Profile Management 3.x

2014-01-12 04:42:14 UTC

Contents

Profile Management 3.x

In This Section

These topics contain up-to-date information about installing, configuring, and administering Profile management 3.x. These task-based topics help you set up the feature quickly and easily. You are assumed to have some knowledge of the Citrix product with which Profile management ships, and of Windows profiles in general.

Learn about the following important topics.

About Version 3.x	Get a general overview of how Profile management works, review the new features, and check known and fixed issues.
System Requirements	Ensure your environment meets all the requirements before you install Profile management.
Upgrades	Read this important information about upgrades.
Troubleshooting	Find solutions to implementation issues.
XenApp / XenDesktop	Review important information about XenApp and XenDesktop deployments involving Profile management.

The following additional documentation is designed to increase your productivity but is not contained in eDocs.

Frequently asked questions about troubleshooting	CTX119038
Frequently asked questions about setting up cross-platform profiles	CTX119039
Frequently asked questions about licensing	CTX119747
Frequently asked questions about how Profile management works	CTX119791
Answers from experts to many questions about Profile management deployments	http://community.citrix.com/blogs

About Profile Management 3.x

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 those described in this document.

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 in Profile Management 3.x

Version 3.2.2

Version 3.2.2 contains fixes for issues present in earlier releases. The fixed issues are documented at CTX127554.

Version 3.2 and Later

Version 3.2 and later versions include a feature that allows you to avoid duplicate items in local profiles when folder redirection is used. It also includes fixes for issues present in earlier releases. The fixed issues are documented at http://support.citrix.com/article/CTX124164.

Version 3.1.1 and Later

The following issues have been fixed in Version 3.1.1 and later versions:

- Items on the Quick Launch toolbar and browser favorites are not displayed correctly and do not work. [#234837]
- On Windows Server 2003 systems, the presence of Citrix offline plug-in 6.0 and Profile management 3.1 affects CPU usage adversely and prevents streamed applications from starting. [#234347]
- Memory leaks occur if you enable the **Profile streaming** and **Always cache** settings. [#234665]
- If you enable the **Profile streaming** setting, some files (for example, usrclass.dat) in locally cached profiles are deleted when users log on. [#234918]
- McAfee VirusScan Enterprise fails when users log on. The associated error refers to mcshield.exe. [#234081]
- Temporary files are not discarded when users log off. The files are used when users log on again if the following conditions apply: the **Delete locally cached profiles on logoff** setting is disabled; **Path to user store** is modified; and **Local profile conflict handling** is set to **Use local profile** (the default). [#234278]
- When a user attempts to log on, a "Windows cannot log you on because your profile cannot be loaded" user environment popup appears and Event ID - 1508 is reported in Windows Event Log. [#235427]

Version 3.1 and Later

Version 3.1 and later versions include the following new key features:

- **Folder mirroring**. Profile management can mirror folders, allowing the correct processing of transactional folders. For example, mirroring the Internet Explorer cookies folder means that index.dat is synchronized only with the latest version of the cookies that it references, not earlier versions that are no longer required. Without mirroring, multiple copies of the referenced files (cookies from multiple sessions, for example) can cause profile bloat.

- **Deleting stale cookies**. Profiles in some deployments can become bloated with stale browser cookies when Web sites are revisited. A setting in the ADM file can be used to delete the stale files.

- **Diagnostic enhancements**. Additional Performance Monitor (Perform) counters allow you to measure the time spent: processing registry changes and file changes at logoff; migrating files from the pending area to the user store; and deleting local profiles. No configuration of Perfmon is required to use these counters.

Version 3.0 and Later

Version 3.0 and later versions include the following new key features:

- **Citrix streamed user profiles**. This feature offers alternative options for speeding up logons and logoffs by fetching parts of users' profiles from the user store only when they are needed. One of the options is to use the **cache entire profile** feature, which fetches all of the files but staggers their delivery in the background.

- **Active profile write back**. To improve profile integrity if sessions terminate abnormally, files that are modified on the local computer can be backed up to the user store during a session, before logoff.

- **Another supported operating system**. Windows Server 2008 R2 is now supported.

- **Installation enhancements**. Profile management checks for more errors during installation and, if they are encountered, writes messages to the event log. A new command-line switch optionally installs Profile management without the .ini files that were previously used for configuration.

- **Diagnostic enhancements**. You can monitor streamed user profile performance using a subset of Performance Monitor counters and data from the log files. In this version, to view the counters you no longer need to be a full administrator on the computer used to manage Profile management. In addition, for each user logon, event log messages display the full path to the user store, and the log file indicates whether streamed user profiles are enabled for each user. You can now also create trace logs with Citrix Diagnostic Facility in the event of advanced troubleshooting initiated by Citrix Technical Support.

- **Localization**. The Profile management software and documentation are now localized into French, German, Spanish, Japanese, and Simplified Chinese.

Existing Features of Profile Management

Profile management 3.x includes the following features from previous releases:

- **Profile migration**. Allows you to migrate profiles to and from physical computers and virtual ones. Depending on the configuration settings, Profile management can copy existing roaming profiles and local Windows profiles to the user store. Existing mandatory profiles can be used as the basis for Citrix user profiles when saved as a template.
- **Wildcard support**. Allows the use of wildcard characters in file names for synchronization, inclusion, and exclusion lists.
- **Extended synchronization**. Synchronizes files and folders located outside of users' profile folders.
- **Logging**. All entries in log files are identified with the user name, domain, and session id (where identifiable).
- **Multilingual profile support**. Uses language-independent profile folder names in the user store for Windows XP and Windows Server 2003.
- **Simplified installation and management**. Enhanced installation and administration features.
- **Consistent user settings**. Solves the "last-write-wins" problem that occurs when the last open session overwrites all of the profile data from previously closed sessions.
- **Easy integration**. Profile management can be integrated easily into existing deployments. No new infrastructure or changes to logon and logoff scripts are required.
- **Unified installer**. The same .msi file can be used for servers and desktops. There are two versions of the file, for 32-bit and 64-bit systems.
- **Active Directory-managed licensing**. You can manage user entitlement using an Active Directory user group.
- **Windows 7 support**. You can now manage profiles on user devices running Windows 7.
- **Integration with Citrix Receiver**. Profile management releases and upgrades can be managed using Citrix Receiver.
- **Improved monitoring and reporting**. Additional Performance Monitor counters allow you to measure several new aspects of logon and logoff, providing improved benchmarking and integration with Citrix EdgeSight.
- **Upgrades without .ini files**. A command line option allows you to exclude the Profile management .ini files from upgrades.

About Profiles

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.

Types of Profiles

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.

Version 1 and Version 2 Profiles

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. The folder structure (or namespace) of Version 1 profiles is mostly interchangeable; 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 Version 2 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 Version 2 profiles, seeht tp://download.microsoft.com/download/3/b/a/3ba6d659-6e39-4cd7-b3a2-9c96482f5353/M anaging%20Roaming%20User%20Data%20Deployment%20Guide.doc

General Recommendations for Profiles

Where network-based profiles are employed, Citrix generally recommends that the following solutions be considered in this order:

1. Mandatory profiles
2. Roaming profiles
3. Citrix user profiles

In all cases, folder redirection is encouraged so that user-specific data is saved separately from the profile.

Note that these are general recommendations only. Citrix recommends this order because administrators can generally implement one of the first two solutions and maintain them with standard knowledge of Microsoft Windows. However, in more complex situations or where these standard solutions cannot address enterprise requirements, Profile management should be considered.

Accessing Multiple Resources

Profiles become more complex as users access multiple resources. When network-based roaming or mandatory profiles are enabled, Microsoft Windows uses the registry data to describe and preserve the user environment. By default, Windows stores a copy of the profile on the local hard drive, loads a copy of the network-based roaming or mandatory profile when the user logs on, and writes the local copy to the network repository when the user logs off. However, in corporate environments, users may access multiple computers daily. Many users switch from a desktop to a laptop, while others use Citrix XenDesktop and Citrix XenApp to access virtualized resources. Depending on the enterprise requirements and configuration, there is likely a need for user data to move with the user as they log on to different computers.

For example, if a user has a local desktop that accesses virtualized applications hosted on XenApp and also accesses a virtualized desktop hosted on XenDesktop, the user settings will not be uniform across all resources unless appropriately configured. In addition, when accessing multiple resources, the behavior of roaming profiles dictates that the "last write wins".

As another 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 background color setting is not retained.

How Profile Management Works

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.

Note: Profile management processes domain user logons not local accounts.

For a more detailed overview of Profile management, see http://community.citrix.com/x/AoEAAg.

Profile Management Use Cases

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

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

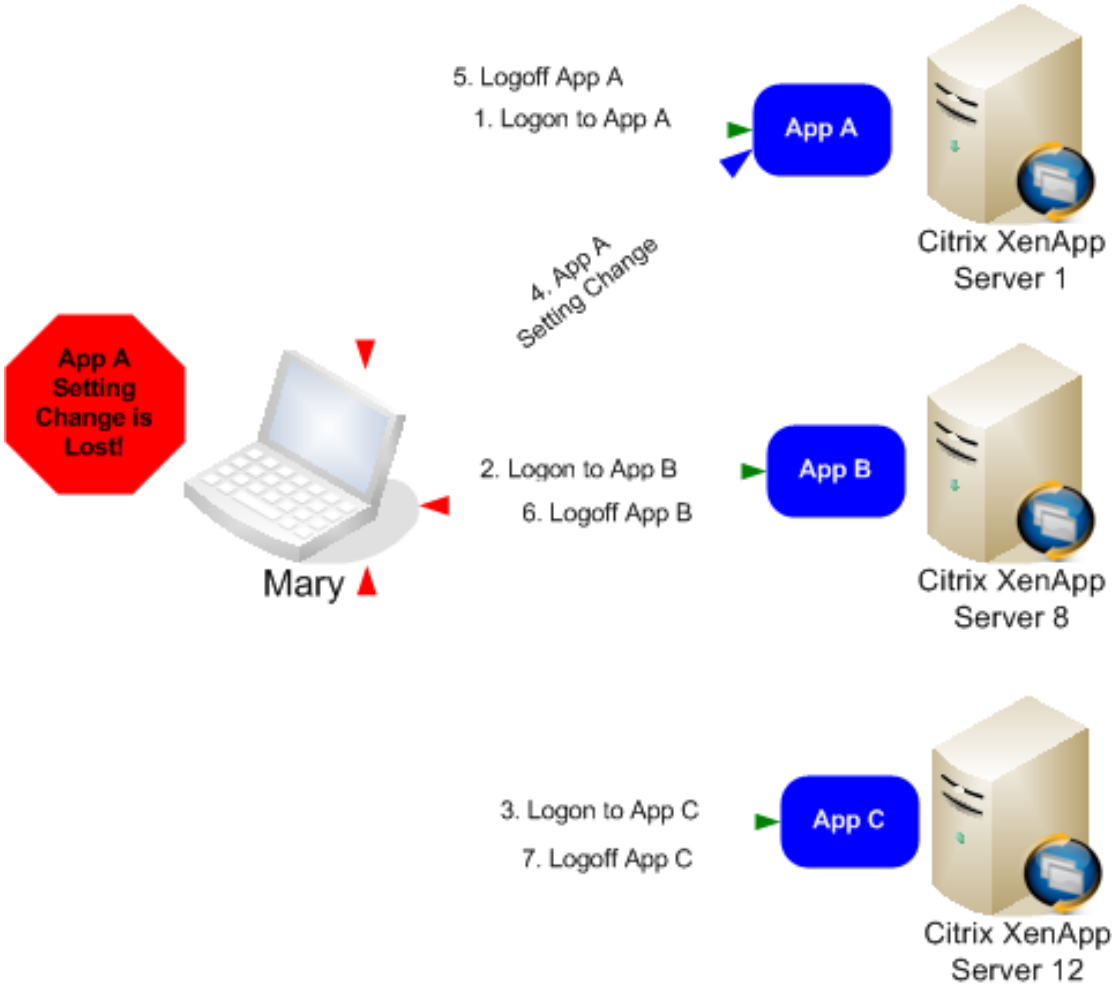
- **Multiple sessions**. The user accesses multiple XenApp server silos and therefore has multiple sessions open. Note however that application isolation and streaming on the server are alternatives to server silos. This scenario is described in more detail in this topic.
- **Last write wins and roaming 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.

Multiple Sessions

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.

Upon 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.

Last Writer Wins and Roaming Profile Consistency Issues

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 cause additional time for the user log on because the profile must be downloaded, the potential for consistency grows during the write phase of the user log off, 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 the profile for temporary data but do not ensure profile clean up upon application termination.

Known Issues in Profile Management 3.0

The following known issues exist in this version.

Installation Issues

If you change the default location of Profile management cache files, they are not deleted when you uninstall the component. [#226881]

On Windows Vista or Windows Server 2008, the log file directory is not deleted when Profile management is uninstalled. This issue does not occur when the component is removed in unattended mode. [#169/-]

If the path to the log file has been set to a non-default location in Group Policy or the .ini file, the file is not deleted when Profile management is removed. To workaround this issue, delete the log file manually. [#219376]

When installing Profile management with Group Policy, some properties of the Profile management MSI file are incorrectly displayed and the incorrect language version may be installed. The default language is shown as **German (Germany)**. In addition, no publisher information is displayed. As a workaround, edit the MSI. For example, open the MSI in Orca, click **View** > **Summary Info**, and in **Languages** remove all language IDs that are numerically lower than the language of the MSI you want to install. (German has the lowest ID.) Then proceed with your installation. [#229733]

Other Known Issues

A gpupdate has no effect on the synchronization of new folders located on volumes that have not been synchronized before. To work around this issue, ensure all users are logged off, restart the Citrix Profile Management service, and allow users to log back on. [#203859]

In Windows Performance Monitor, the log off counter is displayed as a number not as text. To work around this issue, read the four-digit number as Logoff Counter. [#201474]

Junction points and symbolic links appear not to be synchronized. If a user logs off, an error message such as the following may appear in the log file:

```
2009-01-12;12:01:45.231;ERROR;UPM;user5349;21;7468;FindFirstFileAPIWrapper: FindFi
2009-01-12;12:01:45.278;INFORMATION;UPM;user5349;21;7468;IsFSPathExcluded: Excludi
```

This is due to the fact that a junction point is accessed by another process. As junction points are not stored in the user store, this is only a cosmetic issue. Such error messages and can be ignored. [#204572]

Using extended synchronization in unsupported scenarios may result in data loss. This issue does not occur in the supported scenarios. [#216424]

Specific files and folders can be included and excluded from profiles. Inclusion and exclusion take place only at logoff, but log file entries make it appear they occur at logon. [#218834]

In Group Policy, you can change the location of the cache file used to monitor the Master File Table (MFT). The change is processed when policies are refreshed and take effect when the Citrix Profile Management service is next restarted. Changing the path when the Citrix Profile Management service is running has no effect, but the presence of log file entries may incorrectly give the impression that it does. [#218853]

If you set Profile management to synchronize Internet Explorer temporary cache files, some are not processed and the error is noted (as multiple error messages) in the log file. These errors can be ignored, and, because the files are temporary, the effect on the user is negligible. This issue is observed only with Internet Explorer and only in its cache folder (AppData\Local\Microsoft\Windows\Temporary Internet Files). To workaround this issue, exclude this directory from synchronization. [#218212]

When a user's domain password is about to expire on Windows XP Service Pack 3, they are prompted to change it. When they do, the system loads a local copy of the user profile (or the default user profile) instead of the Citrix user profile, the session may become disconnected, and the Citrix user profile data is not saved. To resolve the issue, apply Microsoft hotfix KB958058 to the XP SP3 base virtual disk image on the Citrix Provisioning Server with the disk in private image mode. This issue is limited to Windows XP Service Pack 3. For more information, see the Citrix blog article on this topic at http://community.citrix.com/x/aICcBg. [#218418]

Redirected folders, but not their contents, are created locally the second time a user logs on after enabling Profile management. Although redirected folders are synchronized locally, no redirected files are, so neither logon times nor the user experience is impaired. This issue does not occur until a second logon takes place. A workaround for this issue is available at http://blogs.technet.com/deploymentguys/archive/2008/05/01/dealing-with-duplicate-user-profile-links-in-windows-vista.aspx. [#229737]

In deployments involving XenDesktop 3.0 with virtual desktops shared between multiple users, some user profile changes are not saved at logoff (for example, changes to NTUSER.DAT or index.dat). This issue does not occur in deployments involving other versions of XenDesktop or with virtual desktops that are not shared. [#220044]

If you delete a local profile on Windows Vista or Windows 7, ensure you follow Microsoft best practice to delete the entire profile including the user-specific registry entries. For more information, see http://support.microsoft.com/kb/947215/en-us. Do not delete profiles manually, which can result in errors when users log on. The errors include failures to connect to Windows services. [#227506]

If streamed user profiles are enabled and the Citrix Profile Management service is stopped while files are being fetched from the user store, errors are written to the Windows event log and users are unable to access the files that have not been fetched. (Access is prevented for security reasons.) The workaround for this issue is to restart the service and then allow users to log off and log on again. [#227370]

Known Issues in Profile Management 3.1

The following known issues exist in this version.

