Profile Management 1912 LTSR

Copyright © 1997–2026. Citrix Systems, Inc. All Rights Reserved.

Contents

What's new 7

Cumulative Update 10 (CU10) 7

Fixed issues in 1912 LTSR CU10 8

Cumulative Update 9 (CU9) 8

Fixed issues in 1912 LTSR CU9 9

Cumulative Update 8 (CU8) 9

Fixed issues in 1912 LTSR CU8 10

Cumulative Update 7 (CU7) 10

Fixed issues in 1912 LTSR CU7 11

Cumulative Update 6 (CU6) 11

Fixed issues in 1912 LTSR CU6 12

Cumulative Update 5 (CU5) 12

Fixed issues in 1912 LTSR CU5 13

Cumulative Update 4 (CU4) 14

Fixed issues in 1912 LTSR CU4 14

Cumulative Update 3 (CU3) 15

Fixed issues in 1912 LTSR CU3 16

Cumulative Update 2 (CU2) 16

Fixed issues in 1912 LTSR CU2 17

Cumulative Update 1 (CU1) 18

Fixed issues in 1912 LTSR CU1 18

About this release 19

Fixed issues in 1912 LTSR 20

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Known issues 21

System requirements 22

Quick start guide 25

How Profile Management works 28

About profiles 29

Assign profiles 31

Profile Management architecture 32

Profile Management use cases 36

Access multiple resources 39

Logon diagram 40

Logoff diagram 43

Plan your deployment 45

Decide on a configuration 45

Pilot? Production? 46

Migrate profiles? New profiles? 48

Persistent? Provisioned? Dedicated? Shared? 49

Mobile? Static? 51

Which applications? 52

Review, test, and activate Profile Management 56

Plan for multiple platforms 56

Share Citrix® user profiles on multiple file servers 59

Administer profiles within and across OUs 60

Domain and forest support in Profile Management 62

High availability and disaster recovery with Profile Management 62

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Scenario 1 - Basic setup of geographically adjacent user stores and failover clusters 63

Scenario 2 - Multiple folder targets and replication 68

Scenario 3 - Disaster recovery 70

Scenario 4 - The traveling user 72

Scenario 5 - Load-balancing user stores 72

Plan folder redirection with Profile Management 74

Third-party directory, authentication, and file services 75

FAQs about profiles on multiple platforms and Profile Management migration 76

Install and set up 79

Files included in the download 83

Create the user store 83

Test Profile Management with a local GPO 85

Upgrade and migrate 86

Upgrade Profile Management 89

Migrate user profiles 91

Configure 93

Manage 93

Resolve conflicting profiles 94

Specify a template or mandatory profile 94

Choose a migration policy 96

Enable Profile Management 97

Configuration precedence 97

About the Profile Management .ini file 98

Include and exclude items 99

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Default inclusions and exclusions **101**

Include and exclude items **104**

Use wildcards **107**

Enable logon exclusion check **109**

Define which groups'profiles are processed **110**

Specify the path to the user store **111**

Migrate user store **114**

Automatic migration of existing application profiles **115**

Store certificates **117**

Stream user profiles **118**

Configure folder redirection **120**

Manage cookie folders and other transactional folders **122**

Configure offline profiles **125**

Configure the Customer Experience Improvement Program (CEIP) **126**

Configure active write back **127**

Configure cross-platform settings **128**

Operating systems and applications supported by cross-platform settings **130**

Create a definition file **132**

Application definition file structure **135**

Cross-platform settings - Case study **141**

Initial configuration **141**

Plan the new site **143**

Execute the plan **144**

Other considerations **149**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Force user logoffs 149

Synchronize file security attributes 150

Enable large file handling 150

Enable application profiler 151

Enable native Outlook search experience 151

Automatic backup and restore of Outlook search index database 155

Profile container 156

Policies 158

Profile Management policies 159

Profile Management policy descriptions and defaults 166

Integrate 186

Profile Management and Citrix Virtual Apps™ 187

Profile Management and Citrix Virtual Desktops™ 188

Profile Management and VDI-in-a-Box 192

Profile Management and UE-V 192

Profile Management and Citrix Content Collaboration™ 193

Profile Management and App-V 194

Profile Management and Provisioning Services 194

Preconfigure Profile Management on provisioned images 196

Profile Management and Self-service Plug-in 198

Profile Management and VMware 198

Profile Management and Outlook 199

Using Windows profiles with Password Manager and single sign-on 200

Firefox browser 203

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Google Chrome browser **204**

Secure **205**

Troubleshoot **208**

Check Profile Management settings **208**

Check Profile Management log files **209**

Check Windows events **214**

Troubleshoot common issues **229**

Perform advanced troubleshooting **234**

Contact Citrix Technical Support **238**

Profile Management best practices **241**

Glossary **246**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

What's new

November 6, 2024

Cumulative Update 10 (CU10) is the latest release of the Profile Management 1912 LTSR. CU10 adds 2 fixes compared to the 1912 CU9 release of Profile Management.

Cumulative Update 10 (CU10)

November 15, 2024

Release date: November 15, 2024

About this release

CU10 adds 2 fixes compared to the 1912 CU9 release of Profile Management.

Profile Management 1912 LTSR Cumulative Update 9

Profile Management 1912 LTSR Cumulative Update 8

Profile Management 1912 LTSR Cumulative Update 7

Profile Management 1912 LTSR Cumulative Update 6

Profile Management 1912 LTSR Cumulative Update 5

Profile Management 1912 LTSR Cumulative Update 4

Profile Management 1912 LTSR Cumulative Update 3

Profile Management 1912 LTSR Cumulative Update 2

Profile Management 1912 LTSR Cumulative Update 1

Profile Management (initial release)

Known issues in this release

Deprecation and removals

Citrix Product Subscription Advantage Eligibility Dates

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Fixed issues in 1912 LTSR CU10

September 7, 2025

Compared to: Profile Management 1912 LTSR CU9

Profile Management 1912 LTSR CU10 contains all fixes included in the 1912 LTSR initial release, CU1, CU2, CU3, CU4, CU5, CU6, CU7, CU8, CU9 plus the following, new fix:

- After you upgrade the Microsoft Teams app and the VDA version, new Microsoft Teams version 2.1 or later does not open within the Citrix session. [CVADHELP-24833]
- You might encounter multiple Event Tracing for Windows (ETW) event registrations for the same event in Citrix Profile Management. [CVADHELP-25331]

Cumulative Update 9 (CU9)

September 7, 2025

Release date: April 30, 2024

About this release

CU9 adds 1 fix compared to the 1912 CU8 release of Profile Management.

Profile Management 1912 LTSR Cumulative Update 8

Profile Management 1912 LTSR Cumulative Update 7

Profile Management 1912 LTSR Cumulative Update 6

Profile Management 1912 LTSR Cumulative Update 5

Profile Management 1912 LTSR Cumulative Update 4

Profile Management 1912 LTSR Cumulative Update 3

Profile Management 1912 LTSR Cumulative Update 2

Profile Management 1912 LTSR Cumulative Update 1

Profile Management (initial release)

Known issues in this release

Deprecation and removals

Citrix Product Subscription Advantage Eligibility Dates

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Fixed issues in 1912 LTSR CU9

April 29, 2024

Compared to: Profile Management 1912 LTSR CU8

Profile Management 1912 LTSR CU9 contains all fixes included in the 1912 LTSR initial release, CU1, CU2, CU3, CU4, CU5, CU6, CU7, CU8 plus the following, new fix:

- After upgrading a VDA to version 1912 LTSR CU8, user profiles might fail to load from the store. Instead, users are provided with local profiles. [CVADHELP-23877]

Cumulative Update 8 (CU8)

September 7, 2025

Release date: September 11, 2023

About this release

CU8 adds 10 fixes compared to the 1912 CU7 release of Profile Management.

Profile Management 1912 LTSR Cumulative Update 7

Profile Management 1912 LTSR Cumulative Update 6

Profile Management 1912 LTSR Cumulative Update 5

Profile Management 1912 LTSR Cumulative Update 4

Profile Management 1912 LTSR Cumulative Update 3

Profile Management 1912 LTSR Cumulative Update 2

Profile Management 1912 LTSR Cumulative Update 1

Profile Management (initial release)

Known issues in this release

Deprecation and removals

Citrix Product Subscription Advantage Eligibility Dates

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Fixed issues in 1912 LTSR CU8

September 7, 2025

Compared to: Profile Management 1912 LTSR CU7

Profile Management 1912 LTSR CU8 contains all fixes included in the 1912 LTSR initial release, CU1, CU2, CU3, CU4, CU5, CU6, CU7, plus the following, new fixes:

- The **Reset Profile** button in Citrix Director might be grayed out for some users. [CVADHELP-20497]
- The **upmjit.sys** module might prevent Windows terminals from launching. [CVADHELP-21352]
- After upgrading Profile Management or Windows OS version, the profile containers might fail to load. [CVADHELP-21836]
- With the profile container-based Profile Management enabled, users might have access to the profile files and folders of other users. [CVADHELP-21913]
- Profile Management might reset the customized Outlook OST path during logon. [CVADHELP-21974]
- The automatic migration of existing application profiles feature might not work after you upgrade Microsoft Windows 10 to version 22H2 or later. [CVADHELP-22510]
- When you sign out and sign into Profile Management again, the deleted file might still be present in the user store. [CVADHELP-22618]
- After you upgrade a VDA to 1912 LTSR CU4 or 2203 LTSR CU2 with Profile Management enabled, a PowerShell window might pop up for a short amount of time. The issue occurs during the desktop session logon. [CVADHELP-22620]
- Attempts to sign in with the same user name on two different domains in a forest might fail. [CVADHELP-22965]
- When you configure a customized path for Outlook OST files through Group Policy or the registry and if the customized path contains user environment variables, Microsoft Outlook profiles might fail to load. [CVADHELP-23072]

Cumulative Update 7 (CU7)

September 7, 2025

Release date: March 15, 2023

© 1997–2026 Citrix Systems, Inc. All rights reserved.

