test. Research any errors that appear.
9. So that you can check the Profile management log file when logging on as a user, give the Authenticated Users group full control of the file. This is C:\Windows\System32\LogFiles\UserProfileManager\<domainname># <computername>_pm.log (where <domainname> is the computer's domain and<computername> is its name). If the domain cannot be determined, the log file is UserProfileManager.log.
10. Create a new GPO that contains only the following settings, and link it to your new OU. Ensure the GPO is assigned to the Authenticated Users group. Enable these settings:
    1. Enable Profile management.
    2. Path to user store.
    3. Enable logging.
    4. Log settings. Scroll to select all settings in this section of the ADM file.
    5. Migration of existing profiles. Select Roaming and local profiles.
    6. Local profile conflict handling. Select Rename local profile.
    7. Delete locally cached profiles on logoff.

Disable the setting Process logons of local administrators. This helps when troubleshooting because, if Profile management is misconfigured and prevents user logons, you will still be able to log on as an administrator.

11. Control how the GPO link is applied to the OU by right-clicking the OU and selecting Block Inheritance.
12. Create a new domain test user who has never logged on and who is not a member of any group that is a local administrator on the server.
13. Publish a full desktop to this user and make sure the user is in the Remote Desktop Users group.
14. If the domain has multiple domain controllers (DCs), force AD replication between all the DCs in the same site as the server.
15. Log on to the server as domain Administrator, delete the log file, restart the Citrix Profile Management service, and run gpupdate /force.
16. Check the registry and make sure the only values in HKLM\Software\Policies\Citrix\UserProfileManager\ are the ones for your new GPO.
17. Log out as Administrator.
18. Using the Plug-in for Hosted Apps, log on to the published full desktop as the new domain test user.
19. Make some setting changes to Internet Explorer, and create a blank test file in your My Docs folder.
20. Create a shortcut to the Profile management log file. Open it and examine the entries. Research any items that may require attention.
21. Log out and then back in as domain Administrator.
22. Generate an RSoP report for the test user and the server.

If the report does not contain what you expect, research any items that require attention.

Advanced troubleshooting checklist

Aug 14, 2017

Once you have followed the steps in the basic troubleshooting checklist to try and correct an issue, and eliminated the Profile management log file as a source of useful information, use this checklist to troubleshoot further.

- Check the Resultant Set of Policies (RSoP) from the computer you are analyzing and ensure all GPOs are applied as expected.
- Check that you have the latest version of Profile management installed. Examine the version information of UserProfileManager.exe by right-clicking the file in Windows Explorer and clicking Properties > Version. The latest version is available from the My Account site; select your Citrix product and download Profile management from the Downloads section.
  Tip: You can hotfix your deployment of Profile management 2.1.1 or later by upgrading to the latest version. After upgrading, you can, if desired, enable any later feature.
- Check the Profile management support forum. Someone else may already have encountered the problem and solved it.
- Try to reproduce the issue you are observing on a clean computer with the same operating system as the affected computer. If possible, install the software products that are present on the affected computer one by one, and see if the issue is reproduced after each installation.

Troubleshooting common issues

Aug 14, 2017

For information about known issues with slow logons and workarounds, see CTX101705.

If you have enabled streamed user profiles and want to verify that this feature is being applied to a user's profile:

1. Check the following type of entry in the Profile management log file:
   2010-03-16;16:16:35.369;INFORMATION;;;;1140;ReadPolicy: Configuration value read from policy: PSEnabled=<1>
   The last item should be set to PSEnabled=<1> if the feature is enabled.
2. Check the following entry for the user in the Profile management log file:
   2010-03-16;20:17:30.401;INFORMATION;<domain name>;<user name>;2;2364;ProcessLogon: User logging on with Streamed Profile support enabled.
   If streamed user profiles are not being applied, the item reads ProcessLogon: User logging on with Streamed Profile support disabled.