Installation Issues

If you change the default location of Profile management cache files, they are not deleted when you uninstall the component. [#226881]

On Windows Vista or Windows Server 2008, the log file directory is not deleted when Profile management is uninstalled. This issue does not occur when the component is removed in unattended mode. [#169/-]

If the path to the log file has been set to a non-default location in Group Policy or the .ini file, the file is not deleted when Profile management is removed. To workaround this issue, delete the log file manually. [#219376]

When installing Profile management with Group Policy, some properties of the Profile management MSI file are incorrectly displayed and the incorrect language version may be installed. The default language is shown as **German (Germany)**. In addition, no publisher information is displayed. As a workaround, edit the MSI. For example, open the MSI in Orca, click **View** > **Summary Info**, and in **Languages** remove all language IDs that are numerically lower than the language of the MSI you want to install. (German has the lowest ID.) Then proceed with your installation. [#229733]

Other Known Issues

A gpupdate has no effect on the synchronization of new folders located on volumes that have not been synchronized before. To work around this issue, ensure all users are logged off, restart the Citrix Profile Management service, and allow users to log back on. [#203859]

In Windows Performance Monitor, the log off counter is displayed as a number not as text. To work around this issue, read the four-digit number as Logoff Counter. [#201474]

Junction points and symbolic links appear not to be synchronized. If a user logs off, an error message such as the following may appear in the log file:

```
2009-01-12;12:01:45.231;ERROR;UPM;user5349;21;7468;FindFirstFileAPIWrapper: FindFi
2009-01-12;12:01:45.278;INFORMATION;UPM;user5349;21;7468;IsFSPathExcluded: Excludi
```

This is due to the fact that a junction point is accessed by another process. As junction points are not stored in the user store, this is only a cosmetic issue. Such error messages and can be ignored. [#204572]

Using extended synchronization in unsupported scenarios may result in data loss. This issue does not occur in supported scenarios. For more information, see Supported Uses of Extended Synchronization. [#216424]

Specific files and folders can be included and excluded from profiles. Inclusion and exclusion take place only at logoff, but log file entries make it appear they occur at logon. [#218834]

In Group Policy, you can change the location of the cache file used to monitor the Master File Table (MFT). The change is processed when policies are refreshed and take effect when the Citrix Profile Management service is next restarted. Changing the path when the Citrix Profile Management service is running has no effect, but the presence of log file entries may incorrectly give the impression that it does. [#218853]

If you set Profile management to synchronize Internet Explorer temporary cache files, some are not processed and the error is noted (as multiple error messages) in the log file. These errors can be ignored, and, because the files are temporary, the effect on the user is negligible. This issue is observed only with Internet Explorer and only in its cache folder (AppData\Local\Microsoft\Windows\Temporary Internet Files). To workaround this issue, exclude this directory from synchronization. [#218212]

When a user's domain password is about to expire on Windows XP Service Pack 3, they are prompted to change it. When they do, the system loads a local copy of the user profile (or the default user profile) instead of the Citrix user profile, the session may become disconnected, and the Citrix user profile data is not saved. To resolve the issue, apply Microsoft hotfix KB958058 to the XP SP3 base virtual disk image on the Citrix Provisioning Server with the disk in private image mode. This issue is limited to Windows XP Service Pack 3. For more information, see the Citrix blog article on this topic at http://community.citrix.com/x/alCcBg. [#218418]

In deployments involving XenDesktop 3.0 with virtual desktops shared between multiple users, some user profile changes are not saved at logoff (for example, changes to NTUSER.DAT or index.dat). This issue does not occur in deployments involving other versions of XenDesktop or with virtual desktops that are not shared. [#220044]

If you delete a local profile on Windows Vista or Windows 7, ensure you follow Microsoft best practice to delete the entire profile including the user-specific registry entries. For more information, see http://support.microsoft.com/kb/947215/en-us. Do not delete profiles manually, which can result in errors when users log on. The errors include failures to connect to Windows services. [#227506]

History of Changes to Profile Management 3.x Documentation

This topic records the significant updates that have been made to the Profile management 3.x documentation. These include the addition of new information, the correction of ambiguities, and so on. Minor updates (such as typographical corrections, the reorganisation of existing topics, or the addition of links to other documents) are not listed.

Significant updates were made before this history started, so if you last viewed these topics before the first date listed below, you may want to review the entire set of topics for this release.

Tip: For a list of the most popular topics on administering Profile management, see Most Read Topics for Profile Management.

Date	New or Updated Sections or Topics
25 November 2010	Profile Management ADM File Reference About Extended Synchronization To manage cookie folders and other transactional folders
2 December 2010	Profile Management ADM File Reference
16 December 2010	High Availability and Disaster Recovery with Profile Management System Requirements for Profile Management: Store profiles on a single disk mounted by drive letter.
13 January 2011	To preconfigure Profile management with provisioned images
20 January 2011	Third-Party Directory, Authentication, and File Services
27 January 2011	To manage cookie folders and other transactional folders
3 February 2011	Profile Management ADM File Reference: **Process logons of local administrators** setting. Upgrading Profile Management and Migrating Profiles
3 March 2011	Collecting Diagnostic Information
17 March 2011	How Many Profiles Should I Create? Specific Troubleshooting Information: Printing.
14 September 2011	Decide on a configuration
17 September 2012	Decide on a configuration: UPMConfigCheck
19 September 2012	Collecting Diagnostic Information: CDFControl

Most Read Topics for Profile Management

These Profile management topics are the most commonly read ones. They contain answers to frequently asked questions and solutions to issues that you may encounter when installing or configuring this component:

- Profile management eDocs home page
- System Requirements
- Antivirus issues
- ADM and INI file reference
- Frequently asked questions about upgrades
- Extended synchronization
- Logon operations / Logoff operations
- Security

System Requirements for Profile Management

Systems running Profile management must be based on one of the following operating systems as a minimum:

- **Desktops**. Microsoft Windows XP Service Pack 3, Windows Vista Service Pack 1, or Windows 7
- **Servers**. Standard, Enterprise, and Datacenter Editions of: Windows Server 2003 Service Pack 2 and Windows Server 2008 (including Windows Server 2008 R2)

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 drive if preferred. For more information, see About the User Store.

Active Directory (AD) Group Policy Objects (GPOs) are used for configuration. AD forest functional and domain functional levels of Windows Server 2003 native mode and above are supported. For more information, see Domain and Forest Support in Profile Management. Alternatively, local .ini files may be used for configuration settings, but in general the .ini files should be used for testing purposes only. Note that settings in the .ini files 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 you are planning to use AD to deploy the installer, upgrade any domain controllers running the 64-bit edition of Windows Server 2003 Service Pack 1 to Service Pack 2 if you use them to store the Profile management ADM file. You do not have to upgrade the 32-bit edition.

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.

Make sure the change journal is set up on computers running the Profile Management Service. In addition, profiles on those computers must be stored on a single disk mounted by drive letter. This avoids the possibility of masking from the Service the profile that is intended to be monitored. This can occur when a disk is mounted into the folder used for profiles (for example, a disk is mounted into the C:\Users folder, which is a typical location for user profiles).

Before Installing on Windows XP and Windows Server 2003

Important: In addition to meeting the other system requirements in this topic, ensure the update described in Microsoft Security Bulletin MS09-012 is installed on all computers that will run Profile management. The update is included in recent operating systems; but it may have to be applied manually to others. The update is critical for Windows XP and Windows Server 2003 but should also be applied to any other supported operating system. For information about the update, see http://www.microsoft.com/technet/security/bulletin/MS09-012.mspx.

If you do not apply the update, Profile management installation ends prematurely and no components are installed.

Diagnostic Enhancements Feature

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.

Application Streaming

If you publish applications in Citrix XenApp to stream 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.

Planning Your Profile Management Deployment

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. As a guide to carrying out this important task, 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

Important: If you intend to use one of the .ini files (for example, UPMPolicyDefaults_V1Profile_en.ini) for evaluation purposes, rename the file (for example, to UPMPolicyDefaults_V1Profile_en.old) before you switch to using Group Policy 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.

For more information on .ini file deployments, see Considerations When Upgrading .Ini Files and Testing Profile Management with Local GPO.

Decide on a configuration

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

1. Is this a pilot or a production deployment?
2. Do you plan to migrate existing profiles or create new ones?
3. Are the profiles stored on a server or a workstation?
4. Is this deployment based on dynamically provisioned machines or persistent images (physical or virtual)?
5. Do the computers spend significant time disconnected from the network? This is generally true for mobile devices such as laptops.
6. Which applications are hosted on the computers?
7. Should local profiles be discarded at logoff?

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 Administering Profile Management.

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

- Reviewing and testing your configuration before putting it into production
- Troubleshooting

UPMConfigCheck

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.

Group computers into OUs

If your answers to the questions are the same for different sets of computers, consider grouping them into an Active Directory Organisational 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 or production deployment?

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.

Policy: Path to user store

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 is recommended for XenDesktop Quick Deploy scenarios. It 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 Sharing 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:

- About the User Store
- Creating the User Store
- To specify the path to the user store
- High Availability and Disaster Recovery with Profile Management

Policy: Processed groups

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** policy unconfigured; Profile

Management performs no checking on group membership and all users are processed. This option is recommended for XenDesktop Quick Deploy scenarios.

For more information on this policy, see To define which groups' profiles are processed.

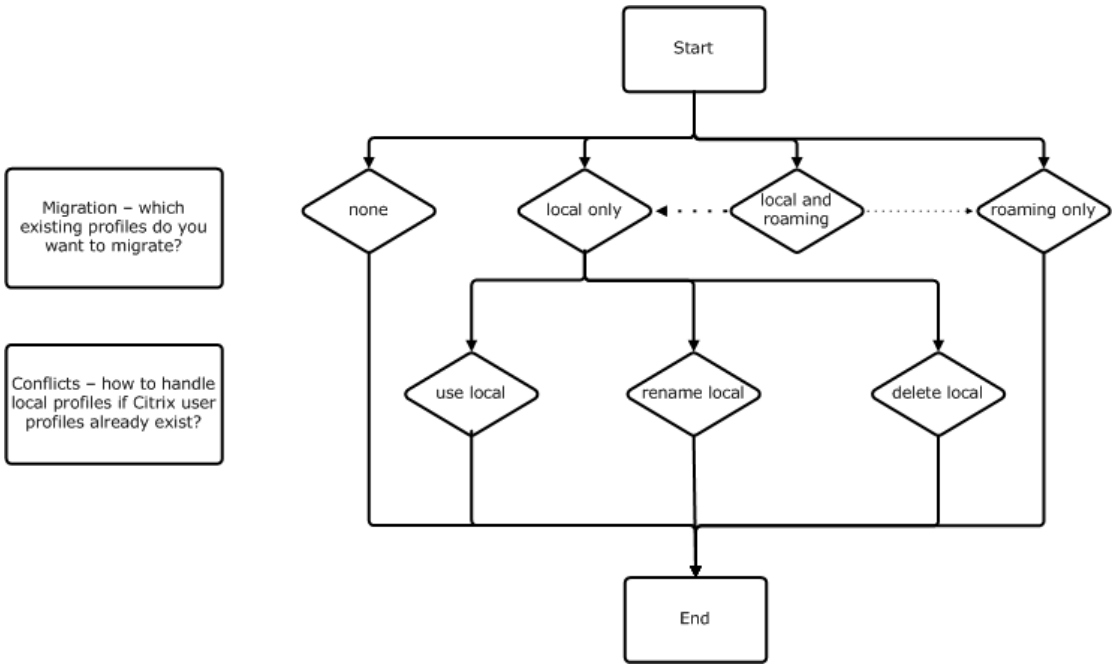
Important: In all cases you must ensure that the number of users processed by Profile management does not exceed the limits set by the relevant EULA.

Migrate or create profiles?

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.



Policy: Template profile

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 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.

XenDesktop Quick Deploy

For Quick Deploy scenarios, Citrix recommends setting:

- **Migration of existing profiles** to **Disabled**
- **Local profile conflict handling** to **Delete local profile**
- **Template profile** to **Disabled**

Server or workstation?

Are you deploying Profile management in a server environment, such as Citrix XenApp or Windows Remote Desktop Services, or in a workstation environment, such as Citrix XenDesktop or Citrix VDI-in-a-Box?

Policy: Process logons of local administrators

If this policy is enabled and you misconfigure Profile management such that users cannot log on, you must bypass Profile management to correct the problem. Members of the BUILTIN\Administrators group cannot do so because they cannot log on.

In server environments, users rarely need administrative rights and are therefore not members of the BUILTIN\Administrators group. They do not, for example, need to install applications on the server. Therefore, do not enable this policy in these environments. This allows administrators to log on and correct the problem.

In workstation environments, users generally need more control over virtual desktops than users accessing shared server-based resources. In some cases, users may need to be members of the BUILTIN\Administrators group. If so, follow the recommendations in Security Planning for XenDesktop and enable **Process logons of local administrators**. If the problem described above then occurs, temporarily disable this policy, correct the problem, then reenable the policy.

Policy: Profile streaming

Enable this policy if profiles cannot be cached locally between logons. Profile streaming tries to minimize the time spent copying files over the network by only copying placeholder files initially, then copying the data in the files only when it is explicitly accessed by an application.

Enabling **Profile streaming** is recommended in workstation environments except for those involving personal vDisks. In such cases, profile streaming is automatically disabled. This ensures that profiles are cached on those disks. (Profile management still synchronizes the profiles with the user store so that they are synchronized with any other desktops without personal vDisks and so that the profiles can be backed up.) Disabling this policy is recommended if profiles are cached locally in any other environment because it is generally faster to synchronize them with the user store.

Policy: Always cache

This policy modifies the behavior of the**Profile streaming** policy. It uses spare bandwidth to cache files locally in the background (even if they have not been requested by the system). This reduces logon times when large files are present in the profile.

Provisioned or Persistent?

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.

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 Citrix Provisioning Services or Machine Creation Services (or a third-party equivalent). Sometimes provisioned systems have persistent local storage; these are classed as persistent.

Several problems arise in a provisioned environment that affect the way Profile management is configured:

- Unexpected power loss results in the loss of all locally held user data.
- If there is a high dependence on storage technology, such as SANs, it is important to minimise Input/Output Operations Per Second (IOPS) to ensure best performance.
- Even planned power loss causes the system to revert to an earlier state, so Profile management itself cannot rely on persisting data across restarts. This includes its own configuration data.

For a procedure for configuring policies on provisioned systems, see To preconfigure Profile management with provisioned images.

Policy: Active write back

This policy is designed for provisioned systems, which generally store user profiles on a volatile disk volume. This means that changes are lost if a provisioned system is restarted for any reason (a power outage, scheduled maintenance, or an extended period of disconnection).

For provisioned systems, including those in Citrix VDI-in-a-Box deployments, enable **Active write back**. This safeguards file-writes to the profile. Profile management detects when an application has written and closed a file, and copies the file back to the network copy of the profile during idle periods.

However, Profile management does not copy any registry changes back to the network except during an ordered logoff, so there is a risk that application data in the registry does not match application data in the files. If this risk is important to you, consider redirecting the application folders instead; this method is particularly suitable for the Documents folder, for example.

For persistent systems, disable **Active write back.** A power outage is less likely to result in data loss in these systems, so disabling the policy is more likely to keep local and network copies of profiles consistent.

The best option for XenDesktop Quick Deploy scenarios is to disable the **Active write back** policy.

Timing of active write back operations

If there is no file activity for 10 seconds and active write back has not run in the last five minutes, Profile management copies files back to the network after that 10-second idle time. So, if a session has been idle for, say, 10 minutes, and a user changes a file, then 10 seconds later active write back is initiated and the file is copied back to the network. If I immediately change the file again and wait for 10 seconds, there is a delay until the next five-minute check (that is, 4 min 50 sec later). The five-minute delay between checks is not configurable.