About this release

CU7 adds one fix compared to the 1912 CU6 release of Profile Management.

Profile Management 1912 LTSR Cumulative Update 6

Profile Management 1912 LTSR Cumulative Update 5

Profile Management 1912 LTSR Cumulative Update 4

Profile Management 1912 LTSR Cumulative Update 3

Profile Management 1912 LTSR Cumulative Update 2

Profile Management 1912 LTSR Cumulative Update 1

Profile Management (initial release)

Known issues in this release

Deprecation and removals

Citrix Product Subscription Advantage Eligibility Dates

Fixed issues in 1912 LTSR CU7

September 7, 2025

Compared to: Profile Management 1912 LTSR CU6

Profile Management 1912 LTSR CU7 contains all fixes included in the 1912 LTSR initial release, CU1, CU2, CU3, CU4, CU5, CU6, plus the following, new fix:

- After installing the Microsoft Windows update, KB5010342 or the update it replaces, the Explorer.exe process might cause high CPU usage. [CVADHELP-21047]

Cumulative Update 6 (CU6)

September 7, 2025

Release date: October 31, 2022

© 1997–2026 Citrix Systems, Inc. All rights reserved.

About this release

CU6 adds three fixes compared to the 1912 CU5 release of Profile Management.

Profile Management 1912 LTSR Cumulative Update 5

Profile Management 1912 LTSR Cumulative Update 4

Profile Management 1912 LTSR Cumulative Update 3

Profile Management 1912 LTSR Cumulative Update 2

Profile Management 1912 LTSR Cumulative Update 1

Profile Management (initial release)

Known issues in this release

Deprecation and removals

Citrix Product Subscription Advantage Eligibility Dates

Fixed issues in 1912 LTSR CU6

September 7, 2025

Compared to: Profile Management 1912 LTSR CU5

Profile Management 1912 LTSR CU6 contains all fixes included in the 1912 LTSR initial release, CU1, CU2, CU3, CU4, CU5, plus the following, new fixes:

- When you launch Edge Chromium on a published desktop with Profile Management enabled, duplicate profiles might be created once you log back on. The issue occurs as Profile Management might fail to delete local profiles during logoff. [CVADHELP-19865]
- Profile Management might not recreate folders used in Microsoft Folder Redirection even when the folder redirection policy is disabled. [CVADHELP-20036]
- Logon data might not be captured in Session Details under the Monitor tab in Citrix Director. As a result, this data might not be available on Citrix Analytics for Performance™, as well. [CVADHELP-20107]

Cumulative Update 5 (CU5)

September 7, 2025

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Release date: March 09, 2022

About this release

CU5 adds 5 fixes compared to the 1912 CU4 release of Profile Management.

Profile Management 1912 LTSR Cumulative Update 4

Profile Management 1912 LTSR Cumulative Update 3

Profile Management 1912 LTSR Cumulative Update 2

Profile Management 1912 LTSR Cumulative Update 1

Profile Management (initial release)

Known issues in this release

Deprecation and removals

Citrix Product Subscription Advantage Eligibility Dates

Fixed issues in 1912 LTSR CU5

September 7, 2025

Compared to: Profile Management 1912 LTSR CU4

Profile Management 1912 LTSR CU5 contains all fixes included in the 1912 LTSR initial release, CU1, CU2, CU3, CU4, plus the following, new fixes:

- Attempting to launch desktops using Profile Management might fail with this error message:

  The Group Policy Client service failed the sign-in.

  Access is denied.

  [CVADHELP-18398]

- The Service Host (svchost.exe) process might exit unexpectedly with an access violation because of the faulting upmperf.dll module. [CVADHELP-18453]
- The isessionmetrics.exe process might cause a memory leak in VDAs. [CVADHELP-18713]
- Profile Management Service might exit unexpectedly due to an unhandled exception. [CVADHELP-18813]

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- On a Windows 10 20H2 desktop, when you configure the user store path with a **!CTX_OSNAME!** variable, Profile Management might create folder names on the user store with incorrect information. The following might be observed:
  - For Version CU3, the new profiles might contain operating system as Win10RS6.
  - For Version CU4, the new profiles might contain operating system as Win10_2009.

  [CVADHELP-19016]

Cumulative Update 4 (CU4)

September 7, 2025

Release date: November 03, 2021

About this release

CU4 adds 10 fixes compared to the 1912 CU3 release of Profile Management.

Profile Management 1912 LTSR Cumulative Update 3

Profile Management 1912 LTSR Cumulative Update 2

Profile Management 1912 LTSR Cumulative Update 1

Profile Management (initial release)

Known issues in this release

Deprecation and removals

Citrix Product Subscription Advantage Eligibility Dates

Fixed issues in 1912 LTSR CU4

September 7, 2025

Compared to: Profile Management 1912 LTSR CU3

Profile Management 1912 LTSR CU4 contains all fixes included in the 1912 LTSR initial release, CU1, CU2, CU3, plus the following, new fixes:

- With Citrix Profile Management installed, redirected folders might be recreated under the local user profile. [CVADHELP-16861]

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- After enabling the **Delete excluded files or folders** policy, the initial logon attempt using Profile Management might take longer. This issue occurs if the user profile contains unnecessary files slowing the logon. [CVADHELP-17230]
- When you change settings in the Group Policy Object, the previous policy settings on the VDI might not cancel in the user registry. The issue occurs if the registry is offline when you cancel the policy settings. [CVADHELP-17358]
- Verification of Active Directory group membership might fail when user devices in offline mode connect to the network during logon. As a result, Profile Management also fails. [CVADHELP-17364]
- When migrating application profiles using the **Automatic migration of existing application profiles** policy, some application profiles and settings might not be migrated successfully. [CVADHELP-17593]
- The Microsoft Windows Search service might exit unexpectedly on Windows 10 version 21H1. [CVADHELP-17687]
- This fix addresses a security vulnerability in the Citrix Profile Management WMI plugin installer. For more information, see Knowledge Center article CTX319750. [CVADHELP-17728]
- Changing the folder redirection path through the Citrix Profile Management policy might result in deletion of data in the legacy folder redirection path. [CVADHELP-17833]
- This fix addresses a security vulnerability in the Citrix Profile Management installer. For more information, see Knowledge Center article CTX319750. [CVADHELP-17939]
- The Universal Windows Platform applications (UWP app) might fail to work on Microsoft Windows 11. [CVADHELP-18298]

Cumulative Update 3 (CU3)

September 7, 2025

Release date: May 12, 2021

About this release

CU3 adds seven fixes compared to the 1912 CU2 release of Profile Management.

Profile Management 1912 LTSR Cumulative Update 2

Profile Management 1912 LTSR Cumulative Update 1

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Profile Management (initial release)

Known issues in this release

Deprecation and removals

Citrix Product Subscription Advantage Eligibility Dates

Fixed issues in 1912 LTSR CU3

September 7, 2025

Compared to: Profile Management 1912 LTSR CU2

Profile Management 1912 LTSR CU3 contains all fixes included in the 1912 LTSR initial release, CU1, CU2, plus the following, new fixes:

- When you navigate to **Control Panel > System and Security > System > Advanced system settings > User Profiles**, the profile for the logged-in user shows a question mark for the Size field. The other user profiles show the correct sizes. [CVADHELP-13993]
- When a folder on the **Folders to Mirror** list is not present in the user store during logons, the local user profile is deleted. [CVADHELP-15248]
- When you enable the **Automatic migration of existing application profiles** policy and migrate the existing profiles, Microsoft Outlook settings might be lost. The issue occurs during the second and subsequent logons after the migration. [CVADHELP-15723]
- With **Desktop** added to the **Exclusion list –directories** policy, an error might occur when users attempt to save any changes in a published application or desktop. [CVADHELP-15792]
- Windows user credentials might remain after being removed from the Credential Manager. [CVADHELP-16083]
- Folders created before enabling **Delete excluded files or folders** through the **Logon Exclusion Check** policy but excluded by the **Exclusion list –directories** or **Enable Default Exclusion list –directories** policy might not be deleted. [CVADHELP-16439]
- New files created with the **Large File Handling - Files to be created as symbolic links** policy setting, might not sync during logoff. [CVADHELP-16526]

Cumulative Update 2 (CU2)

September 7, 2025

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Release date: November 19, 2020

About this release

CU2 adds nine fixes compared to the 1912 CU1 release of Profile Management.