Use UPMSettings.ini (located in the root folder of each Citrix user profile in the user store) to determine the Profile management policies that are being applied. Examining this file may be more convenient than using the Resultant Set of Policy (RSoP) especially if you use a mixture of GPOs and .ini file settings to determine policies.

Use UPMFRSettings.ini (also located in the root folder) to determine which profile folders are not processed because they are on an exclusion list.

If a user profile is corrupt and you are confident the problem lies with a particular file or folder, exclude it from the synchronization process by adding it to the exclusion list.

In some scenarios (not just those involving Profile management), connections to registry profile data are preserved after users log off. This may result in slow logoffs or incomplete termination of user sessions. The User Profile Hive Cleanup (UPHClean) tool from Microsoft can help resolve these scenarios.

Microsoft Delprof.exe and Sepago Delprof2 are tools that help you delete user profiles.

If you use VMware software to create virtual desktops, but users' cached profiles are locked and cannot be deleted, see Profile management and VMware for troubleshooting information.

Diagnosing profile issues can involve locating where the files in a user's profiles are stored. This procedure provides a quick way to check this.

1. In Event Viewer, click Application in the left pane.
2. Under Source in the right pane, locate the Citrix Profile Management event of interest and double-click it.
3. The path to the user store associated with the event is displayed as a link on the General tab.
4. Follow the link to browse the user store if you want to explore the files.

To determine whether a server is processing a user's logons and logoffs correctly, check the file called PmCompatibility.ini in the user's profile in the user store. The file is located in the profile's root folder. The last entry in the file is the name of the server from which the user last logged off. For example, if the server runs Profile management 5.0, the entry would be:

[LastUpdateServerName]
5.0=<computer name>

You can roll back to earlier versions of Profile management. To do this, run del /s from the command line on the file server that hosts the user store. This deletes the file PmCompatibility.ini from each profile. For example, if the local path to the user store is D:\UpmProfiles, run:

```
del /s D:\UpmProfiles\pmcompatibility.ini
```

After the command has completed, users can log on to computers running the earlier version and receive their profile from the user store.

Replicated VMware folders are created in user profiles. The replicates have incremented folder names (000, 001, 002, and so on). For more information about this issue and how to resolve it, see CTX122501.

When users log on to an environment involving Citrix products and Novell eDirectory (formerly known as Novell Directory Services), long logon times may be experienced and errors written to the event log. Sessions may hang or freeze for up to 30 seconds at the Applying your personal settings stage. For more information about this issue and how to resolve it, see CTX118595.

Excluded folders appear in the user store. This is expected and no corrective action is required; folders on an exclusion list are created in the user store but their contents are not synchronized.

Activating debug mode does not automatically enable full logging. In Log settings, verify that you have selected all of the checkboxes for the events you want to log.

Tip: You may have to scroll down to enable the last checkboxes on the list.

You change a GPO setting but it is not operative on the computer running the Citrix Profile Management Service. This might be because GP does not refresh immediately but instead is based on events or intervals specified in your deployment. If you want to refresh GP immediately, run gpupdate /force on the computer.

For your changes to take effect, run the gpupdate /force command from the command prompt as documented at http://technet.microsoft.com/en-us/library/bb490983.aspx.

By default, users are given a temporary profile if a problem is encountered (for example, the user store is unavailable). However, you can instead configure Profile management to display an error message and then log users off. This can help with troubleshooting.

For instructions on configuring this feature, see To force user logoffs.

In some circumstances, when they log on, users receive a new profile instead of their cached profile. For more information about this issue and a workaround for it, see CTX118226.

Users may also receive a temporary profile if a local profile is present after the copy in the user store is removed. This situation can arise if the user store is cleared but local profiles are not deleted at logoff. Profile management treats such partial removal of profiles as a network, share, or permissions error, and provides the user with a temporary profile. For this reason, partial removal is not recommended. To workaround this issue, log on to the affected computer and delete the profile manually.