Policy: Directory of the MFT cache file

The MFT file is an internal cache file used by Profile management to speed up processing of Change Journal notifications. By default, this file is created in the folder in which Profile management is installed. The file is of similar size to the NTFS MFT file (a special NTFS hidden file) and is accessed frequently in response to Change Journal notifications. Consequently, fast access is important for the good performance of Profile management, and the file should be in a location where the effect of network delays are minimized.

For provisioned machines, the MFT cache file must be quickly readable and ideally persistent; achieving this depends on the design of the machines and the location of the associated storage (for example, the SAN). For more information on locating the file in Provisioning Services deployments, see Profile Caching on vDisks.

For information on configuring the MFT cache file with persistent or physical machines, see *Non-provisioned Systems* in this topic.

Write Cache Options in Provisioning Services

When planning a Provisioning Services deployment, you must consider which write cache option is used. This is the location of the vDisk cache. For the good performance of Profile management, the order of preference for the write cache option, as it affects the location of the MFT file, is:

1. **Cache on device hard drive** (where there is a local physical disk)
2. **Cache on device hard drive** (where the local drive is provided by storage technology such as a SAN)
3. **Cache in device RAM**
4. **Cache on a server** (not recommended)

Cache in device RAM is relatively low on the list because Profile management does not need the high-speed access provided by a RAM cache, and a RAM cache uses machine resources intensively.

Encrypted and persistent options are supported but are not necessary for the correct operation of Profile management and may impair performance.

Important: Choosing **Cache on a server** is supported but impairs performance and is not recommended. For more information on write cache options, see the Provisioning Services documentation.

In all of these cases, set the **Directory of the MFT cache file** policy to **Not Configured**.

Machine Creation Services

There is no equivalent of write cache options in Machine Creation Services. Set the **Directory of the MFT cache file** policy to **Not Configured**.

XenDesktop Quick Deploy

For XenDesktop Quick Deploy scenarios, set the **Directory of the MFT cache file** policy to **Not Configured**.

Preparing Provisioned Images with Profile Management

When configuring Profile management on provisioned images, ensure the correct policies are present in the registry. For more information on this, see To preconfigure Profile management with provisioned images. Deleting the MFT file from the image before switching the image back to Shared mode can speed up logons.

Non-provisioned Systems

This case covers both persistent (physical) systems and any provisioned cases not already covered in this topic.

Locate the MFT cache file on a writeable part of the local hard disk. Additionally, set the **Directory of the MFT cache file** policy to **Not Configured**.

If the default location for the MFT file is not suitable because it is not writeable or because it is on a very slow device such as a volume on a network, set the **Directory of the MFT cache file** policy to a folder on a fast, writeable drive.

Mobile or static?

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.

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**

If **Offline profile support** is enabled, **Active write back** is honored but can only work when the computer is connected to the network.

The mobile case is not supported in XenDesktop Quick Deploy scenarios.

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.

The static case

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

Policy: Profile streaming

This feature sets **Profile streaming** differently depending on the XenDesktop environment, as described in Server or workstation?

For deployments not involving XenDesktop (for example, XenApp deployments), enable the **Profile streaming** policy. Setting this policy generally results in the lowest profile load time and therefore the fastest logon. 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. For exceptions relating to the presence of badly behaved third-party software, see Profile Streaming and Enterprise Antivirus Products.

In XenDesktop Quick Deploy scenarios, enable this policy.

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.

In XenDesktop Quick Deploy scenarios, set this policy to **Unconfigured**.

Policy: Always cache

For deployments not involving XenDesktop (for example, XenApp deployments), enable the **Always cache** policy. This is effective only if **Profile streaming** is also enabled. **Always cache** does not increase the logon times of streamed user profiles, but it increases the overall bandwidth used because over time the entire profile might be fetched (depending on the size threshold set). If this policy is not applied, files are fetched across the network only if an application tries to use them.

Also enable this policy in XenDesktop Quick Deploy scenarios.

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 Provisioned or Persistent?

Which Applications?

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 within the profile or outside it, and also in the registry or in the file system. You must balance the desire to let Profile management process those customizations stored outside the profile (by configuring items as included and excluded) with the need to keep the profiles small in order to minimize logon times.

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

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 Including and Excluding Items.

Legacy applications

Legacy applications are badly behaved; they store their personalization files in custom folders outside the profile. Subject to certain limitations, Profile management supports legacy applications through the combination of inclusions and exclusions. This requires you to specify absolute paths in any of these policies:

- **Directories to synchronize**
- **Files to synchronize**
- **Exclusion list - directories**
- **Exclusion list - files**
- **Folders to mirror**

The limitations are described in About Extended Synchronization.

Complex applications

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.

Java and Web Applications

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.

Summary of policies

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		
Folders to Mirror	Folder			Absolute	Relative
Process Internet cookie files on logoff					Flag

Wildcard processing in file names

Policies that refer to files (rather than folders or registry entries) support wildcards. For more information, see Using Wildcards in Inclusion and Exclusion Lists.

Inclusion and exclusion rules

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 Including and Excluding Items.

Non-English folder names in profiles

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.

Next steps

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 Administering Profile Management.

Keep or discard local profiles at logoff?

You can improve the performance of Citrix user profiles across your network by correctly setting the way that the profiles are stored locally, depending on your deployment type and the network's availability.

If a profile is not fully cached at the end of a session, the locally cached portion of the profile is saved as a set of reparse points (uniquely named collections of user data that Profile management can interpret and load later). The reparse points are deleted and recreated when the user next logs on. This causes an increase in input and output operations (known as IOPs) on the network.

Use the rest of this topic to decide whether increasing the IOPs is really necessary in your deployment.

Policy: Delete locally cached profiles on logoff

It is always safe to enable this policy (and delete locally cached profiles when users log off) because each user's complete profile always exists in the user store. However, Citrix certainly recommends enabling this policy if any of the following apply:

- Servers are persistent and accessed by many users, such as in Citrix XenApp or Microsoft Remote Desktop Services deployments. You want to delete the profiles on logoff to avoid lots of stale profiles proliferating on the servers. (The WMI or CIM object repository also fills up.)

  Note: Alternatively, to remove the stale profiles you can disable this policy and instead use a profile deletion tool such as Microsoft Delprof.exe or Sepago Delprof2 from a script when a machine is restarted.

- You use virtual desktops that are shared by multiple users, such as in Citrix XenDesktop deployments that involve pooled machine catalogs. Deleting profiles in this case ensures an individual's private profile data is not shared with other users.

Citrix recommends disabling this policy if any of the following apply:

- You use virtual desktops that are reset at logoff (a XenDesktop or Citrix VDI-in-a-Box use case). Enabling the policy would create unnecessary IOPs caused by Profile management deleting reparse points.

- Virtual desktops are not reset at logoff but are assigned to a single user (a XenDesktop use case). Logons will be faster if their profile is cached on a local, persistent disk, not the virtual desktop.

- Servers are accessed by just a few users (a XenApp or Remote Desktop Services use case with, for example, a small departmental server). The servers must have a persistent disk that is large enough to store the users' profiles.

- Profiles are stored on a personal vDisk (a XenDesktop or VDI-in-a-Box use case). In this case, Profile management does not need to be involved in handling the profiles.

- Your network's availability is limited.

Review, test, and activate Profile management

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.

Policy: Enable Profile management

Until you enable this policy, Profile management is inactive.

Plan for multiple platforms

Why are user profiles on multiple platforms such a challenge?

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.

How does changing the way an application is installed cause issues?

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

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

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.

How Many Profiles Should I Create?

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 for user accounts that have been removed from Active Directory.

Sharing Citrix User Profiles on Multiple File Servers

The user store can be located across multiple files servers, which has benefits in large deployments where the number of 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 .

For more information on using variables when specifying the path to the user store, see To specify the path to the user store and Administering Profiles Within and Across OUs.

Administering Profiles Within and Across OUs

Within OUs

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 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.

To manage different computers with different OSs using a single GPO in a single OU, you can implement a system environment variable and incorporate it 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 `XP` for your Windows XP 32-bit computers and `XPx64` for your Windows XP 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 are 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

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

Across OUs

You can control how Profile management administers profiles across OUs. Depending on your OU hierarchy, one OU may inherit policies from another. You can create policy settings in a separate Group Policy Object linked to the affected OU to override the inherited policies.

Domain and Forest Support in Profile Management

Domain and forest functional levels of Windows Server 2003 or later are supported by Profile management. This includes a Windows Server 2008 domain controller running in mixed mode at a domain or forest functional level of Windows Server 2003. Older operating systems are unsupported.

The use of system environment variables can help to disambiguate usernames in multiple domains. For information on this, see Administering Profiles Within and Across OUs.

High Availability and Disaster Recovery with Profile Management

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.

Comparison with Roaming Profiles

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:

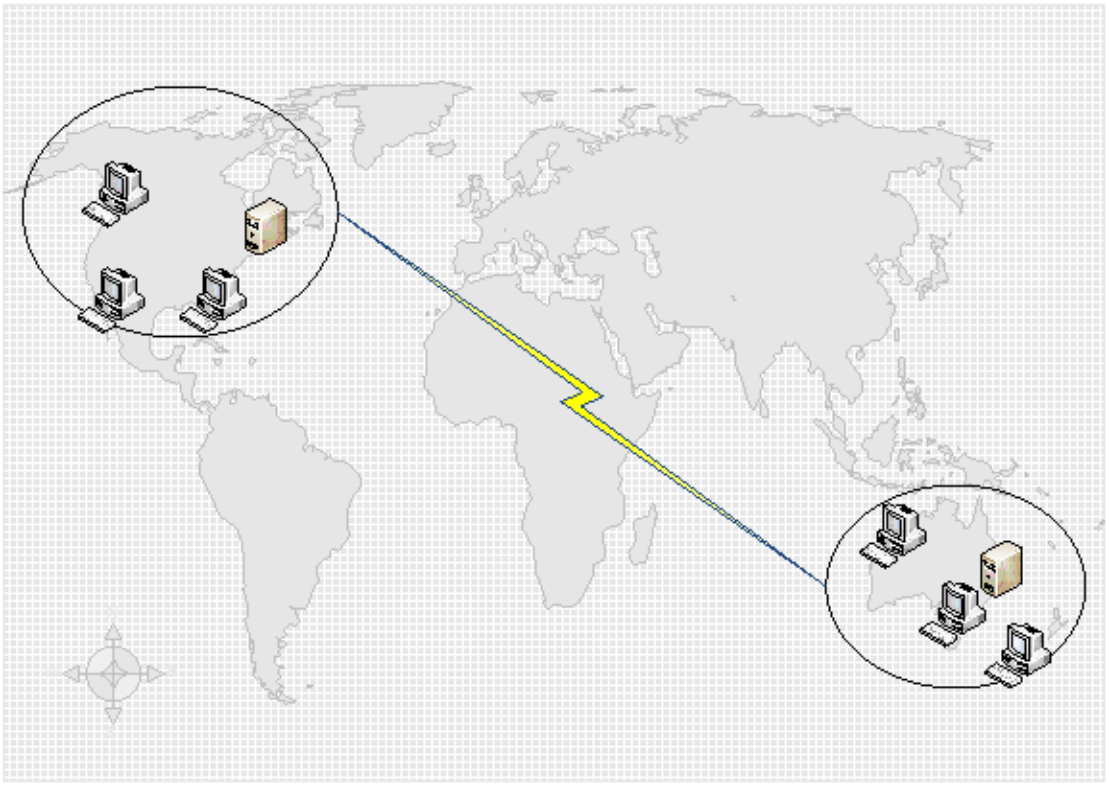
- Profile management support is limited to the scenarios where roaming profiles are also supported. For more information about this, see "Can I use DFS with Offline Files and redirected My Documents folders?" at http://technet.microsoft.com/en-us/library/hh341474(WS.10).aspx.
- The cache option for offline 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

“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).



Option 1 – DFS Namespaces

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

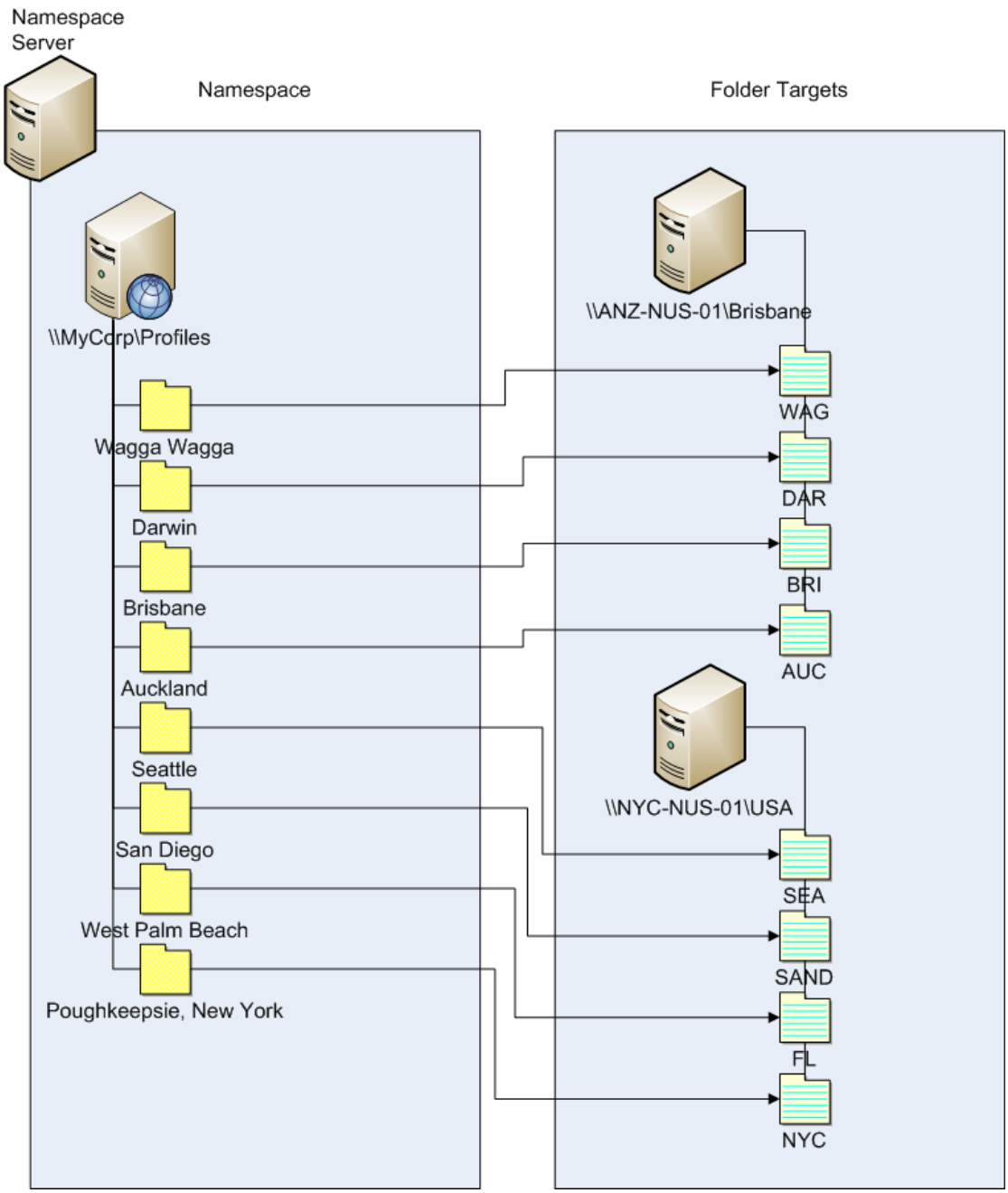
DFS Namespaces can resolve some of the issues presented in the blog article.

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.

Option 2 - DFS Namespaces with Failover Clustering

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

"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.

Option 1 - Referrals to Multiple Folder Targets

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 not supported.

Option 2 - Distributed File System Replication

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.

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.

Important: Distributed file locking is not supported by DFS Replication.