Profile Management 1912 LTSR Cumulative Update 1

Profile Management (initial release)

Known issues in this release

Deprecation and removals

Citrix Product Subscription Advantage Eligibility Dates

Fixed issues in 1912 LTSR CU2

September 7, 2025

Compared to: Profile Management 1912 LTSR CU1

Profile Management 1912 LTSR CU2 contains all fixes included in the 1912 LTSR initial release, CU1, plus the following, new fixes:

- When you add **Appdata\local\temp** to the **Exclusion list - directories**, Profile Management does not create the **Appdata\local\temp** folder in the user profile and runtime errors occur for some applications such as Microsoft Outlook. The issue occurs during second or subsequent logons with the Delete locally cached profiles on logoff policy enabled. [CVADHELP-14054]
- When you log on to a session using a temporary profile, an empty user profile folder might be created under C:\Users. Profile Management deletes the temporary profile on logoff, leaving behind the empty user profile folder. [CVADHELP-14297]
- With the Redirect the **AppData(Roaming) folder** redirection policy enabled, some tiles might disappear from the Start menu. The issue occurs when you log on to a Windows Server 2016 or 2019 machine running Citrix Virtual Apps and Desktops™ 1912 or earlier. [CVADHELP-14336]
- With search index roaming for Outlook enabled for a VDA for multi-session OS using Profile Management, logons might be slow and attempts to launch published applications might fail. [CVADHELP-14610]
- Profile Management does not synchronize the subkeys of a registry key present in the **Registry inclusion list**. For example, when you add Software\Citrix to the **Registry inclusion list**, only HKEY_CURRENT_USER\SOFTWARE\Citrix is saved in the user store. The subkeys are not stored. [CVADHELP-14815]

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- When Citrix Virtual Apps™ Optimization is in use, Profile Management might fail to save registry changes. The issue occurs when the path to Citrix Virtual Apps optimization definitions is not accessible or the path file is invalid. Registry changes are also not saved when the **Enable Virtual Apps Optimization** and the **Active write back** policies are enabled. [CVADHELP-15087]
- Attempts to mount the OutlookOST.vhdx or the OutlookSearchIndex.vhdx file might fail intermittently with a 0x80070020 error. The issue occurs when you log off from a session and launch another session immediately. [CVADHELP-15145]
- When you enable the **Delete locally cached profiles on logoff** policy and add the Downloads folder to the **Exclusion list - directories**, Profile Management does not create the **Downloads** folder when synchronizing profiles from the user store to the local. As a result, the File Explorer reports the error message **Location is not available** when you click **Downloads** under **This PC** or **Quick Access**. [CVADHELP-15386]
- When you configure a user store path as a relative path to the home directory through the **Migrate user store** policy, Citrix Profile Management fails to migrate the user store during logons. [CVADHELP-15476]

Cumulative Update 1 (CU1)

September 7, 2025

Release date: May 7, 2020

About this release

Profile Management 1912 LTSR Cumulative Update 1 (CU1) fixes more than five issues reported since the initial release of the 1912 LTSR.

Profile Management (initial release)

Known issues in this release

Deprecation and removals

Citrix Product Subscription Advantage Eligibility Dates

Fixed issues in 1912 LTSR CU1

September 7, 2025

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Compared to: Profile Management 1912 LTSR initial release

Profile Management 1912 LTSR CU1 contains all fixes included in the 1912 LTSR initial release, plus the following, new fixes:

- With Profile Management enabled, when you launch some applications (such as Calculator and Sticky Notes) from the Start menu, they might exit unexpectedly. The issue occurs with VDA Version 1912 running on Microsoft Windows 10. [CVADHELP-13947]
- After you upgrade a VDA from Version 1808 to Version 1912, Citrix Profile Management might exit unexpectedly with an Event ID 1000. [CVADHELP-14112]
- With the **Logon Exclusion Check** policy enabled, Profile Management might fail to synchronize files under an excluded folder. Instead, Profile Management might delete or ignore the files on logon. The issue occurs with files that match paths containing wildcards in the List of **Files to synchronize** policy. [CVADHELP-14347]
- Attempts to create a user profile on Microsoft Windows 10 Version 2004 might fail. [CVADHELP-14235]
- You might encounter the following issues:
  - File Type Association (FTA) roaming fails.
  - Attempts to open Calculator, Sticky Notes, and similar apps from the Start menu might fail.

  The issues are fixed in Profile Management 1912 CU1 for new user profiles. For existing profiles created by Profile Management 1912, you must enable the permission inheritance of ALL APPLICATION PACKAGES to the **HKEY_CURRENT_USER\SOFTWARE\Microsoft** registry key manually:

  1. Log on to the VDA with the target user account.
  2. Open Registry Editor.
  3. Navigate to **HKEY_CURRENT_USER\SOFTWARE\Microsoft**.
  4. Right-click the **Microsoft** key, select **Permissions** -> **Advanced**, and select **Enable inheritance**.
  5. Click **Apply** and then **OK**.

  [UPM-2695]

About this release

September 7, 2025

© 1997–2026 Citrix Systems, Inc. All rights reserved.

What's new

What's new in 1912 LTSR

This release includes performance enhancements and bug fixes.

Fixed issues in 1912 LTSR

May 2, 2020

Compared to: Profile Management 1909

Profile Management 1912 LTSR contains the following fixes:

- The **Folders to mirror policy** and the **Exclusion list** policies do not work together. The issue occurs because Profile Management does not support using the **Folders to mirror** policy along with either the **Exclusion list** –**files** nor the **Exclusion list** –**directories** policy. [UPM-1708]
- With **Path to user store** enabled, attempts to log on to a machine might fail with the following error message: "ProcessLogon: Locking userstore area failed. The data is invalid."The issue occurs when you specify the path to the user store in this format: `C:\Users\<environment-specific strings>` or `C:\Users<environment-specific strings>`. [UPM-1711]
- When you use the search index in Profile Management, the event log might report multiple errors. [CVADHELP-11442]
- If you log on to a server and then log off, the server might freeze until the message "Please wait for the Citrix Profile Management"appears. When more users log on and log off, the server might freeze more frequently and become unresponsive. As a result, you must reset the server. [CVADHELP-12351]
- Profile Management does not cancel copy operations to the profile store after it fails to load a corrupt local profile **NTUSER.DAT**. Instead, Profile Management copies the corrupt registry hive to the profile store and overwrites the **NTUSER.DAT** file and its backup. [CVADHELP-12781]
- Even though you add a registry path to the exclusion list, the registry path might still be saved. The issue occurs when there is a backslash (\) present at the end of the registry path. [CVADHELP-12835]
- With the **Profile streaming** policy enabled in Profile Management, attempts to download a file in Internet Explorer 11 might fail. [CVADHELP-12970]

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- With active write back for registry entries enabled, the **active write back** policy might not work in Profile Management. The issue occurs when the timer related to active write back cannot reach the timeout value. As a result, the timeout value cannot be captured. [CVADHELP-13175]
- The Citrix Desktop Service (BrokerAgent.exe) might exit unexpectedly and the following exception occurs until you restart the Citrix Profile Management Service:
  - System_Management_Instrumentation_ni!WmiNative.WbemProvider.WmiNative.IWbemServices.Crea
    [CVADHELP-13210]

Known issues

September 7, 2025

The following known issues exist in this release:

- Attempts to use the Outlook Search index roaming feature might fail. The issue occurs when domain computers have no access permission to the VHDX files. To work around the issue, manually grant Domain Computers the full control of the folder where the VHDX files are stored. [CVADHELP-15257]
- On a Windows 10 20H2 desktop, when you configure the user store path with a **!CTX_OSNAME!** variable, Profile Management might create folder names on the user store with incorrect information. The following might be observed:
  - For Version CU3, the new profiles might contain operating system as Win10RS6.
  - For Version CU4, the new profiles might contain operating system as Win10_2009.

  [CVADHELP-19016]
- If you are using user profiles created by Profile Management 1912, you might encounter the following issues:
  - File Type Association (FTA) roaming fails.
  - Attempts to open Calculator, Sticky Notes, and similar apps from the Start menu might fail.

  The issues occur because Profile Management 1912 disables permission inheritance of ALL APPLICATION PACKAGES to the **HKEY_CURRENT_USER\SOFTWARE\Microsoft** registry key. The ALL APPLICATION PACKAGES group consequently loses its permission to all child keys of **HKEY_CURRENT_USER\SOFTWARE\Microsoft**, for example, **HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows**.

  As a workaround, do the following:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. For new users, ask Citrix Technical Support for a private package to create profiles.
2. For existing users, enable the permission inheritance of ALL APPLICATION PACKAGES to the **HKEY_CURRENT_USER\SOFTWARE\Microsoft** registry key manually:
   a) Log on to the VDA with the target user account.
   b) Open Registry Editor.
   c) Navigate to **HKEY_CURRENT_USER\SOFTWARE\Microsoft**.
   d) Right-click the **Microsoft** key, select **Permissions** -> **Advanced**, and select **Enable inheritance**.
   e) Click **Apply** and then **OK**. [UPM-2695]

- You are prompted to restart your machine after installing a VDA. However, the Profile Management service might not start after you restart the machine. When this issue happens, you can see that the following message about Event 7000 appears in the system Event log: "The ctxProfile service failed to start due to the following error: The service did not respond to the start or control request in a timely fashion."As a workaround, change the value of the following registry key to a greater number (for example, 300,000):

  - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\
  - Name: ServicesPipeTimeout
  - Type: REG_DWORD
  - Value: 300000 [UPM-1454]

- Some sections of the Start menu might not populate. To work around this issue, run the `gpupdate /force` command from the command prompt. [UPM-1933]

System requirements

September 7, 2025

Software requirements

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

- **Desktops** - Microsoft Windows 10, Windows 8.1, and Windows 7 Service Pack 1.