If your deployment includes personal vDisks (a XenDesktop feature), users may receive temporary profiles if the default processing of these disks has not been correctly adjusted. For information on this, see To migrate user profiles.

In a XenDesktop deployment, disconnecting from a Remote Desktop Protocol (RDP) session can cause a virtual desktop to become unresponsive or to restart. This impacts Profile management because it causes profile data to be lost when the session ends. The issue is fixed in Citrix Virtual Desktop Agent Version 3.1.3242 and later.

Users are unable to log on to a Citrix environment and receive the following error message: “Windows did not load your roaming profile and is attempting to log you on with your local profile... Contact your network administrator.” This appears in the Application event log on Windows as Event ID 1000, with source Userenv.

For more information about this issue and other workarounds for it, see CTX105618.

In Citrix XenDesktop environments, a user can select a default printer but in some cases the selection is not retained between logons. This has been observed when a XenDesktop policy is used to set printers on pooled virtual desktops based on a Citrix Provisioning Services vDisk in Standard Image mode. This issue does not originate with Profile management even though the Profile management log file shows that the registry entry for the printer is copied at logoff (which is expected) but NTUSER.dat for the user does not contain the entry (which is not expected). The issue in fact originates with the way XenDesktop uses the DefaultPmFlags registry setting. For more information on this, see CTX119066.

In some cases, unexpected printers are added to profiles and, after users remove them, the printers reappear at the next logon. For more information, see the Profile management support forum.

You may experience problems where application settings do not roam correctly across multiple platfoms.Typical these result from:

- Settings that are not applicable from one system to another (for example, hardware specific settings that are not on every system).
- Applications that are installed differently on different systems (for example, an application that is installed on a C: drive on one system but on D: on another, an application that is installed in C:\Program Files on one system but in C:\Program Files (x86) on another, or an Excel add-in installed on one system but not another).
- Applications that store setting information outside of the profile (for example, information stored in the local machine's settings or outside the user profile).
- Language-specific configuration settings stored in the registry. Profile management automatically translates language-specific folder names in Version 1 profiles but not in the registry.

In most instances, these issues can be minimized by better standardization of the systems that cause the issues. However, often the issues result from inherent incompatibilities (with multiple platforms) of the OS or the respective application. If the problematic settings are not critical, excluding them from the profile might resolve the issue.

On rare occasions, a profile can appear to belong to an unknown account. On the Advanced tab of the System Properties dialog box for a computer, Account Unknown is displayed when you click Settings in User Profiles. This is accompanied by an event log entry, "Profile notification of event Create for component <application ID> failed, error code is ???." In the registry, the application ID points to the SHACCT Profile Notification Handler, a Microsoft component.

To confirm that this occurs in your environment, log on as a user whose data is not processed by Profile management, and check for these symptoms.

This is not an issue with Profile management but may be the result of Active Directory interacting badly with virtual machine snapshots. The operation of Citrix user profiles is unaffected; users can log on and off, and their profile changes are preserved.

Collect diagnostic information

Aug 14, 2017

Before attempting to collect information on a problem with Profile management, make sure you can reproduce the problem.

If you are using XenDesktop 7, start troubleshooting in Desktop Director. This console displays properties of profiles that can help you diagnose and correct problems.

1. Open the Profile Management Group Policy Object (GPO) in the Group Policy Management Editor, or open the .ini file in Notepad if you are not using GPO to manage logging. For information on the .ini file including its location, see Files included in the download.
2. Configure the following settings under the Profile Management\Log settings folder:
   - Set Enable logging to Enabled.
   - Select all of the events in Log settings.
   - In Maximum size of the log file, set the maximum size of the Profile management log file in bytes.
3. Run gpupdate /force on the server or desktop.
4. If requested by Citrix Technical Support, collect a diagnostic trace log (available in Profile management 3.x or later) using the instructions in Advanced troubleshooting checklist.
5. Reproduce the problem and collect the log files, including the .log.bak file.
6. Optionally, or if requested, collect the Resultant Set of Policy (RSoP) report, application event logs, USERENV log, UPMSettings.ini, UPMFRSettings.ini, and PmCompatibility.ini. The .ini files are located in the root folder of each Citrix user profile in the user store.