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

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

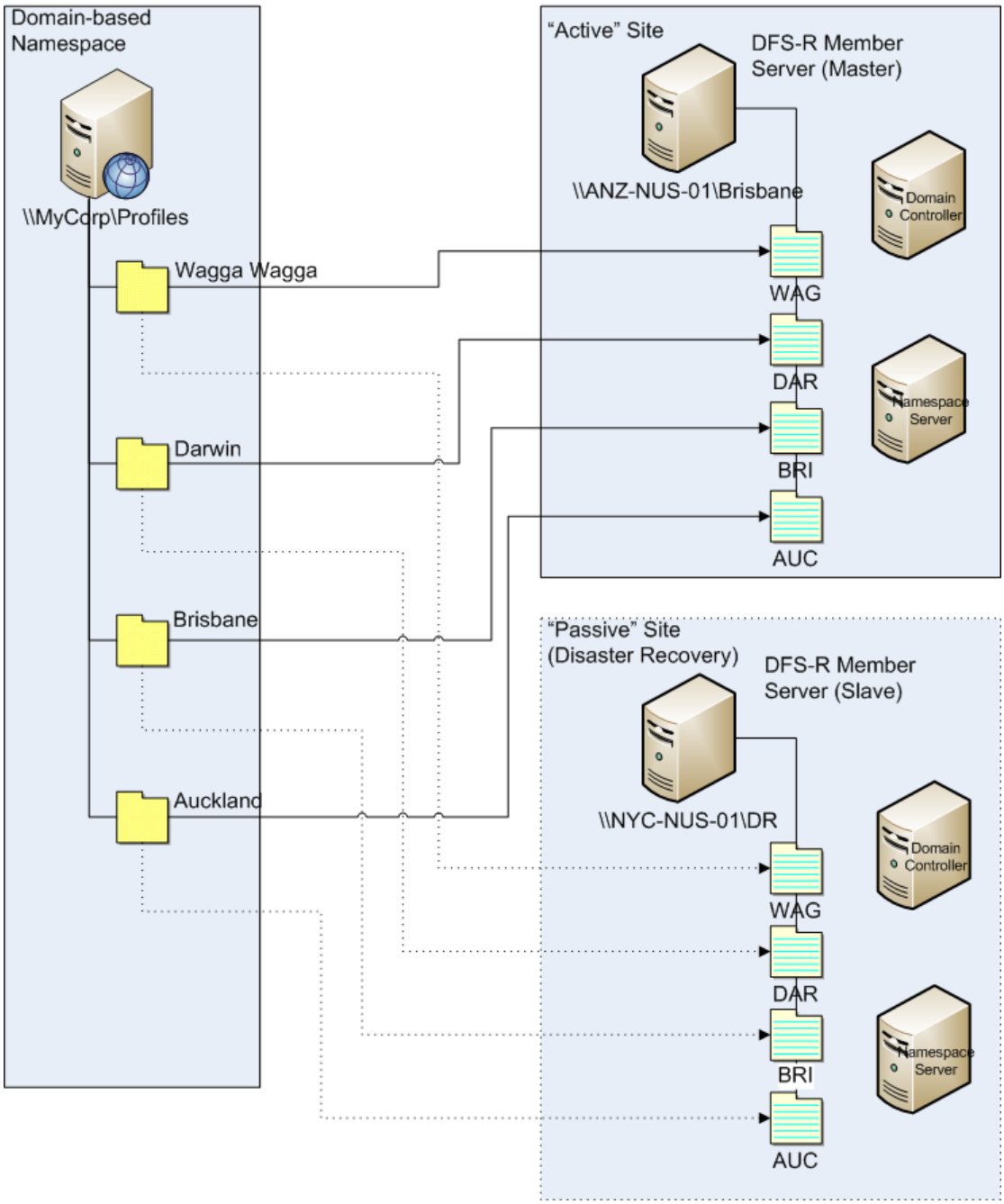
The key features required for disaster recovery (DR) are supported by Profile management:

- **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

“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

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

Background Reading

- 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://community.citrix.com/display/ocb/2009/07/21/Profile+Management+-+Load+Balancing+User+Stores.

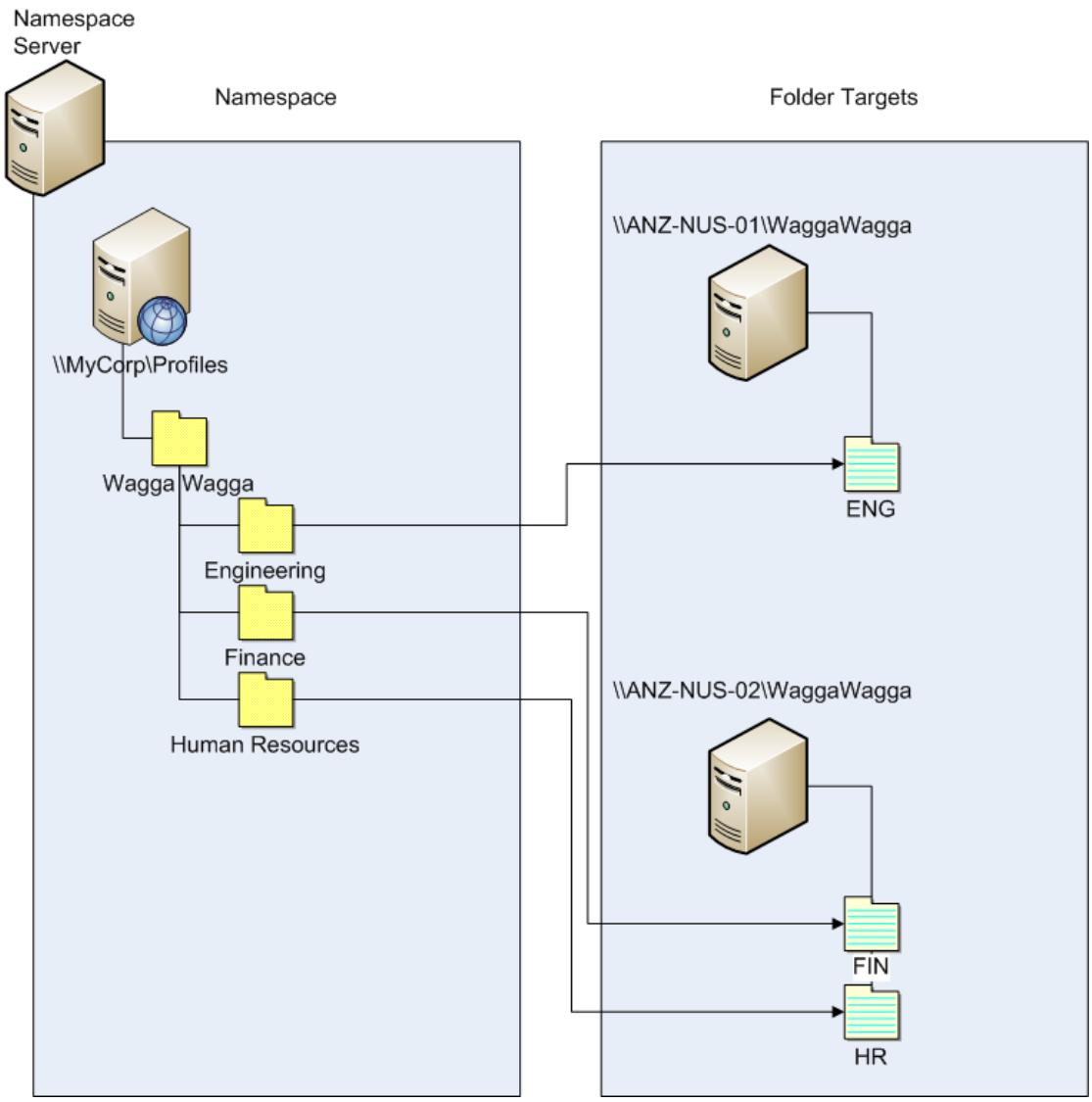
Unlike Scenario 1, this scenario has a single site that is large enough to require multiple NUSs. Using DFS namespaces, we can improve on the solution in Scenario 1.

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.

Planning Folder Redirection with Profile Management

Profile management works with folder redirection and is encouraged. Active Directory allows folders, such as Application Data or Documents, to be saved (redirected) to a network location. Thus, the contents of those folders are stored in the designated location and not included within the user profile, which reduces its size. Depending on the version of Active Directory in use, the specific folders that can be redirected vary.

In addition, where mandatory profiles are employed, configuring folder redirection allows users to save some settings, files, and other data while still enabling the benefits of mandatory profiles. 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.

Note: Active Directory based on Windows Server 2008 allows for folder redirection of additional folders not included within Active Directory based on Windows Server 2003.

Not all folders which can be redirected are directly accessible via Active Directory. All folders which can be redirected on a specific operating system can be found in the registry under HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders.

Important: To configure folder direction successfully, you need to be aware of the differences in folder structure between Version 1 and Version 2 profiles. For more information, see Version 1 and Version 2 Profiles.

Depending how you choose to set up folder redirection, you must configure Profile management appropriately.

For additional security considerations when using folder redirection, see Securing Your Profile Management Deployment and the article called *Configuring Folder Redirection* on the Microsoft TechNet Web site, http://technet.microsoft.com.

Third-Party Directory, Authentication, and File Services

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

Directory Services

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.

Authentication Services

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

File Services

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 Using Profiles On Multiple Platforms

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.

Profiles on Multiple Platforms

Why are user profiles such a challenge?

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.

How can I be certain of avoiding compatibility issues with my profiles?

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 dissimilar systems as well as you can by adjusting the user profiles so that, when profiles roam, any issues are handled properly or to the extreme where settings are 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.

Can I share profiles across different systems?

Citrix recommends having one profile for each platform. This is not necessarily the same as one profile per operating system. For more information on this recommendation, see How Many Profiles Should I Create?. 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. This means you must exclude those settings for all devices sharing profiles. If you restrict your profile to similar systems by following the Citrix recommendation, this type of issue will less likely occur.

Does Citrix support profiles across multiple versions or platforms?

The ability to support these types of scenarios is limited by the degree to which Microsoft can support profiles across platforms. The links in the next question cover their position and best practices.

How do Microsoft support roaming profiles across platforms and versions?

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.

Is sharing a profile between x86 and x64 platforms possible?

Sharing profiles between OS versions of different bitness is not recommended. Sharing one profile between Windows x86 and x64 might work, but some issues are likely.

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.

I want to test how one profile behaves across multiple platforms. Where do I start?

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, Favorites, Cookies
- 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

Items that will not work:

- Shared settings between Version 1 profiles (for example, Windows XP) and Version 2 profiles (for example, Windows 7). Such settings include wallpaper, which is stored in different formats on the two profile versions.

What issues are likely to occur?

Typical issues 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 not installed the same on different systems (for example, applications installed on a C: drive on one system and D: on another, applications

installed under C:\Program Files and C:\Program Files (x86), or Excel add-ins installed on one platform 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.

How does changing the way an application is installed cause issues?

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

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.

By default, the content of the Start menu folder is not saved by Profile management because links pointing to executables are often computer-dependent. In addition, links that are language-specific lead to multiple Start menu entries for the same application. Furthermore, links pointing to documents may not be valid on other machines because the path to the document is relative to another system, or it is a network path that is inaccessible.

Note: Interesting 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.

So again, the rule is always to test and verify.

The Quick Launch Toolbar

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, add the following entries to the folder exclusion list:

- Windows XP or Windows 2003: Application Data\Microsoft\Internet Explorer\Quick Launch
- Windows 7 or Windows 2008: AppData\Roaming\Microsoft\Internet Explorer\Quick Launch

Can I assign profiles based on the computer a user logs on to?

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 XP, Profile management has a Group Policy (GP) setting that has an option to assign a profile to a specified computer. Because it is based on GP, the profile is defined by the OU in which the computer is located.

Windows 7 has a computer setting in GP to assign a profile based on computer. Again, because this is based on GP, the profile assignment depends on the location of the computer's OU container to which the GPO is applied.

Why are profile assignments based on computer desirable?

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.

Migrating Profiles

Does Profile management migrate Windows user profiles to Citrix user profiles?

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. You configure this behavior using the .ini file or Group Policy Object (GPO).

For information about planning and setting up your Profile management migration, see CTX119466.

Which profiles can be migrated to Citrix user profiles?

Profile management can migrate Windows local and roaming profiles. Mandatory profiles (.man profiles) are ignored by Profile management. To ensure Profile management works correctly, deactivate the assignment of mandatory profiles to all users.

The next question covers how you use your existing mandatory profile as a template profile in Profile management.

How do I use a template 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 created for the first time receives the Default User profile of the Windows device they log on to. This may acceptable, and it means any variation in different devices' Default User profiles results in differences in the base profile created for the user. This means you can regard the template profile feature as a Global Default User profile.

For more information, see To specify a template profile.

Troubleshooting Profile Management

This topic describes the settings in Group Policy (GP) that control how Profile management stores log data. In addition, the checklists and other troubleshooting advice in this section of eDocs are designed to help you identify and solve issues. Note that, in many cases, issues result from components other than Profile management or from a misconfiguration of the environment.

Important: 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.

UPMConfigCheck

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.

Policy: Enable logging

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.

Policy: 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 **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.

Policy: 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.

In XenDesktop deployments that use Machine Creation Services be aware of the persistent folder that imposes a 15 MB limit on log files (not just Profile management ones). To allow for this, 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; 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 1 MB 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.

Policy: Path to log file

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, you must 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, note the following:

- 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.

- 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.

Some logon and logoff processing is done in the context of the user using impersonation. Citrix recommends that you grant write permissions on the log folder for the users group so that Profile management can write to the log files during impersonation.

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**, which is described above.

Basic Troubleshooting

As a first step in troubleshooting any issue that you or your users experience, follow these steps:

1. Check the configuration .ini file on the affected user device.
2. Check the settings in Group Policy (GP).

   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.
3. Check the HKLM\Software\Policies registry entry on the affected device to see if there are any stale policies due to GP tattooing issues, and delete them.
4. 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.

Specific Troubleshooting Information

Slow Logons

For information about known issues with slow logons and workarounds, see CTX101705.

Installation on Windows XP or Windows Server 2003 Fails

Profile management installation ends prematurely and no components are installed on the target computers.

This situation may occur if the required Microsoft MSI update is not present on the computers. It is especially likely to occur on new Windows XP and Windows Server 2003 systems where no Windows patches have been applied, and on existing systems running these operating systems where automatic updates are disabled.

To correct this issue, apply the Microsoft update described in Microsoft Security Bulletin MS09-012, and then install Profile management. For information about the update, see http://www.microsoft.com/technet/security/bulletin/MS09-012.mspx.

Checking That Profiles Are Being Streamed

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 rea
   ```

   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;ProcessLog
   ```

   If streamed user profiles are not being applied, the item reads `ProcessLogon: User logging on with Streamed Profile support disabled.`

Problems With Streamed User Profiles and Antivirus Products

If you use enterprise antivirus products and encounter issues such as logons hanging or taking a very long time, consult the troubleshooting information in Profile Streaming and Enterprise Antivirus Products.

Determining Which Policies Are In Force

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.

Excluding Corrupt Profile Data

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.

Cleaning Connections to Registry Entries

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. For more information on this tool, see http://www.microsoft.com/downloadS/details.aspx?FamilyID=1b286e6d-8912-4e18-b570-42470e2f3582&displaylang=en.

Deleting Local Profiles

If you delete a local profile on Windows Vista or Windows 7, ensure you follow Microsoft best practice to delete the entire profile including the user-specific registry entries. Do not delete profiles manually, which can result in errors when users log on. For more information, see http://support.microsoft.com/kb/947215/en-us.

Deleting Locked, Cached 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.

Identifying Where Profiles Are Stored

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.

Checking Servers

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 3.0, the entry would be:

```
[LastUpdateServerName]
3.0=<computer name>
```

Rolling Back to Version 2.1

You can roll back to a Version 2.1 deployment if Version 3.0 has been deployed too early. See Managing Multiple Versions of Profile Management for the reasons this might happen.

Run the following PowerShell command on the file server that hosts the user store. This deletes the file PmCompatibility.ini in each profile in the user store:

```
Get-ChildItem LocalPathToUserStore -include pmcompatibility.ini -recurse | foreacl
```

After the command has completed, users can log on to computers running Version 2.1 and receive their profile from the user store.

Profile Management Running on VMware Creates Multiple Sequential Profiles

For information about this issue and how to resolve it, see CTX122501.

Long Logon Times With Novell eDirectory

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 in User Store

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.

Missing Information In Log File

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.

GPO Settings Inoperative

I changed a setting in my GPO 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 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.

Users Receive New Not Cached Profiles

If a user is running Citrix Presentation Server Client 10.200 for Windows or later on Windows XP, at logon their cached profile is not loaded. Instead, a new profile is created. For more information about and a workaround for this issue, see CTX118226.