  In Citrix Virtual Desktops™ environments, Windows Store applications (also known as UWP apps) are supported.

- **Servers** - Standard and Datacenter Editions of Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, and Windows Server 2008 R2 Service Pack 1.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

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

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

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

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

Citrix® product compatibility

Profile Management can be used with the following Citrix products:

- Citrix Virtual Desktops
- Citrix Virtual Apps™
- VDI-in-a-Box

For the compatibility matrix of Profile Management and Citrix Virtual Apps and Desktops, see Additional Lifecycle Information for Citrix Profile Management.

For more information about using this Current Release (CR) in a Long Term Service (LTSR) environment and other FAQs, see Knowledge Center article.

Downloads

To download Profile Management

1. Navigate to the Citrix download page.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Log on to My Account. Your account must be associated with the licensing entitlement for the Citrix product that you have deployed. If your account is not associated with your license entitlement, contact Citrix Customer Service.
3. In Find Downloads, select your product and select Components as the download type.
4. Download the latest version of Profile Management.

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

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

Cross-platform settings

To use the cross-platform settings feature in this release, install Microsoft Core XML Services (MSXML) 6.0 Service Pack 1 or later on all computers running the Profile Management Service. This component is part of Microsoft .NET Framework 3.5 and is required to process definition files.

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

Migrating existing profiles to Citrix user profiles

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

- Windows roaming profiles
- Local profiles based on any of the following operating systems:
    - Windows 10

© 1997–2026 Citrix Systems, Inc. All rights reserved.

  - Windows 8
  - Windows 7
  - Windows Vista
  - Windows XP
  - Windows Server 2016
  - Windows Server 2012 R2
  - Windows Server 2012
  - Windows Server 2008 R2
  - Windows Server 2008
  - Windows Server 2003
- Citrix user profiles created with User Profile Manager 2.0

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

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

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

Quick start guide

September 7, 2025

This is a quick reference to installing and configuring Profile Management.

Prerequisites

Verify that all system requirements are met. For details, see System requirements.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Installation

Profile Management is included with the installation of the Virtual Delivery Agent (VDA). For VDAs, to install or upgrade Profile Management, simply install or upgrade your VDA software.

Deploying Profile Management consists of installing an .msi file and either an .adm, or an .admx file. To do this, follow the steps in Install and set up.

> **Note:**
>
> To avoid potential conflicts, add the Citrix Profile Management process (`%ProgramFiles%\Citrix\User Profile Manager\UserProfileManager.exe`) to your antivirus software's exclusion list. For more information, see Citrix Antivirus Best Practices.

Configuration

Decide on where to configure Profile Management

There are three locations you can configure Profile Management:

- Using a GPO in Active Directory
- Using policies in Citrix Studio

  For instructions on configuring Profile Management using a GPO in Active Directory or policies in Citrix Studio, see Knowledge Center article CTX222893.
- Using Workspace Environment Management™ (WEM)

  For instructions on configuring Profile Management using WEM, see Knowledge Center article CTX229258.

Citrix recommends that you choose only one of the three ways to configure Profile Management.

Create the user store

Recommendations on creating secure user stores –including creating a file share and setting folder permissions –are available in Microsoft article Deploying Roaming User Profiles. These minimum recommendations ensure a high level of security for basic operation.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Specify the path to the user store

Enable Profile Management

Verify basic settings

Enable logging for troubleshooting. If the Enable logging policy is disabled, only errors are logged.

To verify your basic settings, follow these steps:

1. After Profile Management is configured, log on to a VDA and run **gpupdate /force** as an administrator.
2. Log off and log back on to the VDA.
3. Go to the default log file path, **C:\Windows\System32\Logfiles\UserProfileManager**, open the **pm.log** file, look for **logon events** and verify that the following messages are present:

   "Starting logon processing…"

   "Finished logon processing successfully in [s]: "

To expand on your Profile Management configuration, you can:

Plan your Profile Management deployment

To plan a Profile Management deployment, decide on a set of policy settings that, together, form a configuration that is suitable for your environment and users. The **Automatic configuration** feature in User profiles simplifies some of this decision-making for Citrix Virtual Desktops deployments.

To determine the recommended approach to deploying, answer the following basic questions about your environment:

- Pilot? Production?
- Migrate profiles? New profiles?
- Persistent? Provisioned? Dedicated? Shared?
- Mobile? Static?
- Which applications?

To stream user profiles, see Stream user profiles.

To enable Active Write Back, see Configure active write back.

To specify a mandatory profile, see Specify a template or mandatory profile.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configure exclusions

For details, see Include and exclude items.

Configure folder redirection

For details, see Configure folder redirection.

Configure applications

For details, see Enable native Outlook search experience.

Verify Profile Management settings

Follow the steps in Verify-basic-settings to do verification.

Check the **pm_configure.log** file for policy settings. Verify that the following messages are present:

- Configuration value read from Policy: LoggingEnabled=
- Configuration value read from INI file: CEIPEnabled=
- Configuration value PSAlwaysCache set neither in policy nor in INI file. Defaulting to:

Troubleshoot

For details, see Troubleshoot.

How Profile Management works

September 7, 2025

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 experience different settings depending on the resource silo they access.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

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

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

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

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

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

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

About profiles

January 22, 2026

A Windows user profile is a collection of folders, files, and registry and configuration settings that define the environment for a user who logs on with a user account. These settings can 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 folder redirection. However, if folder redirection is not used these settings are stored within the user profile.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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. Except mandatory profiles, a distinct profile typically exists for each user. 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 might occur if the same profile is assigned to a user within a Remote Desktop Services session and a local session.

Profile versions

Versions of Microsoft Windows user profiles are as follows:

- Version 5 –Windows 10
- Version 4 –Windows 8.1 and Windows Server 2012 R2
- Version 3 - Windows 8 and Windows Server 2012
- Version 2 - Windows Vista, Windows 7, Windows Server 2008, and Windows Server 2008 R2
- Version 1 –Operating systems earlier than Windows Vista and Windows Server 2008

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

However, the namespace is different between Version 1 and later profiles. This folder structure was changed in the later operating systems to provide user-specific folders isolated for user and application data. Version 1 profiles store data in the root folder, **Documents and Settings**. Version 2 profiles store data in a more intuitively named folder called **Users**. For example, the

© 1997–2026 Citrix Systems, Inc. All rights reserved.

folder contents of AppData\Local in Windows Vista is the same as the contents of Documents and Settings\<username>\Local Settings\Application Data in Windows XP.

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

Assign profiles

September 7, 2025

What methods can I use in Windows to assign profiles to users?

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

You can assign profiles to users in several ways:

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

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

- **Remote Desktop Services**. To assign Remote Desktop Services profiles on Windows Server 2008 R2, use the GPO setting Set path for Remote Desktop Services Roaming User Profile. It is located in Computer Configuration\Administrative Templates\Windows Component\Remote Desktop Services\Remote Desktop Session Host\Profiles. On earlier multi-session operating systems, use the setting Set path for TS Roaming Profiles, which is located in Computer Configuration\Administrative Templates\Windows Components\Terminal Services.

  To configure profiles for individual users, you can also set Set path for TS Roaming Profiles on the individual accounts in the User Account Properties pages in AD. However, typically it is much better to make this assignment in GP.

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

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

What is the priority order for delivering profiles to domain users if more than one method is used?

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

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

Profile Management architecture

September 7, 2025

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

Important information about Profile Management stores

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

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Folder structure of the user store

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

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

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

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

Folder	Notes
\	The root of a profile in the user store.
\UPM_Profile	This folder contains files and folders from the profile.
\UPM_Drive_C	This folder contains any included items from outside the profile (in this case from drive C). This folder is present during upgrades from Profile Management 4.x or earlier. Managing items outside the profile is not supported in Profile Management 5.0.
\Pending	This folder contains the lock file, any pending files, and the stamp file if the streaming feature is in use.

Some examples are shown in this table.

Example Folder Name	Notes
\UPM_Profile\Data	The synchronized content of the **Data** folder in the user profile.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

Pending area

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

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

Folder structure of the user store with multiple platforms

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

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

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

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The user store and AD forests

Citrix user profiles cannot be managed across forests. They can be managed across domains in the same forest allowing multiple users with the same logon name to access the same resources in the forest. This involves uniquely identifying profiles with the %USERDOMAIN% and %USERNAME% variables in the path to the user store.

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

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

Localizing the user store

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

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Version 1 English Folder	User Store Folder	Full Path Relative to the User Profile
Accessibility	Accessibility_upm_var	\Start Menu\Programs\Accessories
Accessories	Accessories_upm_var	\Start Menu\Programs
Administrative Tools	AdminTools_upm_var	\Start Menu\Programs
Application Data	AppData_upm_var	\Local Settings
Cookies	Cookies_upm_var	
Desktop	Desktop_upm_var	
Entertainment	Entertainment_upm_var	
Favorites	Favorites_upm_var	\Start Menu\Programs\Accessories
History	History_upm_var	
Links	Links_upm_var	
Local Settings	LocalSettings_upm_var	\Local Settings
My Documents	MyDocuments_upm_var	\Favorites
My Music	MyMusic_upm_var	
My Pictures	MyPictures_upm_var	
My Videos	MyVideos_upm_var	\My Documents
NetHood	NetHood_upm_var	\My Documents
PrintHood	PrintHood_upm_var	\My Documents
Programs	Programs_upm_var	
Recent	Recent_upm_vars	
Start Menu	StartMenu_upm_var	\Start Menu
Templates	Templates_upm_var	
Temporary Internet Files	TemporaryInternetFiles_upm_var	
SendTo	SendTo_upm_var	
Startup	Startup_upm_var	\Local Settings
System Tools	SystemTools_upm_var	
		\Start Menu\Programs
		\Start Menu\Programs\Accessories

Profile Management use cases

September 7, 2025

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

of these scenarios:

- Citrix Virtual Apps™ with published applications
- Citrix Virtual Apps with published desktops
- Citrix Virtual Apps with applications streamed into an isolation environment
- Applications streamed to Citrix Virtual Desktops™
- Applications installed on Citrix Virtual Desktops
- Applications streamed to physical desktops
- Applications installed locally on physical desktops

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

- **Multiple sessions** - The user accesses multiple Citrix Virtual Apps 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** - The last write to the roaming profile causes all settings to be saved. Therefore, roaming profiles might not retain the right data if multiple sessions are open and interim changes are made. In addition, settings might 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.