Data collection can become complex if Citrix Provisioning Services is part of your deployment and the problem occurs when profiles are being initialized. In this scenario, you must make the above configuration updates in the .ini file (and unconfigure the above GPO log settings) or preferably follow the instructions in To preconfigure Profile management on provisioned images.

The diagnostic enhancements feature allows you to create and package trace logs for Citrix Technical Support. These capture events about servers (but not user devices or virtual desktops) relating to many aspects of Profile management's performance particularly the operation of streamed user profiles.

For information on creating trace logs about user devices or virtual desktops, see CTX124455.

Only package and send a trace log if you are asked to do so by Technical Support.

Before you can use Citrix Diagnostic Facility to capture trace logs, ensure it is available with the Citrix product or component that is used on the device, virtual desktop, or Citrix server whose profiles you want to monitor.

The Access Management Console and Delivery Services Console contain a powerful tool, Citrix Diagnostic Facility, which gathers and packages trace logs. These can be valuable when Citrix Support diagnose problems in your deployment.

1. In the Access Management Console or Delivery Services Console, start generating a trace log using the procedure in CTX104578.
2. When selecting which modules to trace, choose one or all of the following Profile management modules:
   - **UPM_Service**. This records each time the Profile Management Service was invoked (for example, at logon, at logoff,

or when mid-session synchronization operations or periodic maintenance takes place).

- **UPM_DLL_Perfmon**. This allows you to trace Windows Performance Monitor counters associated with and errors generated by Profile management.
- **UPM_Driver**. This records file-system changes and each time the Citrix streamed user profiles driver is used.

3. Complete the remaining steps in article CTX104578.

You can save Profile management's internal data state to a dump file. This is helpful when you can isolate an issue to a specific point in a session but there is no associated entry in the log file.

1. Create a file called $$upm_log$$.txt in the root of the drive on which the affected user profile is located (typically C:). Profile management dumps its internal data state to the file UserProfileManagerInternalData.log in the log file folder and deletes the file $$upm_log$$.txt.

For information about setting NT Symbolic Debugger (NTSD) as your default Windows postmortem debugging tool, see CTX105888.

Contact Citrix Technical Support

Aug 14, 2017

If you have checked the log file and the other troubleshooting advice in this section, and believe the problem you experience is due to Profile management, contact Technical Support. Always include the following files and as much other information as possible:

- All Profile management log files (in %SystemRoot%\System32\Logfiles\UserProfileManager). Ensure that you have all of the log settings activated.
  Log files from the affected machine should contain at least the following information:
  - Start of the service (including the version and build number of Profile management)
  - Reading of the configuration by the service
  - One full logon process of the affected user
  - The activity the user performed when the issue occurred
  - One full logoff process for the affected user

  Tip: Ensure that you have increased the maximum size of the log file.
- The Resultant Set of Policy (RSoP) for the machine and affected user.
- Details of the operating system, language, and version installed on the affected system.
- Details of Citrix products and versions installed on the system.
- PmCompatibility.ini and UPMSettings.ini. These files are located in the root folder of each Citrix user profile in the user store.
- If available, the Userenv debug file. Consult your Microsoft documentation for information on this tool.
- If available, the session dump file. For more information on this Citrix tool, see To produce a session dump file.

Glossary

Aug 14, 2017

This topic contains terms and definitions used in the Profile management software and documentation. Profile-related terms used in other Citrix software is also included. To understand other concepts relating to Windows user profiles, visit the Microsoft Web site.