Profile Data Lost When XenDesktop Sessions Become Unresponsive

In a XenDesktop deployment, disconnecting from a Remote Desktop Protocol (RDP) session can cause a Citrix Virtual Desktop Agent running on Windows XP 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 Virtual Desktop Agent Version 3.1.3242 and later.

Users Cannot Log On (Event ID 1000, Source Userenv)

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 and workarounds for this issue, see CTX105618.

Printing

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 disk in standard 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 http://forums.citrix.com/thread.jspa?threadID=283076&tstart=0.

Collecting Diagnostic Information

This topic guides you through the steps involved in collecting information that can help diagnose problems with the operation of Profile management. Before following these instructions, make sure you can reproduce the problem.

1. Edit the Profile Management Group Policy Object (GPO) in the Group Policy Management Editor, or edit 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:

    - Turn on **Enable logging**.

    - Select all of the events in **Log settings**.

    - In **Maximum size of the log file**, consider increasing the value to 5MB or more if you have sufficient disk space. There are some consequences associated with increasing the log file size; for information on this, see Profile Management ADM File Reference.

3. Run gpupdate /force on the server or desktop, and ideally restart the Profile Management Service. You must restart it if you are using an .ini file.

4. If requested by Citrix Technical Support, collect a diagnostic trace log (available in Profile management 3.x or later) using the instructions in Other Troubleshooting Steps.

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, and PmCompatibility.ini. The .ini files are located in the root folder of each Citrix user profile in the user store.

Note that 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 with provisioned images.

To obtain diagnostic information with CDFControl

CDFControl is an event tracing controller and consumer that captures Citrix Diagnostic Facility (CDF) trace messages from various Citrix tracing providers, including those in Profile management. Only use CDFControl if you are asked to do so by Citrix Technical Support. For information on this tool, see CTX111961.

Examining the Profile Management Log File

After performing the basic troubleshooting steps, check the Profile management log file as follows. Log file entries are a good starting point when troubleshooting.

Citrix UPM Log Parser is available as a free download from the Citrix Support Web site. You may find this tool helpful when analyzing log files. For information about it, see Log Parser for Citrix Profile Management.

1. Make sure that logging is activated.
2. Check the log file for errors. You can locate these by searching for the word ERROR.
3. Check the log file for warnings. You can 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 Other Troubleshooting Steps.

Log Parser for Citrix Profile Management

Citrix UPM Log Parser 1.0 is designed to help analyze the log files generated by this component. No data is modified by this tool.

To install UPM Log Parser

1. Download the package from http://support.citrix.com/article/CTX123005.
2. Extract the contents of the zip file to a folder.
3. Run CitrixUPMLogParser.exe.

To remove UPM Log Parser

1. Delete CitrixUPMLogParser.exe from the computer it is installed on.

Security Permissions Required by UPM Log Parser

If you want to access the log files on a remote computer, you must have the required remote access rights to the computer's registry and file system (through the admin share).

To use UPM Log Parser

1. Run CitrixUPMLogParser.exe.

2. Enter the name of the remote computer on which the log file you want to examine is located. If the computer is reachable, the tool tries to locate UserProfileManager.log in <systemroot>\system32\LogFiles\UserProfileManager.

   The first error in the file is selected and information about the event is displayed. The logging level, the Windows version and service pack, and the Profile management version are also displayed if this information is contained in the log file.

   Errors are highlighted in red, logon events in green, logoff events in blue, and Profile Management Service start and stop events in gray.

   Note the following about how log files are located by the tool:

   - If the log file cannot be found, the tool uses the location in HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\UserProfileManager\PathToLogFile to retrieve the log file location. (The location is configurable using GPO or the .ini file.)

   - If no machine name is specified, the local computer is used and you are prompted for a log file.

   - If the remote computer cannot be pinged, the tool displays an error and prompts you to enter another computer name.

   - If the remote computer responds to ping requests but cannot be accessed, the local computer is used instead.

3. Use **Find** to search the log file and optionally filter by information type and event type.

   Press **F3** to move to the next matching item.

4. When you have finished examining the current log file, click **Close Log File** before opening another one.

Advanced Troubleshooting of Log Files

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 deactivated 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
   - 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
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 all Profile management .ini files.
8. Using **My Computer** > **Properties** > **Advanced**, delete all profiles except those you want to test. Research any errors that appear.
9. Give the Authenticated Users group full control of the log file, c:\Windows\System32\LogFiles\UserProfileManager.log. This allows you to check the file when logging in as a user without logging off.
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:
    a. **Enable Profile management**.

b. **Path to user store**.

c. **Enable logging**.

d. **Log settings**. Scroll to select all settings in this section of the ADM file.

e. **Migration of existing profiles**. Select **Roaming and local profiles**.

f. **Local profile conflict handling**. Select **Rename local profile**.

g. **Delete locally cached profiles on logoff**.

Disable the setting **Process logons of local administrators**. This helps when troubleshooting because, if Profile management accidentally prevents end-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.

Events Logged by Profile Management

The following events are logged by Profile management and 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**.

In this table, causes and suggested actions for resolution are included for each event. Long event descriptions are truncated with elipsis (...)

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.
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: The CJ notification event could not be opened...	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	The CJ notification event could not be set to the signaled state...	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.

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: Unable to query the journal...	The Citrix Profile management service 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.	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.
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 will not complete processing on this folder. Back up critical data manually.	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.
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.	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.

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.
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.

Other Troubleshooting Steps

Once you have followed the basic troubleshooting steps to try and correct the 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**.

  If you are not using the latest version, upgrade.
- Check the support forum at http://support.citrix.com/forums/forum.jspa?forumID=185. Someone else may already have encountered the problem and solved it.
- Enable user environment debug logging (available on Windows XP and Windows Server 2003). Instructions on this are provided at http://support.microsoft.com/kb/221833/. The user environment debug log contains a lot of information about the logon process.

  Analyze the output file. Help with analysis is available at http://technet.microsoft.com/en-us/library/cc786775.aspx.
- Try to reproduce the issue you are observing on a clean computer with the same operating system as the affected computer. Ensure the clean computer only has the operating system and Profile management installed.

  Install the software products that are present on the affected computer one by one and see if the issue is reproduced after each installation.

To create a diagnostic trace log

This topic contains instructions for using the diagnostic enhancements feature, which 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 http://support.citrix.com/article/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 used.

   - **UPM_DLL_Perfmon**. This allows you to trace Windows Performance Monitor counters associated with and errors generated by Profile management.

   - **UPM_Driver**. This records each time the Citrix streamed user profiles driver is used.

3. Complete the remaining steps in article CTX104578.

To produce a session dump file

You can save Profile mangement'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.

To set Microsoft NT Symbolic Debugger as your default Windows postmortem debugging tool

For information about setting NT Symbolic Debugger (NTSD) as your default Windows postmortem debugging tool, see CTX105888.

Contacting Citrix Technical Support

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 information. Always include the following files and as much other information as possible:

- All Profile management log files (in %SystemRoot%\System32\Logfiles\UserProfileManager). Be sure you have all log settings activated.

  A log file 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
- 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.
- 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.
- If available, the session dump file.

Securing Your Profile Management Deployment

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 Security Recommendations for Roaming User Profiles Shared Folders 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.

Permissions

The minimum access permissions that Citrix recommend for the user store are:

- Full control of the user store root folder
- The following NTFS permissions:

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 user store, 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.

Citrix also recommends that you grant write permissions on the log folder for the users group so that Profile management can write to the log files during impersonation.

If you use a template profile, users need read access to it.

ACLs

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.

Profile Streaming and Enterprise Antivirus Products

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

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.

Troubleshooting

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.

Installing and Setting Up Profile Management

Install Profile management on each computer whose user profiles you want to manage.

Typically, you install the Profile management software on computers using a distribution tool, an imaging solution, streaming technology, or Citrix Merchandising Server. You can also install it directly on any computer using one of the installers in the download package.

Unattended installations are supported.

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

Installation 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.

Files Included in the Download

The following files are included in this release.

File Name	Description
One of the following depending on the version you download: Profilemgt3.0.0_x86.msi, Profilemgt3.1.0_x86.msi, Profilemgt3.1.1_x86.msi, or Profilemgt3.2.0_x86.msi	Installer for 32-bit systems
One of the following depending on the version you download: Profilemgt3.0.0_x64.msi, Profilemgt3.1.0_x64.msi, Profilemgt3.1.1_x64.msi, or Profilemgt3.2.0_x64.msi	Installer for 64-bit systems
One of the following depending on the version you download: Ctxprofile3.0.0.adm, Ctxprofile3.1.0.adm, or Ctxprofile3.2.0.adm	ADM file used in Group Policy. Ctxprofile3.1.0.adm is used with Version 3.1.1 in addition to Version 3.1.
welcome.html	List of documentation resources

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

File Name	Description
UPMPolicyDefaults_V1Profile_en.ini	.Ini file for English Windows XP and Windows 2003
UPMPolicyDefaults_V2Profile_all.ini	.Ini file for Windows Vista, Windows 7 and Windows Server 2008
UserProfileManager.exe	Windows service carrying out functions on computers managed by Profile management

Testing Profile Management with Local GPO

Before deploying Profile management in a production environment, Citrix recommends using a test environment. While you can create this setup on a local machine with the supplied .ini files, 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.

For testing purposes, consider using a Windows Management Instrumentation (WMI) filter to temporarily restrict your configuration to just one machine in an OU.

Important: For these reasons Citrix does not recommend the use of local GPOs as a long-term, enterprise solution.

Testing the User Experience

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

Testing Operating System Variations

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.

To install Profile management

Install the software on all computers whose user profiles you want to manage. This procedure installs Profile management on a single computer.

If you perform the installation on Windows XP or Windows Server 2003 and have disabled support for short file names (also known as 8.3 file names), each folder in the installation location must conform with the short file naming convention, for example C:\Citrix\ProfMgr. This issue does not occur on other supported operating systems.

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.

To install Profile management from the command line

Important: In this version of Profile management, the following keys have been 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 files 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.

1. At a command line, run the following command:

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

This command performs the installation without displaying a user interface and then performs a restart.

Optionally, you can suppress the restart using the `/norestart` option, but, depending on the operating system, Profile management will not function until the computer has restarted. For example, you do not need to restart user devices running Windows Vista.

`INSTALLDIR` can be user specified.

For information on the `OVERWRITEINIFILES=yes` option, see Considerations When Upgrading .Ini Files.

Setting `INSTALLPOLICYINIFILES` to `no` prevents the installation of Profile management .ini files. If you have used the .ini files with a previous version of the software and want to continue to use the settings contained in them 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.

Deploying Profile Management with Citrix Receiver

You can use Citrix Receiver and Merchandising Server (components of the Citrix Delivery Center solution) to distribute Profile management MSI packages. No configuration of Profile management is required to do this. For instructions on deploying components this way, see the Citrix Receiver documentation.

To add the ADM file to Group Policy

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 Upgrading 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 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 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 files instead of the .adm file. If, after successful testing, you move from .ini files to an AD deployment, be sure to add to the .adm file any required inclusions and exclusions in addition to the minimum defaults that are documented in To set default inclusions and exclusions.

1. On the domain controller, import the Profile management .adm file from the download package. The file is located in the Group Policy Templates folder.

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 Administering 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 users.

5. Edit the GPO in Group Policy Editor:

   a. Expand **Computer Configuration** and right-click **Administrative Templates** under the GPO.

   b. Click **Add/Remove Templates** and click **Add.**

   c. Browse to the .adm file that you copied locally and click **Open.**

   d. Click **Close**. This creates a Citrix folder and a Profile Management subfolder that stores the settings from the .adm file.

To remove Profile management

This procedure removes Profile management from a single computer.

1. From the list of installed programs in **Add or Remove Programs** (on Windows XP) or **Programs and Features** (on Windows Vista), select **Profile management** and click **Remove** (XP) or **Uninstall** (Vista).

2. Click **Yes**.

3. Restart the computer.

You can also remove Profile management in unattended mode.

Upgrading Profile Management and Migrating Profiles

This section contains procedures for upgrading Profile management software and information about transitioning your existing Windows user profiles to Citrix user profiles. As a prerequisite, read Planning for Migration and Conflicts.

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.

For this reason, Citrix recommends upgrading all computers to the latest version of Profile management before enabling any Version 3.x setting.

Tip: You can hotfix your Profile management 2.1 deployment by upgrading to Version 3.x. If you do so, install the Version 3.x ADM file and be sure to disable the new features introduced in that release. At a minimum, you must disable the active profile write back feature (enabled by default) before installing Profile management on all user devices, virtual desktops, and XenApp servers. When all copies of Version 2.1 are upgraded, you can, if desired, enable any 3.x feature. Coexistence of Version 2.1 and any version earlier than Profile management 3.2 is not supported. For more information, see http://forums.citrix.com/thread.jspa?threadID=276625&tstart=0.

Important: Deployments that contain Version 3.x with Version 2.1 or any earlier version, including Citrix Technical Preview or beta releases, are unsupported. If you require a mixed deployment (for example, as a temporary measure while you're migrating profiles), 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 no Version 3.x setting is enabled until all the computers have been upgraded to Version 3.x. After you enable any Version 3.x setting in a "mixed" user store, users can still log on to a computer that runs Version 2.1, but they receive a temporary Windows user profile (not their network, Citrix user profile) and changes they make to that profile are not saved.

When migrating from Version 2.1 or earlier to Version 3.0 or later, using separate OUs and user stores can be inconvenient. To avoid these constraints, you can use one of the following two strategies. Both rely on Active Directory (AD) groups to separate *Version 2* and *Version 3* users. The terms Version 2 and Version 3 here are shorthand for Profile management 2.1 or earlier and Profile management 3.0 or later. 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 3 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.

Strategy 1 – One-off Migration

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 3 file. The latter is compatible with the earlier version, so Version 2 computers continue to operate normally.

2. Ensure all of the Version 3 settings are not enabled. This is the default setting.

3. Start upgrading all the computers from Version 2 to Version 3. Fit this in with your normal maintenance and update schedules. With one exception, Version 3 acts as Version 2 until you enable any Version 3 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 3 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 3 deployment (albeit one without any configured Version 3 features) and PmCompatibility.ini is updated to reflect this.

4. Optionally, set your Version 3 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 3 processed users group. Allow sufficient time for the AD Group Policy changes to propagate, and let the remaining users log on.

Strategy 2 – Phased Migration

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 3 file. The latter is compatible with the earlier version, so Version 2 computers continue to operate normally.

2. Ensure all of the Version 3 settings are not enabled. This is the default setting.

3. Upgrade a few computers (the first batch) to Version 3. Alternatively, install Version 3 on new computers. By default, your Version 3 processed users group contains an empty

group, so no user is processed as a Version 3 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 3 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 3 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 3 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 3 group. Wait for the AD Group Policy changes to propagate to the Version 3 computers. Next time they log on, the users' sessions are processed with Version 3 settings.

8. Upgrade the next batch of computers and migrate the next batch of users, as above.

Upgrading Profile Management

This topic describes the process for upgrading your entire Profile management deployment using Active Directory. Follow this procedure if you want to create a new Group Policy Object (GPO) in the deployment. Alternatively, upgrade only the ADM file using the second procedure in this topic.

To upgrade a Profile management deployment

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 file to Group Policy. If you upgrade it beforehand, log files may 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 scheduled downtime to allow the AD changes that you make during this procedure to propagate through your deployment. Allow at least 24 hours of downtime for this.

1. Create a new Group Policy Object (GPO).
2. Add the new ADM file to the new GPO.
3. Back up and then import the configuration from your existing GPO to the new GPO.
4. Upgrade the Profile management software on all computers by installing this version over the earlier version.
5. Apply the new GPO.

To upgrade an existing ADM file

If any earlier version of the Profile management ADM file already exists in Group Policy, you can upgrade it using this procedure. All policy settings in the earlier version are preserved when you upgrade. For more information on this, see *A new ADM file is released with a new version of the software. What do I do?* in Frequently Asked Questions About Upgrading Profile Management.

1. In the Group Policy Object Editor, right-click **Administrative Templates** and select **Add/Remove Templates**.
2. Select the existing version of the Profile management ADM file (for example, ctxprofile3.0.0), click **Remove** and then **Close**. The Administrative Templates\Citrix folder is deleted.
3. Right-click **Administrative Templates** and select **Add/Remove Templates** a second time.