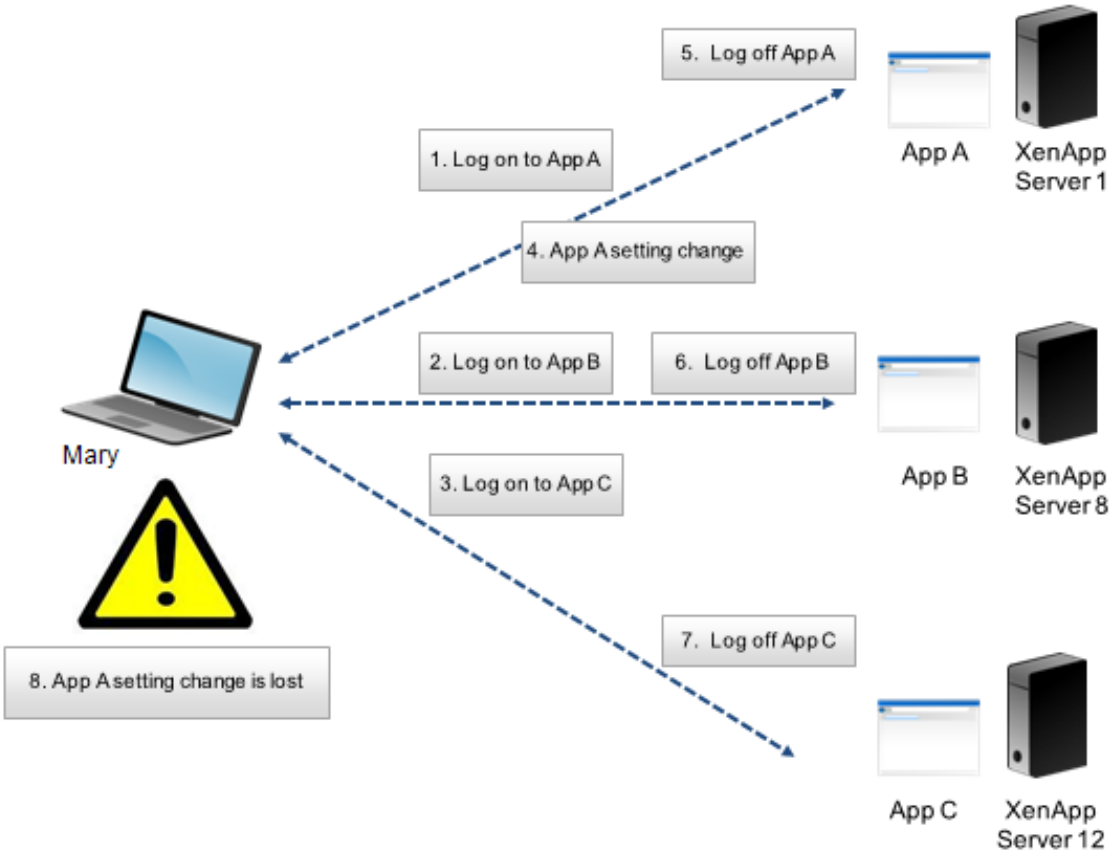
Multiple sessions

Especially in large environments, it might be necessary for users to open multiple sessions to access different applications that are housed on different Citrix Virtual Apps servers, whether in the same farm or multiple farms. Where possible, consider application isolation or streaming to house applications on the same Citrix Virtual Apps server to allow users to access all applications from a single server and thus a single session. However, this might 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 Citrix Virtual Apps servers, the impact on profiles must be ascertained.

The following diagram illustrates an example where application settings can be lost when multiple sessions exist.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



For example, Mary wants to access App A, App B, and App C and she is routed to Server 1, Server 8, and Server 12 respectively. Upon logon to each application, Mary's Terminal Services roaming profile is loaded onto each server and folders are redirected for each session. When Mary is logged on to App A on Server1, Mary changes Setting1 and logs off that session. Mary then completes work in the other two applications and logs off.

At logoff, the change that Mary made within the session on Server 1 is overwritten because the settings within the last closed session are retained, not the interim change. When Mary logs on to App A 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

“Last write 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 various ways, and user frustration can mount as the number of devices accessed increases.

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

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

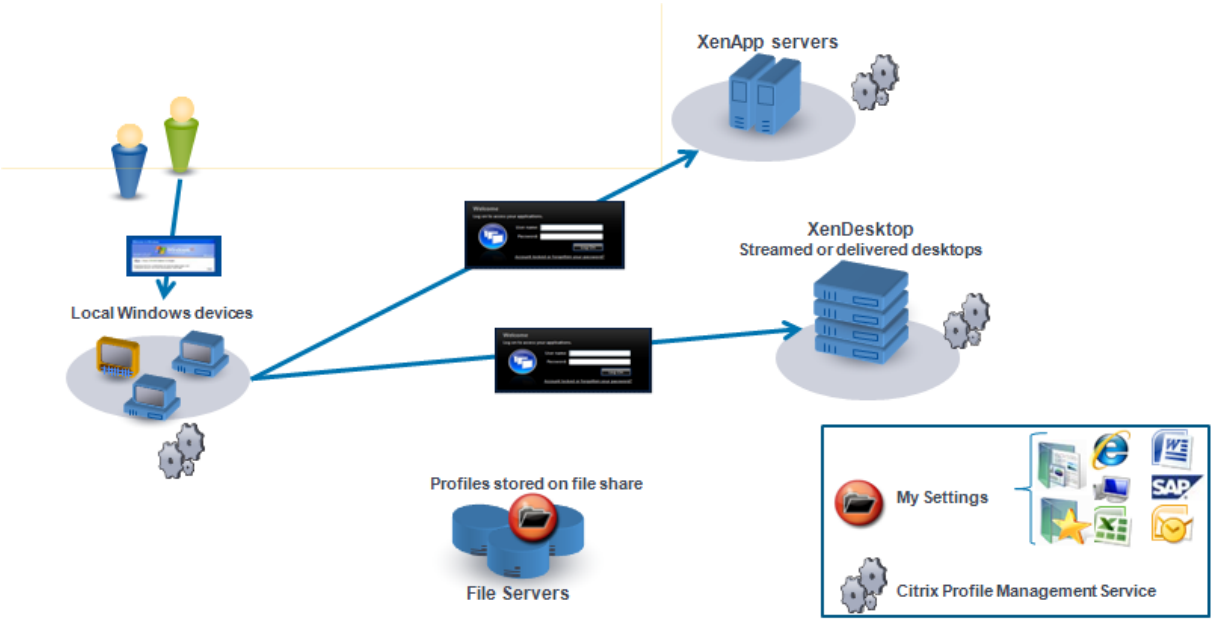
Access multiple resources

September 7, 2025

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

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.