Term	Definition
Base platform	See cross-platform settings store.
Base profile	The base profile is defined by a UNC path to a profile in the user store. If the cross-platform settings feature is used, registry settings and files that can be shared across platforms form a subset of the base profile. This subset is copied to the cross-platform settings store, and, from there, they are added to the profile used as the target for migration or roaming. Although the cross-platform settings store contains a subset of the base profile, this (and the target profile) are always stored as complete profiles and can, if necessary, be used as standard Windows roaming or local profiles. Note however that if the streamed user profiles feature is used, the base profile may temporarily be incomplete; some files may exist in the pending area until the user logs off. See roam for considerations when defining base profiles in roaming scenarios.
Cache	The terms cache and synchronize refer to the act of downloading files from the user store, or uploading to it. The term fetch is more specific and refers to how the streamed user profiles feature downloads, any time after logon when the user needs them, a subset of files from the user store.
Citrix mandatory profile, Citrix roaming profile, Citrix user profile	Citrix user profile is the general term for the profile that a user receives when Profile management is installed and enabled. There are two types of Citrix user profiles: Citrix roaming profiles and Citrix mandatory profiles. A Citrix roaming profile is the standard collection of files, folders, and registry settings that are customized by users in their day-to-day work, that are saved in the user store at logoff, and that are treated by Profile management policies. A Citrix mandatory profile is similar to a Citrix roaming profile in how it is treated by Profile management, but no changes are saved in the user store at logoff. At logon, a fresh copy of the mandatory profile is loaded. Citrix user profiles are different from Microsoft local, Microsoft roaming, or Microsoft mandatory profiles.
Computer	As used in these Profile Management topics, the general term computer can refer to any machine on which the Citrix Profile Management Service is installed. This can be a user device, virtual desktop

Term	Definition
	(possibly provisioned from a XenDesktop virtual machine), or a XenApp server that hosts published applications.
Cross-platform definition file	This is an .xml file supplied with Profile management that contains the information needed to make the cross-platform settings feature work. There is one file per supported application.
Cross-platform settings store	This location, which is separate from the user store, holds the settings for supported applications once the cross-platform settings feature is configured. You must choose which platform's profile data is used to seed the cross-platform settings store. This is the base platform.
Fetch	See cache.
Legacy application	A legacy application is a badly behaved one because it stores settings in a non-standard location. This includes systems that store temporary application data in user profiles and, by doing so, create profile bloat.
Migrate	Migration is the planned, one-way movement of profiles from one platform to another (for example, from Windows XP to Windows 7).
Profile bloat	Windows user profiles can increase in size when temporary files are not deleted. This causes slow logons and is referred to as profile bloat.
Roam	Roaming is the use of different base profiles from multiple computers or sessions (for example, one base profile for a computer running Windows 2008 R2 and a second one for Windows 7). Users roam when they connect back and forth between computers or sessions that have different base profiles. Depending on how you configure your Organizational Units (OUs), a base profile can be shared across platforms. For example, the same profile can be used by both Windows 2008 R2 and Windows 7 OUs; in this case users do not roam because the same base profile is shared. Base profiles can only be shared by operating systems with the same profile version (Version 1 or Version 2 profiles). This means users always roam when both Version 1 and Version 2 profiles are active.
Synchronize	See cache.
User store	The user store is the central, network location for storing Citrix user profiles. See also cross-platform settings store.
vDisk, personal	A vDisk is a virtual disk created from a master image by Citrix Provisioning Services. A personal vDisk is a disk used by Citrix XenDesktop to store profiles, user-installed and departmental

Term	Definition
vDisk	applications, and user data. Personal vDisks are separate from the disks used for the operating system, registry, and base applications.
Version 1 profile, Version 2 profile	Profiles in Microsoft Windows XP and Windows Server 2003 are known as Version 1 profiles. Those in Windows Vista, Windows 7, Windows Server 2008, and Windows Server 2008 R2 are known as Version 2 profiles. Version 1 and Version 2 profiles have different namespaces. This affects some aspects of their configuration.