4. Click **Add**, browse to the location of the new version of the ADM file, select it, and click **Close**. The new ADM file is imported but the old settings are retained.

Considerations When Upgrading .Ini Files

If you edited the .ini file in an earlier version of Profile management and upgrade to this 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 this version, you must do one of the following:

- Manually add the new settings from this version's .ini file to your edited .ini file
- Save a copy of the earlier 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

Frequently Asked Questions About Upgrading Profile Management

This topic contains questions and answers about upgrading to Citrix Profile management 3.x.

For answers to frequently asked questions about other subjects, see Frequently Asked Questions About Using Profiles On Multiple Platforms and Frequently Asked Questions About Using Profiles On Multiple Platforms.

For more information on upgrading Profile management and how different versions coexist, see http://community.citrix.com/display/ocb/2011/02/18/Case+Study+-+XD+upgrade+from+UPM+2.x+to+3.x and http://community.citrix.com/x/NwWCCQ.

What important information should I review before upgrading to Version 3.x?

Consider the following important points before you upgrade to Profile management 3.x. Read each point carefully:

- Do not upgrade from Version 2.x to any version earlier than Version 3.2. There are issues when Versions 2.x and 3.x coexist that were resolved in Version 3.2. For more information, see the fixed issues for Version 3.2 at http://support.citrix.com/article/CTX124164.
- Do not upgrade from versions earlier than Version 2.x. Upgrading from Version 2.1.1 is recommended because it has logic to detect when it is used with newer versions, and operates appropriately.

What is the upgrade procedure?

Follow one of the procedures in Upgrading Profile Management and Migrating Profiles.

What are the recommendations for testing Profile management?

Test Profile management 3.x before rolling out the software in a production environment. Your pilot should use a separate Organizational Unit (OU), and should not use the same accounts as users in the production environment. It should at least use a different user store. Version 3.x marks profiles in the user store with Version 3.x tags because it uses a newer schema. Version 2.1.1 can detect this schema but cannot process it, so it tries to load a temporary profile to avoid overwriting 3.x profiles. This is not desirable in a production environment, so you are recommended to use a different user store for testing Version 3.x.

A new ADM file is released with a new version of the software. What do I do?

The ADM files are designed so you can replace the Version 2.x file with the Version 3.x one; the existing settings are preserved. You can replace the files in the same Group Policy Object (GPO). You do not have to create a new GPO, but if you prefer to do so see the instructions in Upgrading Profile Management.

For upgrades from Version 2.x to Version 3.x, the active profile write back feature is enabled by default. During the upgrade process, you must configure this feature as **Disabled**.

You must not enable any of the new features in Profile management 3.x while the upgrade is in progress. Profile management 3.0 introduced a new schema, which would be corrupted if Version 2.0 wrote to it. A compatibility check was therefore introduced in Profile management 2.1.1 to help avoid this corruption in the event that 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 on, 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 3.x 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.

How do I roll back Profile management if I upgraded incorrectly?

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 of these files are deleted, you can revert to Profile management 2.1.1 and restart the deployment with that version's ADM file.

If the .ini files are not deleted, Profile management 2.1.1 checks, finds that version 3.x systems are also using the user store, and gives the users a temporary profile. Any users who find they have been given a temporary profile must alert their support desk, who can tell them to log off. The support desk can then manually delete the .ini file from the user store.

Administering Profile Management

Once you have added the ADM file to Group Policy, set up Profile management to match the needs of your Citrix deployment using the procedures in this section. For example, perform basic setup operations such as specifying the location of the user store and the groups whose profiles you want to manage. If necessary, you can also perform advanced setup operations such as identifying any files and folder to exclude from processing.

Basic Profile Management Tasks

There are many settings that allow you to customize the way user profiles are processed. This section lists the tasks used to configure commonly used settings.

Typically, you don't need to follow all of these tasks because defaults are provided. Enabling the software is, however, mandatory. The tasks that you are most likely to use are listed first:

1. Testing Profile management
2. Enabling Profile management

   Important: Perform this task only after testing any other settings were configured as intended.
3. Deciding how to resolve conflicting profile data
4. Choosing an appropriate migration policy that turns existing Windows user profiles into Citrix user profiles
5. Specifying the path to the user store
6. Defining the groups whose profiles you want Profile management to process
7. Setting up logging (if you want to troubleshoot profile management)

You configure Profile management in Group Policy Object Editor, under the **Computer Configuration** > **Administrative Templates** > **Citrix** > **Profile Management** folder. (In Windows Server 2008, the folder is **Computer Configuration** > **Administrative Templates** > **Classic Administrative Templates (ADM)** > **Citrix** > **Profile Management**.) Any settings not configured there (that is, settings in the Not Configured state) take the default values from the Profile management .ini files if you installed these.

For information on any setting, consult Profile Management ADM File Reference.

To specify the path to the user store

Before following this procedure, refer to About the User Store and understand how your use of the extended synchronization and multilingual profile storage features affect it.

1. Under **Profile Management**, double-click the **Path to user store** policy.

2. Select **Enabled** and enter the path. If you enter a relative path, it is relative to users' home directories. Enter a complete UNC path to define an explicit path name. You can use AD variables (for example, #sAMAccountName#) or system environment variables (for example, the combination of %USERNAME% and %USERDOMAIN%). AD variables are case-sensitive. Unlike #cn# or #sAMAccountName#, the system environment variables allow users to be defined unambiguously in Active Directory networks with multiple domains. User environment variables are not supported.

   Example: \\servername\profilestore\%USERNAME%\%ProfileVer% can resolve to \\servername\profilestore\JohnSmith\WinXP or \\servername\profilestore\JohnSmith\Win2k8ts.

For more information on using variables when specifying the path to the user store, see Sharing Citrix User Profiles on Multiple File Servers and Administering Profiles Within and Across OUs.

For information on managing system environment variables in Windows XP, see http://support.microsoft.com/kb/310519.

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 define which groups' profiles are processed

If you do not define any groups with this setting, all Windows user profiles are processed.

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.

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

When a user first logs on after Profile management is enabled, no Citrix user profile exists for that user. You can decide which existing Windows profile (roaming, local, or both) is copied by Profile management and used in all further processing. If this setting is disabled, no profile is migrated.

For more information on planning a migration strategy, see Planning for Migration and Conflicts.

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.

   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.

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 profile

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 Windows profile that resides on any network file share.

As prerequisites:

- Ensure the template profile does not contain any user-specific data
- Ensure users have read access to the template profile
- If you specify a mandatory profile as a template, first rename the file NTUSER.MAN to NTUSER.DAT

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 roaming, local, or mandatory 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: If the path consists only of NTUSER.DAT, ensure that you do not include the file name in the path.
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**.

To resolve conflicting profiles

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. For more information on managing conflicts, see Planning for Migration and Conflicts.

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 data.
    - **Delete local profile**. Profile management deletes the local data and processes the data in the user store.
    - **Rename local profile**. Profile management renames the local data (for backup purposes) and processes the data in the user store.

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 set default inclusions and exclusions

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

- Use Profile Management ADM File Reference to map setting names in the .ini file and the .adm file
- When pasting inclusions and exclusions from the .ini file, remove the trailing = (equals sign) from each item

For example, you paste `Software\Microsoft\Windows\CurrentVersion\Explorer\TrayNotify=` from `ExclusionListRegistry` in the .ini file as `Software\Microsoft\Windows\CurrentVersion\Explorer\TrayNotify` under `Profile Management\Registry\Exclusion list` in the .adm file.

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

- Use Profile Management ADM File Reference to map setting names in the .ini file and the .adm file
- When pasting inclusions and exclusions from the .ini file, remove the trailing = (equals sign) from each item

For example, you paste `Software\Microsoft\Windows\CurrentVersion\Explorer\TrayNotify=` from `ExclusionListRegistry` in the .ini file as `Software\Microsoft\Windows\CurrentVersion\Explorer\TrayNotify` under `Profile Management\Registry\Exclusion list` in the .adm file.

Registry Inclusion List

Default Value	Notes
<empty>	All entries in the HKCU hive are included by default.

Registry Exclusion List

Default Value	Notes
Software\Microsoft\Windows\CurrentVersion\Explorer\TrayNotify	Windows Explorer caches tray notification icons as binary data in the registry.

Folder Inclusion List

This table shows the included folders on English systems. For other languages, you must edit the entries. For example, for German systems use Favoriten instead of Favorites.

Default Value	Notes
Windows XP and Windows Server 2003	
Local Settings\Application Data\Microsoft\Credentials	Must be included because it is inside an excluded folder. Stores user certificates.
Local Settings\Application Data\Citrix\Citrix offline plug-in	Must be included because it is inside an excluded folder. Location of the per-user storage for the Citrix offline plug-in.
Windows Vista and Windows Server 2008	
AppData\Local\Microsoft\Credentials	Needs to be included because it is inside an excluded folder. Stores user certificates.
AppData\Local\Citrix\Citrix offline plug-in	Needs to be included because it is inside an excluded folder. Location of the per-user storage for the Citrix offline plug-in.

Folder Exclusion List

Folders in this table are excluded from synchronization.

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.

Default Value	Notes
Windows XP and Windows Server 2003	
Application Data\Citrix\PNAgent\AppCache	This is a cache.
Application Data\Citrix\PNAgent\Icon Cache	This is a cache.
Application Data\Citrix\PNAgent\ResourceCache	This is a cache.

Application Data\ICAClient\Cache	This is a cache.
Application Data\Macromedia\Flash Player\#SharedObjects	This is a cache.
Application Data\Macromedia\Flash Player\macromedia.com\support\flashplayer\sys	This contains flash cookies.
Application Data\Sun\Java\Deployment\cache	This is a cache.
Application Data\Sun\Java\Deployment\log	This is a log folder.
Application Data\Sun\Java\Deployment\tmp	This is a temporary folder.
Local Settings	Mostly specific to the computer. Also excluded with roaming profiles.
Start Menu	The Start menu is mostly specific to the computer.
Windows Vista and Windows Server 2008	
$Recycle.Bin	Also excluded with roaming profiles.
AppData\Local	Mostly specific to the computer. Also excluded with roaming profiles.
AppData\LocalLow	Mostly specific to the computer. Also excluded with roaming profiles.
AppData\Roaming\Citrix\PNAgent\AppCache	This is a cache.
AppData\Roaming\Citrix\PNAgent\Icon Cache	This is a cache.
AppData\Roaming\Citrix\PNAgent\ResourceCache	This is a cache.
AppData\Roaming\ICAClient\Cache	This is a cache.
AppData\Roaming\Macromedia\Flash Player\#SharedObjects	This is a cache.
AppData\Roaming\Macromedia\Flash Player\macromedia.com\support\flashplayer\sys	This contains flash cookies.
AppData\Roaming\Microsoft\Windows\Start Menu	This (the Start menu) is mostly machine-specific.
AppData\Roaming\Sun\Java\Deployment\cache	This is a cache.
AppData\Roaming\Sun\Java\Deployment\log	This is a cache.
AppData\Roaming\Sun\Java\Deployment\tmp	This is a temporary folder.

File Inclusion List

Files in this table are included on synchronization. Wildcards are supported for file inclusions.

Default Value	Notes

Windows XP and Windows Server 2003	
Local Settings\Application Data\Microsoft\Office*.qat	Quick Access Toolbar entries for Microsoft Office. For further information, refer to http://support.microsoft.com/kb/926805/en-us.
Local Settings\Application Data\Microsoft\Wallpaper1.bmp	The background graphic used on Windows XP desktops.
Windows Vista and Windows Server 2008	
AppData\Local\Microsoft\Office*.qat	Quick Access Toolbar entries for Microsoft Office. For further information, refer to http://support.microsoft.com/kb/926805/en-us.

File Exclusion List

Files in this table are excluded from synchronization. Wildcards are supported for file exclusions.

Default Value	Notes
Windows XP and Windows Server 2003	
<empty>	By default, no files are excluded.
Windows Vista and Windows Server 2008	
<empty>	By default, no files are excluded.

To enable Profile management

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.**

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.

Optimizing Profile Management Performance

Use the settings in this section once you are familiar with the basic operation of Profile management, you have tested it and rolled it out in a production environment, and have a clear business requirement to use these advanced profile configuration settings.

About Profile Management Settings

Conflicts

Profile management does not check any settings for conflicts. For example, you can set the same directory to be both included and excluded but this leads to unpredictable results.

Default Configuration

Profile management comes with a default configuration stored in .ini files. The .ini files must be located in the installation folder so that the Citrix Profile Management service can recognize them. The default configuration is suitable for most environments. It processes the profiles of all users in all groups.

To find the .ini file used by each operating system, see Files Included in the Download. If you are not sure which file is used, examine the log file and search for the text `Reading from policy defaults file`.

If you are configuring a non-English version of Windows XP and Windows Server 2003, you must create an appropriate language version of the .ini file using UPMPolicyDefaults_V1Profile_en.ini. Rename a copy of this file to reflect your language (for example, UPMPolicyDefaults_V1Profile_es.ini for Spanish) and localize the folder names. Use these file names:

- For French operating systems, UPMPolicyDefaults_V1Profile_fr.ini
- For German operating systems, UPMPolicyDefaults_V1Profile_de.ini
- For Spanish operating systems, UPMPolicyDefaults_V1Profile_es.ini
- For Japanese operating systems, UPMPolicyDefaults_V1Profile_ja.ini
- For Simplified Chinese operating systems, UPMPolicyDefaults_V1Profile_zh-CN.ini

The operating system language uses the appropriate version of the file, so if that version is not present Profile management might not work as expected.

The same .ini file is used for all languages on Windows Vista and Windows Server 2008.

Modifying .Ini Files

If you add entries to an .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
```

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 entries specify files to be synchronized:

```
[SyncFileList]
Local Settings\Application Data\Microsoft\Office\*.qat=
Local Settings\Application Data\Microsoft\Wallpaper1.bmp=
```

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.

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 you restart the Citrix Profile Management service on the target computers.

Configuration Precedence

You can configure Profile management using Group Policies and .ini files. 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. This is documented at http://technet.microsoft.com/en-us/library/cc785665(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.

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.

You can view the description of any setting and its default value in the Group Policy Object Editor. Alternatively, refer to Profile Management ADM File Reference.

Tuning Profiles

You can fine tune how profiles are processed using the following settings: **Inclusion list**, **Exclusion list**, **Directories to synchronize**, and **Files to synchronize**. These define the files, folders, and registry keys (in the HKCU hive) that are processed or ignored when users log on or log off.

By selecting the values for these settings that meet your organization's needs, you can further improve the logon and logoff experience of your users.

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.

Before Tuning Profiles

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.

In deployments with many XenApp servers, for example, you may decide to delete locally cached profiles in order to save disk space on the servers, which would otherwise (if cached profiles are stored) fill up with many user files.

In XenDesktop deployments where pooled desktops are set to restart at each logoff, there is little point in caching profiles because they are overwritten at each logoff.

If you do not stream user profiles and you want to cache profiles locally, make sure Profile management's **Delete locally cached profiles on logoff** setting is disabled. If you stream user profiles, that setting is overriden and any locally cached profiles are deleted; this is not detrimental because the improved logon times resulting from local caching are surpassed when profiles are streamed.

Monitoring and Logging Profile Management

You can log many aspects of your Profile management deployment, but logging is typically enabled when you troubleshoot problems or if you want to gather performance data. You can change the verbosity of logging and select different log settings. You must enable logging so that log files are created.

The log file is created on the computer on which Profile management is installed, in the folder %SystemRoot%\System32\LogFiles\UserProfileManager.

You can use Windows Performance Monitor to track several aspects of logon and logoff.

About the Profile Management Log File

The event log is used primarily for the purpose of error reporting. Only errors are written to it. All other warning and informational messages, in addition to errors, are written to the log file. This is the file %SystemRoot%\system32\LogFiles\UserProfileManager\UserProfileManager.log.

Log Entry Types

- **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.

Log File Format

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

To set up logging

This topic contains procedures for configuring log file settings in Group Policy Object Editor. For expanded instructions on collecting diagnostic information for Profile management, see Collecting Diagnostic Information.

1. In Group Policy Object Editor, navigate to the **Computer Configuration** > **Administrative Templates** > **Citrix** > **Profile Management** folder. (In Windows Server 2008, the folder is **Computer Configuration** > **Administrative Templates** > **Classic Administrative Templates (ADM)** > **Citrix** > **Profile Management**.)
2. Open the **Log settings** folder.
3. Double-click the **Enable logging** policy.
4. Select **Enabled.**
5. Click **OK.**
6. Click the **Log settings** policy.
7. Select **Enabled.**
8. Select the type of events that you want Profile management to log.

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 set an alternative location for log files

You can adjust the location where Profile management log files are stored.

Some logon and logoff processing is done in the context of the user using impersonation. Citrix recommends that you grant write permissions on the log folder for the users group so that Profile management can write to the log files during impersonation.

1. Open the **Log settings** folder.
2. Double-click the **Path to log file** policy.
3. Select **Enabled.**
4. In **Path to log file**, enter an alternative path for the log files.
5. 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.

Performance Monitoring and Profile Management

Profile management collects data about the efficiency of your deployment using Microsoft Windows Performance Monitor (Perfmon) counters. For each session, counters are stored under the object called Citrix Profile Management. In Profile management 3.0 or later, these include:

- **Logon Bytes**. The size of the Citrix user profile when it is retrieved from the user store at logon (Bytes).
- **Logoff Bytes**. The size of the Citrix user profile when it is copied to the user store at logoff (Bytes).
- **Local Profile Setup Duration**. The time taken to create or prepare a Citrix user profile on the local computer (milliseconds).
- **Logon Duration** and **Logoff Duration**. The duration of logon and logoff processing by the Citrix Profile Management service (milliseconds). **Logon Duration** helps to measure the reduction in logon times when profiles are streamed.
- **Processed Logon Files - <file size range>** and **Processed Logoff Files - <file size range>**. A series of counters that together measure the profile size. Separately for logon and logoff, the number of files that are synchronized is categorized by file size. **Processed Logon Files** helps to measure the reduction in the number of locally copied files when profiles are streamed.

In Version 3.1 or later, these additional counters can also be used:

- **Registry Change Logoff Processing Duration**. The time spent processing registry changes at logoff.
- **File Logoff Change Processing Duration**. The time spent processing file changes at logoff.
- **Userstore Logoff Migrate Duration**. The time spent migrating files from the pending area to the user store.
- **Delete Local Profile Duration**. The time spent deleting local profiles at logoff (that is, if the policy **Delete locally cached profiles on logoff** is enabled).
- **Initial Profile Migrate Duration**. The time spent converting existing Windows user profiles to Citrix user profiles during the initial migration.

Perfmon information is also stored in the log file (except that logon and logoff times are summarized in seconds instead of milliseconds). No configuration of Perfmon is required.

To provide access to performance data

You can let other administrators use Windows Performance Monitor (Perfmon) to monitor how well your Citrix user profiles are performing. They do not need full administration privileges on any of the domain controllers used to configure Profile management.

1. Ensure the administrators who will use Perfmon are members of the Performance Monitoring Users group.

Including and Excluding Items

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*.

Exclusions are processed at logoff not logon.

In addition to files and folders contained in profiles, you can include and exclude:

- Registry entries related to profiles in the HKCU hive. Entries in the HKLM hive are not processed by default and cannot be configured to do so.
- Files and folders that are not included in the profile (using the extended synchronization feature).

The default configuration specifies included and excluded items in the file system and registry. Default inclusions and exclusions are listed in To set default inclusions and exclusions.

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.

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.

To include items

1. Under **Profile Management** > **Registry**, double-click the **Inclusion list** policy.
2. Select **Enabled.**
3. Add any registry keys in the HKCU hive that you want to be processed during logoff.
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 outside the user profile or in excluded folders.
7. Under **Profile Management** > **File system** > **Synchronization**, double-click the **Files to synchronize** policy.
8. Select **Enabled.**
9. Add any files that you want Profile management to process but that are located outside the user profile or in excluded folders.

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 exclude items

1. Under **Profile Management** > **Registry**, click the **Exclusion list** policy.
2. Select **Enabled.**
3. Add any registry keys in the HKCU hive that you do not want to be processed during logoff.
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.
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.

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 in Inclusion and Exclusion Lists

You can use ? (question mark) and * (asterisk) as wildcard characters in file inclusion and exclusion lists. The ? (question mark) matches a single character. The * (asterisk) matches zero or more characters.

Wildcards work recursively but are not supported in folder names. Ensure you specify a path when using wildcards.

Examples

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.

About Extended Synchronization

Extended synchronization is the combining of inclusion lists and an exclusion lists. This is a powerful way of ensuring no extraneous items are processed by Profile management. Although this sounds like a good way of improving the efficiency of profile synchronization for any deployment, in practice you only need to combine inclusion lists and exclusion lists for *badly behaved applications*.

To use extended synchronization, you:

- Add to an inclusion list a subfolder of a folder that is on an exclusion list
- Add to an exclusion list a subfolder of a folder that is on an inclusion list

No other configuration is required. The following examples describe each of these cases.

Note: Inclusions take precedence over exclusions, so if the same folder appears in both lists it is included.

Example: Excluding Temporary Data

Your Windows XP users have an application called MyApp that creates and stores many supporting files in the \Application Data\MyApp folder. A subfolder is called Stuff contains temporary data that does not need to be synchronized.

You add the MyApp folder to the inclusion list and add the Application Data\MyApp\Stuff folder to the exclusion list. At logoff, these files remain on the user device and are not transferred to the user store. If you configure local profiles not to be cached, this temporary data is deleted at logoff along with the cached profile.

Example: Including Internet Explorer Passwords

Your Windows Vista users roam between one desktop and another. They want their Internet Explorer passwords to follow them, which means that their Microsoft credentials must be processed by Profile management.

You add the Local Settings folder to the exclusion list because by default it is a folder where applications store user data that typically should not roam. You add the Local Settings\Application Data\Microsoft\Credentials folder to the inclusion list so that its contents are synchronized and available to users whichever desktop they log on to.

Supported Uses of Extended Synchronization

Extended synchronization is designed to enable personalization settings that are not properly stored in the user's profile location (for example, those from *badly behaved applications*) to be captured as part of the user profile. This topic describes supported and unsupported scenarios.

The feature is not intended to manage multi-user access to these files or folders (for example, it is not designed to support an application that is not multiuser aware) and is not intended to become a file and folder synchronization mechanism (for example, one that allows you to synchronize the entire contents of c:\docs across machines).

The feature extends personalization settings that exist outside the default user profile location and provides a consistent experience across all resources accessed by the user.

Supported Scenarios

The supported scenarios are all based on a single-user with exclusive access to a workstation environment (typically XenDesktop, but a native workstation environment is also supported where the license permits.)

Scenario 1: Assigned Desktop (XenDesktop) Not Shared with Any Other User

This scenario also covers a domain workstation, again not shared with any other user.

Extended Synchronization supports synchronization of one or more external folders (that is, folders outside the user's profile area). For example, assume we have an application App1 which stores its personalization in two folders c:\App1 and c:\App1Blobs.

Prior to a user logging on and creating their profile you must configure all the folders to be synchronized. Extended synchronization does not support the addition of further folders after logon, once the user's profile has been created. It is essential to pilot the application before deploying it to a production environment.

Once extended synchronization has been configured as described above, the user may log on and create (or migrate) their profile. Extended synchronization supports the use of pre-installed applications (for example, using a standard image with all applications already installed) and also applications that are installed by the user after the profile has been created.

Scenario 2: Pooled Desktop (XenDesktop), Not Shared with Any Other User

This is very similar to Scenario 1. In this supported configuration, the application will have been installed as part of a shared image, but will not have been run, so that personalization takes place on the first use of the application.

Unsupported Scenarios

Other scenarios - those typically involving shared access by multiple users to a workstation, or simultaneous access by multiple users to a server - are not supported. Specific examples of unsupported scenarios include:

- Domain workstations, including domain-joined XenDesktop workstations, shared by multiple users. Fast User Switching disabled.
- Domain servers, concurrently shared with other users, whether Remote Desktop Services and XenApp environments.
- Domain workstations. Fast User Switching enabled.

These unsupported scenarios all involve a folder or folders being shared by multiple users, which gives rise to privacy and security issues, as well as profile bloat.

More Information

The scenarios described in this topic may be further constrained by any End User License Agreements (EULAs) that apply to the Citrix products in your deployment.

To use extended synchronization

By default, only files, folders, and registry settings that are part of Windows user profiles are synchronized by Profile management. However, you can include other items. You may need to do so because a *badly behaved application* stores data in a non-standard location.

Caution: Only use extended synchronization in a supported scenario. Using this feature in an unsupported one may result in data loss. For more information, see Supported Uses of Extended Synchronization.

Check the syntax of any Profile management setting in Profile Management ADM File Reference.

1. Include items using absolute paths in the **Directories to synchronize** and **Files to synchronize** settings.

2. Exclude items using absolute paths in the **Exclusion list - directories** and **Exclusion list - files** settings.

3. Mirror indexed files using absolute paths in the **Folders to mirror** setting.

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

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.

Example

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

With the Citrix streamed user profiles feature, files and folders are fetched from the user store to the local computer only when they are accessed by users after they have logged on. Registry entries, items specified using the extended synchronization feature, and any files in the pending area are exceptions. They are fetched immediately. For more information on the pending area, see Pending Area.

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.
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.
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. The profiles of users in all other groups will not be streamed.
9. 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 active profile write back

To ensure profile integrity, files and folders (but not registry entries) that are modified on the local computer can be backed up to the user store in the middle of a session, before logoff. This is particularly useful in Citrix XenDesktop deployments, where a user might otherwise leave their session open for a long period without local file changes in their profile being mirrored in the user store.

This feature is not intended to support users opening multiple active sessions. However, 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**.

To configure Profile management for folder redirection

This feature can be configured in Version 3.2 or later.

Folder redirection is a feature of Microsoft Windows. For information on how this feature works with Profile management, see Planning Folder Redirection with Profile Management.

If, while configuring folder redirection, you select the Group Policy option **Move the contents of <folder name> to the new location**, by default Profile management does not delete the folder after its contents are moved. This results in two identically named items in the local profile, the folder itself and a shortcut to the folder. Because they appear side by side, these duplicates can confuse users.

To prevent the confusion in these circumstances, enable the Profile management ADM file setting as described in this procedure. If the setting is enabled, the folder is deleted from the local profile when the user next logs on.

Important: Only follow this procedure if the **Move the contents of <folder name> to the new location** option is selected. If it is unselected (for example, you may be performing server moves or maintenance and don't want Group Policy to move files), do not follow the procedure.

1. Under **Profile Management** > **Advanced Settings**, double-click the **Delete Redirected Folders** policy.
2. Select **Enabled.**

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 manage cookie folders and other transactional folders

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 profile 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.

To mirror folders

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

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.

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.

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.

To delete stale cookies

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

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:

To process cookie folders

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.

Administering Profiles Within and Across OUs

Within OUs

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 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.

To manage different computers with different OSs using a single GPO in a single OU, you can implement a system environment variable and incorporate it 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 `XP` for your Windows XP 32-bit computers and `XPx64` for your Windows XP 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 are 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

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

Across OUs

You can control how Profile management administers profiles across OUs. Depending on your OU hierarchy, one OU may inherit policies from another. You can create policy settings in a separate Group Policy Object linked to the affected OU to override the inherited policies.

Integrating Profile Management with Citrix Products

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 Troubleshooting Profile Management.

This section also contains information about how some third-party products interact with Profile management or profiles in general.

Profile Management and XenApp

This version of Profile management is available to customers who are licensed to use Enterprise and Platinum Editions of XenApp (version 4.5 or later). You can also install Profile management on local desktops, allowing users to share their local profile with published resources.

Profile management works in XenApp environments that employ Terminal Services. In these environments, you must set up an OU for each supported operating system. For more information, see the article "Using User Profiles in Windows Server 2003" on the Microsoft TechNet Web site at http://technet.microsoft.com.

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: Citrix does not recommend using extended synchronization on folders that are shared by multiple users (for example, folders containing shared application data). If you apply this feature to such folders, the application data created by one user may be overwritten by Profile management when another user logs off.

Streamed Applications

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 for Profile Management.

Profile Management and XenDesktop

This version of Profile management is available to customers who are licensed to use:

- the Advanced, Enterprise, or Platinum edition of XenDesktop 2.1 or 3.0
- the VDI, Enterprise, or Platinum edition of XenDesktop 4.0 or later

You can use Profile management with XenApp in a XenDesktop environment. For more information, see Profile Management and XenApp. If that environment also uses Provisionsing Services, see Profile Management and Provisioning Services.

If you upgrade Profile management in a XenDesktop deployment, consider the effect on the log file locations as described in Upgrading Profile Management.

Do not install the Profile Management Service on XenDesktop servers. Install it on the virtual images (for example, vDisks created with Citrix Provisioning Services) that you use to create virtual desktops. The Citrix Profile Management Service starts before Group Policy is applied if Profile management has not been configured correctly on the images before they are rolled out.To avoid this, perform the configuration using the documented procedures before you put the images into a production environment. If you are using vDisks, follow the best practice described in Profile Caching on vDisks.

Consider using the active profile write back feature as a safeguard in your XenDesktop deployment.

Important: Citrix does not recommend using extended synchronization on folders that are shared by multiple users (for example, folders containing shared application data). If you apply this feature to such folders, the application data created by one user may be overwritten by Profile management when another user logs off.

Typical Settings for Use with XenDesktop

This section contains typical settings for use in a XenDesktop deployment.

The following settings from the Profile management ADM file derive from a realistic deployment using virtual desktop images created with Citrix Provisioning Services and shared by multiple users. Set all other options as described elsewhere in this documentation.

Note the following about these settings:

- **Path to user store** . This setting makes use of an environment variable, ProfVer, which is only set once (before imaging the Master Target device) for each operating system in the XenDesktop environment. Alternatively, if you have many Provisioning Server private virtual disks (vDisks) or many physical devices, it may be simpler for each OU to have a separate GPO that defines the path to the user store (and that also enables Profile management). For details of this environment variable, see .

- **Processed groups** . All domain users' profiles are managed by Profile management.

- **Exclusion list - directories** (file system) and **exclusion list** (registry). These setting prevents 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 user's application data is stored helped define these settings.

- **Log settings**. This deployment includes fairly detailed recording of events in the Profile management log.

- **Local profile conflict handling** and **migration of existing profiles**. This deployment existed before Profile management was added to it. This has two consequences:

    1. Local profiles and Citrix profiles (those managed by Profile management) might co-exist, causing potential conflicts that must be resolved by deciding which profile type takes precedence. In this case, the deployment favored Citrix profiles over local profiles. The data in the latter is discarded if a conflict arises.

    2. A decision must be made on which existing Windows profile (roaming, local, or both) is copied to the user store and used in all further processing. In this case, both profile types can be present.

Citrix/Profile Management

Processed groups

Setting: Enabled

Processed groups: MyDomainName\Domain Users

Citrix/Profile Management/File system

Exclusion list - directories

Setting: Enabled

Exclusion list:

$Recycle.Bin

AppData\Local\

AppData\Local\Google\Chrome\User Data\Default\Cache

AppData\Local\Google\Chrome\User Data\Default\Plugin Data

AppData\LocalLow

AppData\Roaming\Citrix\PNAgent\AppCache

AppData\Roaming\Citrix\PNAgent\Icon Cache

AppData\Roaming\Citrix\PNAgent\ResourceCache

AppData\Roaming\ICAClient\Cache

AppData\Roaming\Macromedia\Flash Player\#SharedObjects

AppData\Roaming\Macromedia\Flash Player\macromedia.com\support\flashplayer\sys

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

Setting: Enabled

List of directories to synchronize:

AppData\Local\Citrix\RadeCache

AppData\Local\Google\Chrome\User Data\Default

AppData\Local\Microsoft\Credentials

AppData\Local\Microsoft\Feeds

AppData\Local\Microsoft\Windows Sidebar

Files to synchronize

Setting: Enabled

List of files to synchronize:

AppData\Local\Google\Chrome\User Data\First Run

AppData\Local\Microsoft\Office*.qat

Citrix/Profile Management/Log Settings

Enable logging

Log Settings

Setting: Enabled

Define events or actions which Profile management logs in depth:

Common warnings: Enabled

Common information: Enabled

File system notifications: Enabled

File system actions: Enabled

Registry actions: Enabled

Registry differences at logoff: Enabled

Active Directory actions: Enabled

Policy values at logon and logoff: Enabled

Logon: Enabled

Logoff: Enabled

Personalized user information: Enabled

Maximum size of the log file

Setting: Enabled

Maximum size in bytes: 1048576

Citrix/Profile Management/Profile handling

Local profile conflict handling

Setting: Enabled

If both a non-Profile Management local profile and a Profile Management user store profile exist: Delete local profile.

Migration of existing profiles

Setting: Enabled

Types of user profiles to be migrated if the user store is empty: Local and Roaming

Citrix/Profile Management/Registry

Exclusion list

Setting: Enabled

Exclusion list: Software\Microsoft\Windows\CurrentVersion\Explorer\TrayNotify

Profile Management and Provisioning Services

This section applies to Citrix user profiles on virtual disks (vDisks) created with Citrix Provisioning Services.

You can use Profile management on vDisks running in Standard Image and Private Image modes but not Difference Disk Image mode.

Profile Caching on vDisks

To lay out your vDisk effectively, be aware that the Profile management cache is located separately from the vDisk cache. For information about vDisk cache locations, see your Provisioning Services documentation.

The Profile management cache default location is C:\Program Files\User Profile Manager. If your vDisk has a local physical disk that is not streamed, consider locating the Profile management cache on this disk. This is especially recommended for vDisks running in Standard Image mode because the cache is recreated each time Profile management restarts or the Change Journal's Journal ID is updated (a frequent scenario for vDisks running in this mode). If, on the other hand, the cache is stored on a local physical disk, the cache is not recreated with each restart or update.

It is also good practice for vDisks running in Standard Image mode to ensure, before taking the Master Target Device image, that all non-essential, locally cached profiles are removed from the Device, 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.

To remove non-essential, locally cached profiles from the Master Target Device

This is the procedure on Windows XP.

1. Right-click **My Computer**.
2. Select **Properties**.
3. On the **Advanced** tab, click **Settings** in **User Profiles**.
4. Highlight each profile you want to remove and click **Delete**.

To maintain Profile management on vDisks

Follow this procedure when maintaining Profile management on a vDisk image that runs in Standard Image mode (for example, when you upgrade the software). If you don't follow this procedure, users' logons may hang while their profiles are loaded.

1. Stop the vDisk running in Standard Image mode.
2. Change to Private Image mode.
3. Perform the maintenance tasks you require. For example, to upgrade Profile management:

a. Upgrade to the new version and let the vDisk start.

b. Stop the Citrix Profile Management service.

c. Delete the Profile management cache.

4. Put the vDisk back into Standard Image mode.

To retrieve log files from vDisk images

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 with provisioned images

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, those settings should be sensible defaults for the provisioned virtual machine when it starts running and the user logs on. At a minimum, you should ensure you have sensible defaults for these settings:

- **Enable Profile management**. You need to enable the software once your preparation and testing of Profile management and the image as a whole are complete.
- **Process logons of local administrators**. Typically, you do not need to process administrators' logons.
- **Processed groups**. Specify the groups you want to have Citrix user profiles.
- **Directory of the MFT cache file**. Sets the path to the directory in which a cache file of the Master File Table (MFT) directory content is stored.
- **Path to log file**. Specifying this location ensures log traces are properly captured on the image. This defaults to the folder %SystemRoot%\System32\LogFiles\UserProfileManager.

The defaults are used if the image does not immediately get a `gpupdate` 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, only once your testing proves successful, that you transfer the settings to the .adm file.

1. If using an .adm file, change the desired settings using the file in the appropriate GPO. If using an .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 using an .ini file, change the desired settings in the file.

6. Stop the Profile Management Service.

7. Delete the Profile management cache from the installation directory. Typically, this is located under C:\Program Files\Citrix\User Profile Manager.

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 VMWare

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 Microsoft Outlook

This topic describes best practice for integrating Microsoft Outlook with roaming profiles.

Read the following article before integration:

http://office.microsoft.com/en-gb/help/HA011402691033.aspx.

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, 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 Citrix Password Manager

This topic applies to Password Manager 4.5 and 4.6. It describes the use of various Windows profile options and how best to integrate Password Manager with these profiles. The profiles covered in the topic are local profiles, roaming profiles, and mandatory profiles or hybrid profiles.

This topic does not contain any information specific to Profile management.

Local Profiles

Local profiles are stored on the local server to which the user has logged on. Password Manager saves registry information in the HKCU\Software\Citrix\MetaFrame Password Manager hive of the User Registry located at:

```
%SystemDrive%\Documents and Settings\%username%\NTUSER.DAT.
```

Password Manager also saves files in:

```
%SystemDrive%\Documents and Settings\%username%\Application
Data\Citrix\MetaFrame Password Manager.
```

On Windows Vista, Password Manager uses:

```
%APPDATA%\Roaming\Citrix\MetaFrame Password Manager
```

Important: It is critical that Password Manager 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

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 or Hybrid Profiles

Mandatory profiles are by definition user read-only profiles. Password Manager 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 Password Manager to work correctly with mandatory profiles, the Application Data Folder must be redirected.

With Password Manager, 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

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 Password Manager. 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

Best Practices

- 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.

Profile Management ADM File Reference

This topic describes the settings in the ADM file, the template used to configure Profile management settings. In the Group Policy Object Editor, the settings appear under **Computer Configuration** > **Administrative Templates** > **Citrix**.

Modifying Settings

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.

Sections in the ADM File

All Profile management policies are contained in the following sections, located in the Citrix folder:

Profile Management

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

Enable Profile management

By default, to facilitate deployment, Profile management does not process logons or logoffs. Turn on processing by enabling this setting.

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.

This setting corresponds to the ServiceActive setting in the .ini file.

This setting requires User Profile Manager 2.0.0 or later.

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 setting is configured here, Profile management processes only members of these user groups. If this setting is disabled, Profile management processes all 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, members of all user groups are processed.

This setting corresponds to the ProcessedGroups setting in the .ini file.

This setting requires User Profile Manager 1.0.0 or later.

Process logons of local administrators

Specifies whether logons of members of the BUILTIN\Administrators group are processed. If this setting is disabled or not configured, Profile management assumes that logons by domain users, but not local administrators, must be processed. This setting allows domain users with local administrator rights to bypass any processing, log on, and troubleshoot a computer that experiences 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 setting is disabled, logons by local administrators are 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, administrators will not be processed.

This setting corresponds to the ProcessAdmins setting in the .ini file.

This setting requires User Profile Manager 1.0.0 or later.

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 setting: system environment variables enclosed in percent signs (for example, %ProfVer%) and attributes of the Active Directory user object enclosed in hashes (for example, #sAMAccountName#). Note that system environment variables generally require additional setup.

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.

For example, \\server\share\#sAMAccountName# stores the user settings to the UNC path \\server\share\JohnSmith (if #sAMAccountName# resolves to JohnSmith for the current user).

Important: Whichever attributes or variables you use, check that this setting expands to the folder where NTUSER.DAT is located.

For more information on using variables when specifying the path to the user store, see Sharing Citrix User Profiles on Multiple File Servers and Administering Profiles Within and Across OUs.

If this setting 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.

This setting corresponds to the PathToUserStore setting in the .ini file.

This setting requires User Profile Manager 1.0.0 or later.

Active write back

With this setting, 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 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, it is enabled.

This setting corresponds to the PSMidSessionWriteBack setting in the .ini file.

This setting requires Profile management 3.0.0 or later.

Back to top

Profile Management\Profile handling

Delete locally cached profiles on logoff

Specifies whether locally cached profiles are deleted after logoff.

If this setting is enabled, a user's local profile cache is deleted after they have logged off. This is recommended for terminal servers. If this setting is disabled cached profiles

are not deleted.

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, cached profiles are not deleted.

This setting corresponds to the DeleteCachedProfilesOnLogoff setting in the .ini file.

This setting requires User Profile Manager 2.0.0 or later.

Local profile conflict handling

This setting 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 setting 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 setting 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 setting is set to **Rename local profile**, Profile management renames the local Windows user profile (in order to back it up) and then imports the profile from the user store.

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, existing local profiles are used.

This setting corresponds to the LocalProfileConflictHandling setting in the .ini file.

This setting requires User Profile Manager 2.0.0 or later.

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 (formerly known as Terminal 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 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, existing local and roaming profiles are migrated.

This setting corresponds to the MigrateWindowsProfilesToUserStore setting in the .ini file.

This setting requires User Profile Manager 2.0.0 or later.

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. If it consists only of NTUSER.DAT, ensure you don't include the file name in the path.

For example:

- Avoid: \\myservername\myprofiles\template\ntuser.dat

- Use: \\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.

If this setting is disabled, templates are not used. If this setting 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**.

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 template is used.

This setting corresponds to the TemplateProfilePath,TemplateProfileOverridesLocalProfile, and TemplateProfileOverridesRoamingProfile settings in the .ini file.

This setting requires User Profile Manager 2.0.0 or later.

Back to top

Profile Management\Advanced settings

Directory of the MFT cache file

Sets the path to the directory in which a cache file of the MFT directory content is stored.

Example: D:\Data\UPMCache

This cache is auto-created if not present by scanning the MFT upon service startup. If this setting is disabled, the cache is created in the folder where you installed Profile management.

If this setting is not configured here, the default value from the .ini file is used. If this setting is not configured here or in the .ini file, the file is stored in the installation directory.

This setting corresponds to the USNDBPath setting in the .ini file.

This setting requires User Profile Manager 1.0.0 or later.

Number of retries when accessing locked files

Sets the number of retries when accessing locked files.

If this setting is disabled the default value of five retries 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 value of five retries is used.

This setting corresponds to the LoadRetries setting in the .ini file.

This setting requires User Profile Manager 1.0.0 or later.

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 setting to force processing of index.dat and remove the extra cookies. The setting increases logoff times, so only enable it if you experience this issue.

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 processing of index.dat takes place.

This setting corresponds to the ProcessCookieFiles setting in the .ini file.

This setting requires Profile management 3.1 or later.

Delete Redirected Folders

If you configure folder redirection and select the Group Policy option **Move the contents of <folder name> to the new location**, by default Profile management does not delete the folder after its contents are moved. This results in two identically named items in the local profile, the folder itself and a shortcut to the folder. Because they appear side by side, these duplicates can confuse users. To prevent the confusion in these circumstances, enable this setting. Otherwise, do not enable it.

If this setting is configured here, the folder is deleted from the local profile when the user next logs on.

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 folder is not deleted from the local profile.

This setting corresponds to the DeleteRedirectedFolders setting in the .ini file.

This setting requires Profile management 3.2 or later.

Back to top

Profile Management\Log settings

Enable logging

Activation of this setting enables debug mode (verbose logging). In debug mode, extensive status information is logged in the log files in %SystemRoot%\System32\Logfiles\UserProfileManager.

Some logon and logoff processing is done in the context of the user using impersonation. Citrix recommends that you grant write permissions on the log folder for the users group so that Profile management can write to the log files during impersonation.

If this setting is disabled only errors are logged.

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, only errors are logged.

This setting corresponds to the LoggingEnabled setting in the .ini file.

This setting requires User Profile Manager 1.0.0 or later.

Log settings

Defines detailed log settings, those events or actions that Profile management logs in depth.

If this setting is not configured here, Profile management uses the settings from the .ini file. If this setting is not configured here or in the .ini file, errors and general information are logged.

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

This setting requires User Profile Manager 1.0.0 or later.

Maximum size of the log file

Sets the maximum size of the log file in bytes. If the log file grows beyond this 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 setting is disabled, the default value of 1 MB 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 of 1 MB is used.

This setting corresponds to the MaxLogSize setting in the .ini file.

This setting requires User Profile Manager 1.0.0 or later.

Path to log file

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

Some logon and logoff processing is done in the context of the user using impersonation. Citrix recommends that you grant write permissions on the log folder for the users group so that Profile management can write to the log files during impersonation.

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 location %SystemRoot%\System32\Logfiles\UserProfileManager is used.

This setting requires Profile management 2.1 or later.

Back to top

Profile Management\Registry

Exclusion list

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

Example: Software\Policies

If this setting 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.

This setting corresponds to the setting ExclusionListRegistry in the .ini file.

This setting requires User Profile Manager 1.0.0 or later.

Inclusion list

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

Example: Software\Adobe.

If this setting is enabled, only keys on this list are processed. If this setting is disabled, the complete HKCU hive is 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 of HKCU is processed.

This setting corresponds to the setting InclusionListRegistry in the .ini file.

This setting requires User Profile Manager 1.0.0 or later.

Back to top

Profile Management\File system

Exclusion list - files

List of files that are ignored during synchronization. File names can be specified as absolute paths or as paths relative to the user profile (%USERPROFILE%). Wildcards are allowed. Wildcards are applied recursively.

Examples:

- Desktop\Desktop.ini ignores the file Desktop.ini in the Desktop folder. C:\MyApp\myapp.tmp ignores the file myapp.tmp in the directory C:\MyApp.
- C:\MyApp*.tmp ignores all files with the extension .tmp in the folder C:\MyApp and its subfolders.

If this setting 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.

This setting corresponds to the SyncExclusionListFiles setting in the .ini file.

This setting requires User Profile Manager 2.0.0 or later.

Exclusion list - directories

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

Examples:

- Desktop ignores the Desktop folder in the user profile
- C:\MyApp\tmp ignores the folder C:\MyApp\tmp

If this setting 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.

This setting corresponds to the SyncExclusionListDir setting in the .ini file.

This setting requires User Profile Manager 2.0.0 or later.

Back to top

Profile Management\File system\Synchronization

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. You can use this setting to synchronize folders that are not part of the user profile. In addition, you can use it to include subfolders of excluded folders.

Paths on this list can be absolute or relative. Relative paths are interpreted as being relative to the user profile.

Examples:

- Desktop\exclude\include ensures that the subfolder called include is synchronized even if the folder called Desktop\exclude is not
- C:\MyApp\data ensures that the folder called data is synchronized even though the folder called C:\MyApp is not (because it is not part of the profile)

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

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, only non-excluded folders in the user profile are synchronized.

This setting corresponds to the SyncDirList setting in the .ini file.

This setting requires User Profile Manager 1.0.0 or later.

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 setting can be used to include files outside the user profile in the synchronization process. In addition, it 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
- C:\MyApp\myapp.cnf specifies the file myapp.cnf in the folder C:\MyApp\
- AppData\Local\MyApp*.cfg specifies all files with the extension .cfg in the profile folder AppData\Local\MyApp and its subfolders

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

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, only non-excluded files in the user profile are synchronized.

This setting corresponds to the SyncFileList setting in the .ini file.

This setting requires User Profile Manager 1.0.0 or later.

Folders to mirror

Profile management can mirror a folder relative to the profile's root folder. Use this setting for files whose contents index data and where separate instances of the data are likely to exist. 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.

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 mirrored.

This setting corresponds to the MirrorFoldersList setting in the .ini file.

This setting requires Profile management 3.1 or later.

Back to top

Profile Management\Streamed user profiles

Profile streaming

With profile streaming, users' profiles are fetched from the user store to the local computer only when they are needed. Registry entries are fetched immediately, but files and folders are only fetched when accessed by 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, it is disabled.

This setting corresponds to the PSEnabled setting in the .ini file.

This setting requires Profile management 3.0.0 or later.

Always cache

Optionally, to enhance the user experience, use this setting with the **Profile streaming** setting.

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 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, it is disabled.

This setting corresponds to the PSAlwaysCache setting in the .ini file.

This setting requires Profile management 3.0.0 or later.

Timeout for pending area lock files (days)

You can set a timeout period 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 (for example, when it goes down). Use this setting to prevent bloat in the pending area and to ensure the user store always contains the most up-to-date files.

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 value of one day is used.

This setting corresponds to the PSPendingLockTimeout setting in the .ini file.

This setting requires Profile management 3.0.0 or later.

Streamed user profile groups

Enter one or more Windows user groups.

If this setting is enabled, only the profiles of those groups' members are streamed. If this setting 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.

This setting corresponds to the PSUserGroupsList setting in the .ini file.

This setting requires Profile management 3.0.0 or later.

Back to top

Profile Management Glossary

As used in these Profile Management topics, the term *computer* refers to user devices (virtual or physical), virtual desktops, and servers that host published applications.

The term *Citrix user profile* refers to profiles that users receive when Profile management is installed and enabled. Citrix user profiles are different from local, roaming, or mandatory Windows profiles.

The general terms *to synchronize* and *to cache* refer to the act of downloading files from the user store, or uploading to it. The term *to 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.

Migration refers to the incorporation of Windows profile data into a Profile management deployment.

Upgrading refers to the process of installing one version of the software over an earlier version.

A *badly behaved application* is one that 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.