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

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

Logon diagram

September 7, 2025

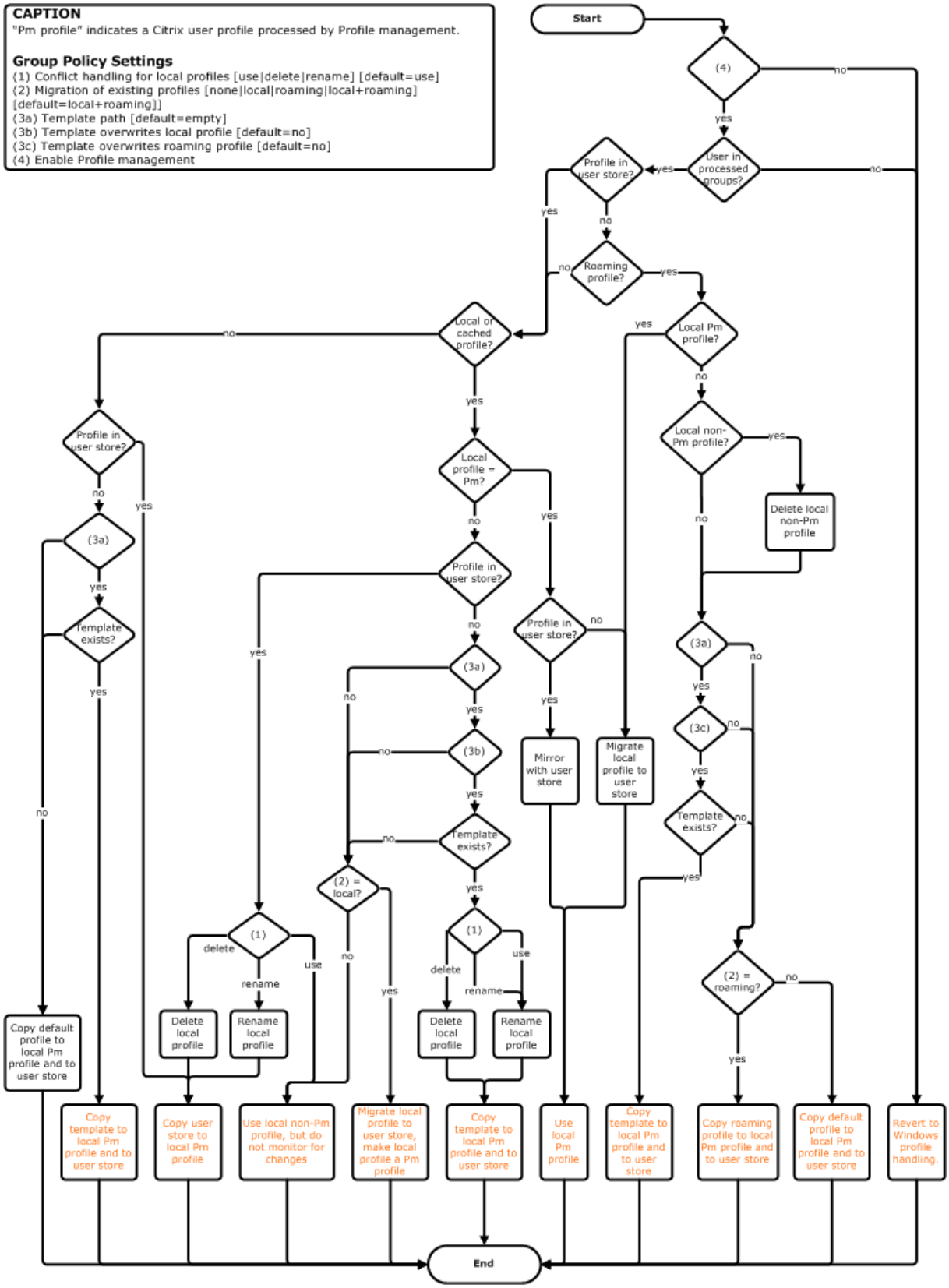
This diagram helps you work out the details of your user profile migration strategy. It also explains these aspects of performance:

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Logoff diagram

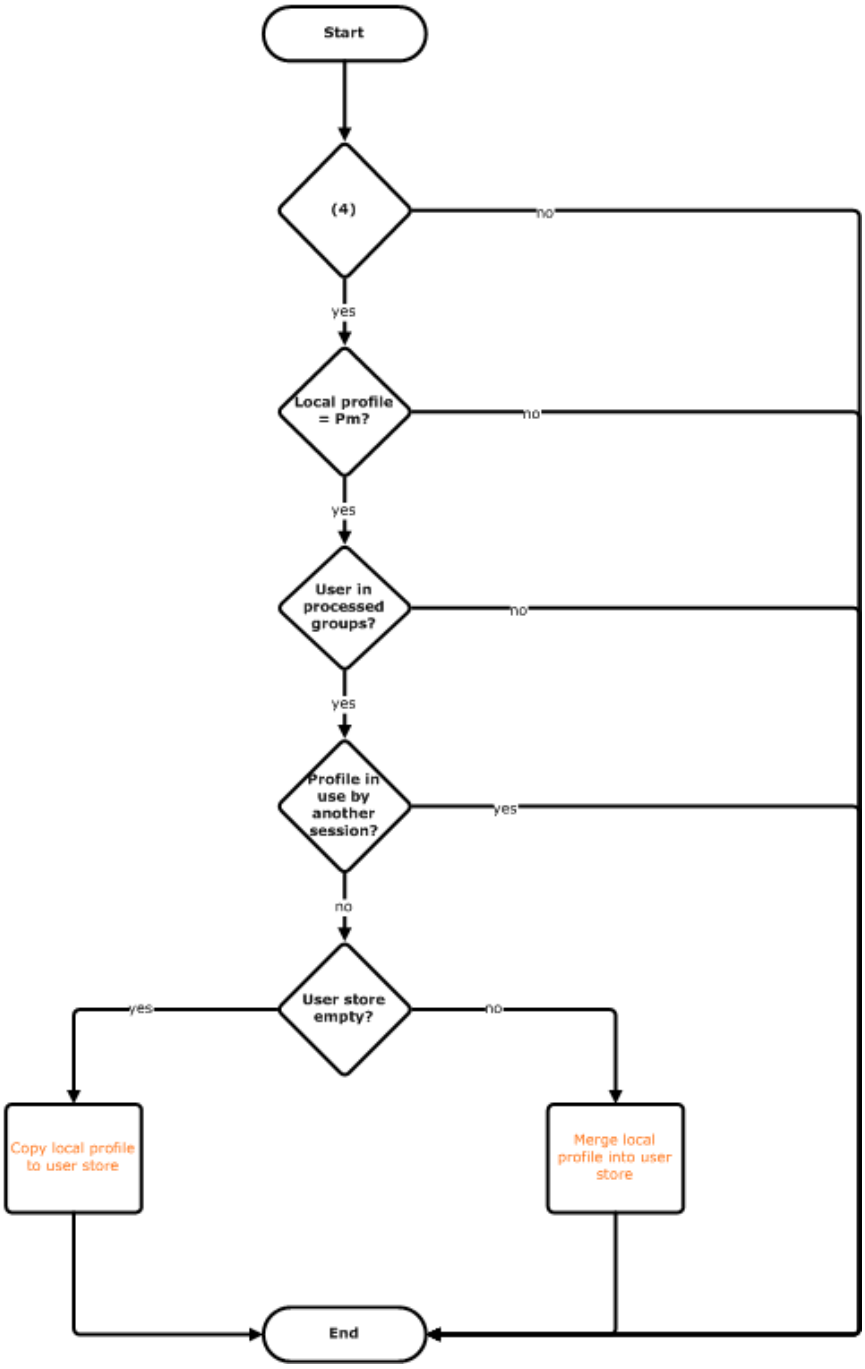
September 7, 2025

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

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



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Plan your deployment

September 7, 2025

To plan a Profile Management deployment, you decide on a set of policy settings that together form a configuration that is suitable for your environment and users. The automatic configuration feature simplifies some of this decision-making for Citrix Virtual Desktops deployments. As a guide to carrying out this important task on any deployment, see Decide on a configuration.

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

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

Plan a pilot study with the .ini file

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

Important: If you intend to use the .ini file (UPMPolicyDefaults_all.ini) for evaluation purposes, rename the file before you switch to using Group Policy (GP) in a production environment. For example, rename the file to UPMPolicyDefaults_all_old.ini. Renaming the file allows you to be certain that only production settings are applied, and that no settings you specified during your evaluation are used.

If the file is not renamed, Profile Management examines it for any settings not configured in Group Policy and adopts any non-default settings it finds. So, to eliminate the risk of unwanted settings being introduced, configure all settings you want to use in your production environment using Group Policy, not the .ini file.

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

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

Decide on a configuration

September 7, 2025

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

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

Depending on the answer to each question, you configure Profile Management differently as explained in the remaining topics in this section. You configure only the policies that fit the answers to these questions; you can leave other policies in their default setting. For a list of policies that you do not configure, see Manage.

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

- Review, test, and activate Profile Management
- Troubleshoot

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 Knowledge Center article 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 Organizational Unit (OU). And consider configuring Profile Management by using a single Group Policy Object (GPO) attached to that OU. If your answers to these questions are different, consider grouping the computers into separate OUs.

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

Pilot? Production?

September 7, 2025

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The aim of a pilot deployment is to be able to demonstrate a solution quickly and reliably. An important goal might 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 assumes that enough storage is available in users' home directories and that no file-server quotas are applied. Citrix does not recommend the use of file-server quotas with profiles. The reasons for this are given in Share Citrix user profiles on multiple file servers.

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

- Profile Management architecture
- Create the user store
- Specify the path to the user store
- High availability and disaster recovery with Profile Management

Policies: Processed groups, Excluded groups

The complexity of production deployments means that you might need to phase the rollout of Profile Management, rather than release it to all users at the same time. You might tell users that they 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 EULA not built-in license checking. You might 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 restricted by invitation to a small group of users, possibly from several departments, where no single, representative AD group can be used. In this case, leave the Processed groups and Excluded groups policies unconfigured. Profile Management performs no checking on group membership and all users are processed.

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

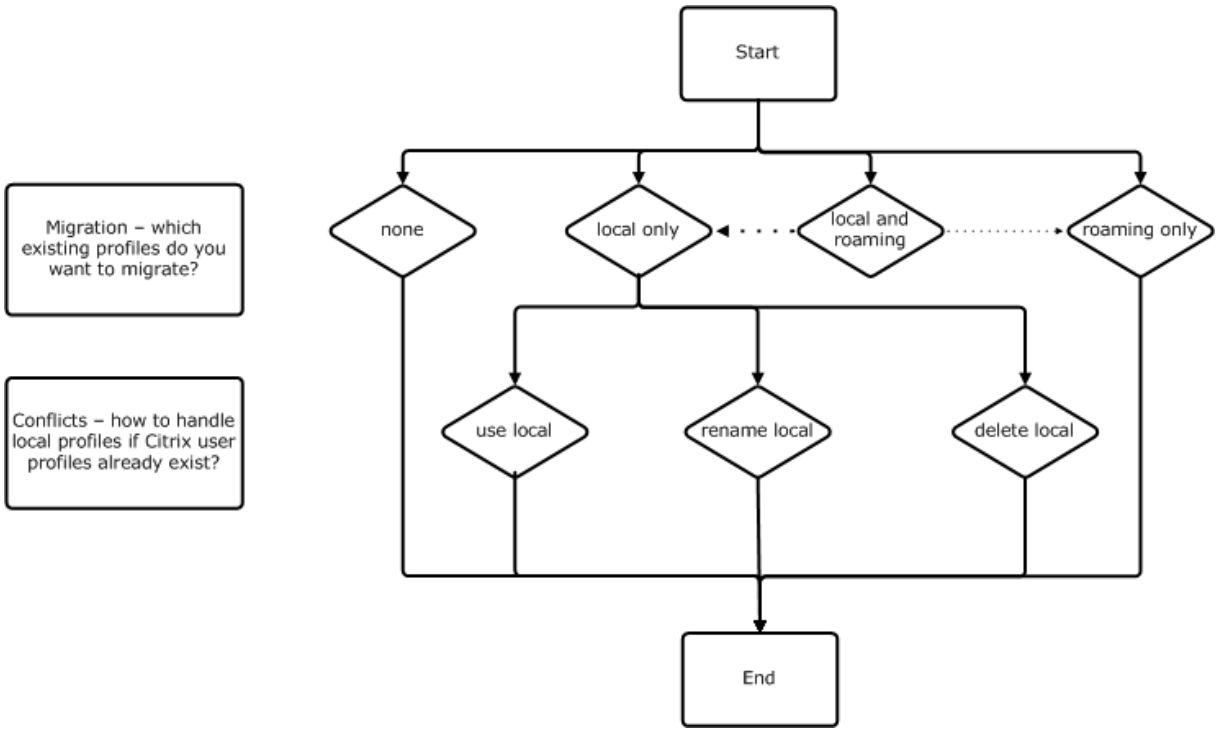
Migrate profiles? New profiles?

September 7, 2025

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 might need to migrate existing profiles into the Profile Management environment and preserve the personalizations that have built up over many years.

If you decide to migrate existing profiles, configure the Migration of existing profiles and the 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 Specify a template or mandatory profile. If you

© 1997–2026 Citrix Systems, Inc. All rights reserved.

do not create a template, Profile Management gives users the default Windows profile. If no template is required, leave this policy disabled.

The **Template profile** policy is similar to the **Path to user store** policy. This policy specifies the location of a profile that can be used as the basis for creating a user profile when the user first logs 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, you must perform tasks such as identifying the applications that users access. You must configure the registry states, shortcuts, and desktop settings in the profile accordingly. You must set permissions on profile folders and modify users' logon scripts.

> **Note:**
>
> When selecting mandatory profiles in Citrix Virtual Desktops™ deployments, we recommend that you use Citrix Studio rather than the Profile Management .adm or .admx file.

Persistent? Provisioned? Dedicated? Shared?

September 7, 2025

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

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

Together, these two factors define the following machine types:

- **Both persistent and dedicated** - Examples are single-session OS machines with a static assignment and a Personal vDisk that are created with Machine Creation Services (in Citrix Virtual Desktops™), desktops with Personal vDisks that are created with VDI-in-a-Box, physical workstations, and laptops
- **Both persistent and shared** - Examples are multi-session OS machines that are created with Machine Creation Services (in Citrix Virtual Desktops), and Citrix Virtual Apps™ servers

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Both provisioned and dedicated** - Examples are single-session OS machines with a static assignment but without a Personal vDisk that are created with Provisioning Services (in Citrix Virtual Desktops)
- **Both provisioned and shared** - Examples are multi-session OS machines with a random assignment that are created with Provisioning Services (in Citrix Virtual Desktops), desktops without Personal vDisks that are created with VDI-in-a-Box, and Citrix Virtual Apps servers

The following Profile Management policy settings are suggested guidelines for the different machine types. They usually work well, but you might want to deviate from them as your deployment requires.

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

Policy	Both persistent and dedicated	Both persistent and shared	Both provisioned and dedicated	Both provisioned and shared
Delete locally cached profiles on logoff	Disabled	Enabled	Disabled (note 5)	Enabled
Profile streaming	Disabled	Enabled	Enabled	Enabled
Always cache	Enabled (note 1)	Disabled (note 2)	Disabled (note 6)	Disabled
Active write back	Disabled	Disabled (note 3)	Enabled	Enabled
Process logons of local administrators	Enabled	Disabled (note 4)	Enabled	Enabled (note 7)

Notes

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. Disable Delete locally cached profiles on logoff. This retains locally cached profiles. Because the machines are assigned to individual users, logons are faster if their profiles are cached.
6. Disable Always cache. However, you can ensure that large files are loaded into profiles as soon as possible after logon by enabling this policy and using it to define a file size limit (in MB). Any file this size or larger is cached locally as soon as possible.
7. Enable Process logons of local administrators except for profiles of users who roam between Citrix Virtual Apps servers. In this case, disable this policy.

Mobile? Static?

September 7, 2025

Are your machines permanently connected to the Active Directory domain? Laptops and similar mobile devices probably are not. Similarly, some deployments might 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 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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

Important: Do not enable
Offline profile support with Citrix VDI-in-a-Box. This policy is not suitable for this product because desktops created with it do not have persistent local storage.

The static case

Policy: Offline profile support

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

Policy: Streamed user profile groups

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

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

Policy: Timeout for pending area lock files

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

Policy: Active write back

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

Which applications?

September 7, 2025

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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. The decisions you take depend on where the applications store persistent customizations, which can either be in the registry or in the file system.

Analyze and understand your users' applications thoroughly to establish where the applications store their settings and users' customizations. Use a tool such as Process Monitor to monitor application binaries. Google is another resource. For information on Process Monitor, see https://docs.microsoft.com/en-us/sysinternals/downloads/procmon.

Once you understand how the applications behave, use inclusions to define which files and settings are processed by Profile Management. 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 include the subfolders of AppData\Local explicitly.

Simple applications

Simple applications are those applications 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 Include and exclude items.

Legacy applications

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 Manage cookie folders and other transactional folders.

Cross-platform applications

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

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

Java and Web Applications

Java applications can leave many small files in a profile, which can dramatically increase 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**. 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**. An absolute path on a local volume. Examples: C:\BadApp*.txt, C:\BadApp\Database\info.db.
- **Registry Relative**. Refers to a path within the HKCU hive. Examples: Software\Policies, Software\Adobe.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Flag**. Uses flags 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	Application Type - Legacy	Application Type - 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 Use wildcards.

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 Include and exclude items.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 to configure your Profile Management deployment. The questions are listed in Decide on a configuration. Once you have answered all 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. For a list of policies that you must not configure, see Policies not requiring configuration in Manage.

Review, test, and activate Profile Management

September 7, 2025

This topic assumes that you have answered all questions about your deployment listed in Decide on a configuration. And you 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. You can use the .ini file to test. 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

September 7, 2025

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 single-session operating system (OS) and a multi-session OS. Some settings might 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 might 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 might 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 system, different add-ons are installed and expected by a document.

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

Even though the platforms are installed identically, if an application is configured differently on each, errors might 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 users can modify that part of the menu. Adding custom links (to executables or documents) is common. 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. The reason is that the path to the document is relative to another system, or it is a network path that is inaccessible.

By default, Profile Management does not save the content of the Start menu folder because links pointing to executables are often computer-dependent. However, in situations where the systems are 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 at https://helgeklein.com/blog/2009/09/citrix-user-profile-

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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, saving the **Quick Launch** toolbar might not be desirable because the links might 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.

What types of profiles to create?

Important: Because of the difference in their structure, we recommend 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 might 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 fails 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 must create separate profiles for the three different versions of the Word application.

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

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Share Citrix® user profiles on multiple file servers

September 7, 2025

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

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

The user store can be located across multiple file servers, which has benefits in large deployments where many profiles must be shared across the network. Profile Management defines the user store with a single setting, **Path to user store**, so you define multiple file servers by adding attributes to this setting. You can use any LDAP attributes that are defined in the user schema in Active Directory. For more information, see https://docs.microsoft.com/en-us/windows/win32/adschema/attributes-all?redirectedfrom=MSDN.

Suppose that 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 https://docs.microsoft.com/en-us/sysinternals/downloads/adexplorer.

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

You can, however, use the related Active Directory property, #homeDirectory#. So, if you want to store profiles on the same share as the users'HOME directories, set the path to the user store as #homeDirectory#\profiles.

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

- Specify the path to the user store
- Administer profiles within and across OUs
- High availability and disaster recovery with Profile Management

Administer profiles within and across OUs

September 7, 2025

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 or .admx file to a subset of computers in the OU. WMI filtering is a capability of Group Policy Management Console with Service Pack 1 (GPMC with SP1).

For more information on WMI filtering, see https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc779036(v=ws.10) and https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc758471(v=ws.10).

For more information on GPMC with SP1, see https://www.microsoft.com/en-us/download/details.aspx?id=21895.

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

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

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

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

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

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

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

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

Across OUs

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

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Domain and forest support in Profile Management

September 7, 2025

Profile Management supports domain and forest functional levels of Windows Server 2008 and Windows Server 2012. Older operating systems are unsupported.

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

High availability and disaster recovery with Profile Management

September 7, 2025

As a prerequisite, familiarize yourself with the structure of the user store and how to create it. For more information, see Profile Management architecture and Create the user store.

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

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

Profile Management assumes that it operates in an environment that is reliable. Principally, this reliability applies to the availability of Active Directory (AD) and a networked user store (NUS). When either 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 might be affected by the same issues as affect Microsoft roaming profiles. Unless stated to the contrary, Profile Management does not resolve such issues.

In particular, note the following:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Profile Management support is limited to the scenarios where roaming profiles are also supported.
- The cache option for offline files must be disabled on roaming user profile shares. The same restriction applies to Profile Management shares.
- A roaming profile is not loaded from a DFS share. The same restriction applies to Profile Management shares. For more information, see https://support.microsoft.com/en-us/help/2533009.

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

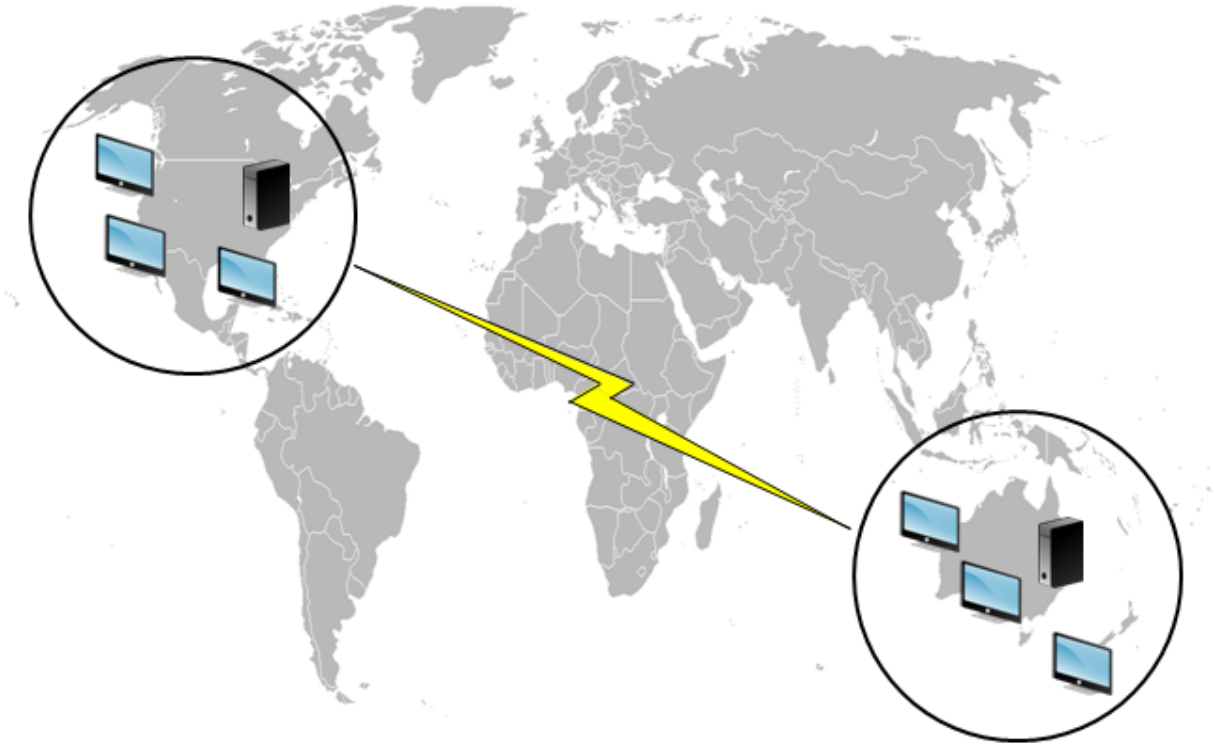
March 11, 2026

"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. The aim is to reduce latency and to minimize the traffic sent over the intercontinental link to Australia or New Zealand (ANZ).

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Option 1 –DFS Namespaces

Background reading

For an overview of the Microsoft DFS Namespaces technology, see DFS Namespaces overview.

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. It 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.

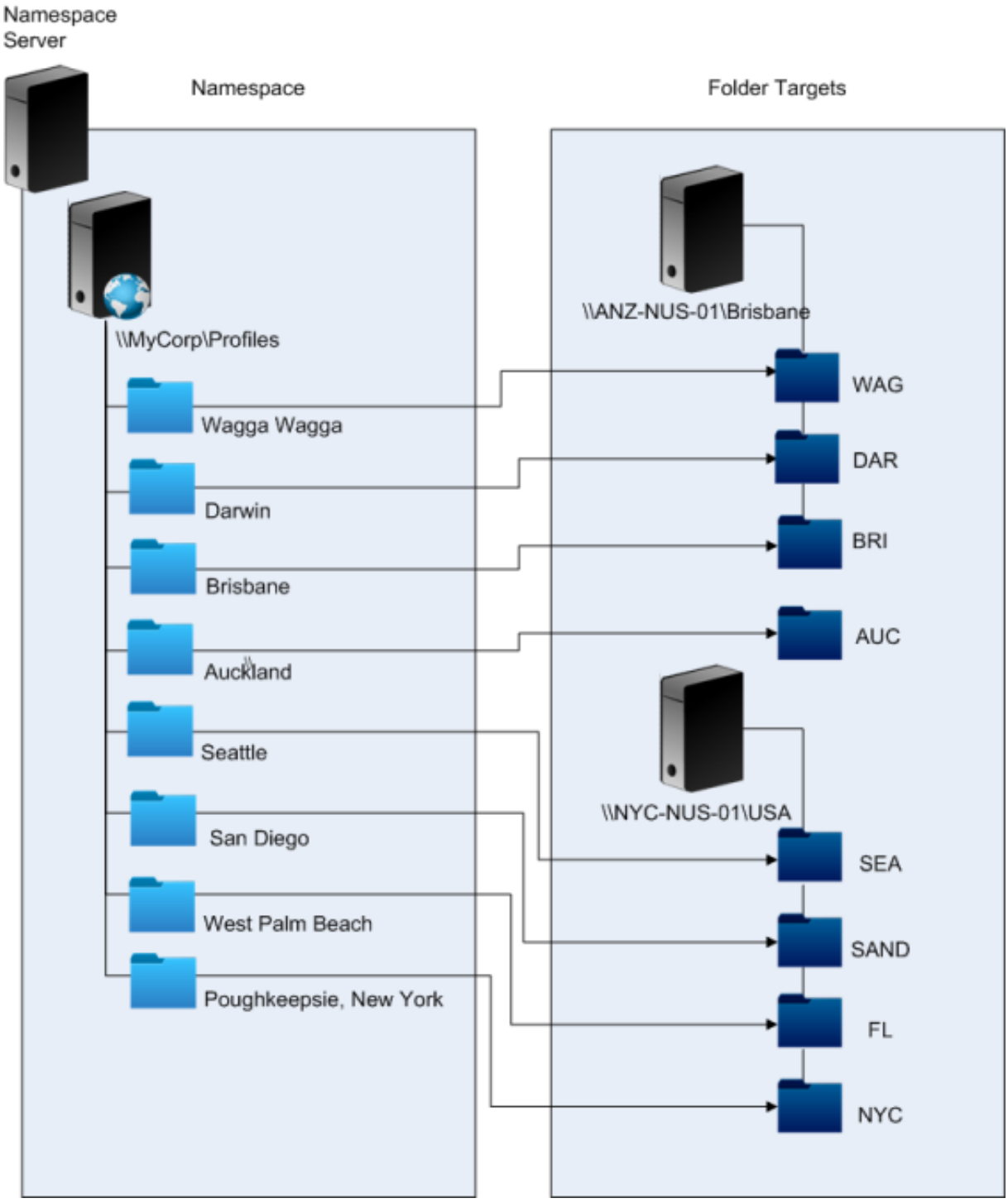
We might have the following locations configured in Active Directory (part of the user records).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



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

\\MyCorp\Profiles\#l#

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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. It works so long as you are sure that, for any given user, every desktop and server are guaranteed to belong to the same site.

This technique fails if, say, a user normally based at Poughkeepsie visits Wagga Wagga. Their laptop profile might come from Brisbane, but the profile used by their published applications might 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. The reason is that 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 Deploying a two-node clustered file server.
- For information about choosing a namespace type, see https://docs.microsoft.com/en-us/windows-server/storage/dfs-namespaces/choose-a-namespace-type.

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. Domain-based namespaces do not support the use of failover clusters as namespace servers. Folder targets might be hosted on failover clusters, regardless of the type of namespace server.

Important: The state of file locks might 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. It is possible that a failover at a critical point might result in profile corruption.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Scenario 2 - Multiple folder targets and replication

September 7, 2025

"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 need to 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 https://docs.microsoft.com/en-us/windows-server/storage/dfs-namespaces/tuning-dfs-namespaces.

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 might 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. However, file replication has been used in some specialized deployments in which only a single session can be guaranteed and
Active write back is disabled. For information on these special cases, contact Citrix Consulting.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Option 2 - Distributed file system replication

Background reading

- For an overview of Distributed File System Replication (DFSR), see https://docs.microsoft.com/en-us/windows-server/storage/dfs-replication/dfsr-overview.
- For a statement of support about replicated user profile data, see https://techcommunity.microsoft.com/t5/ask-the-directory-services-team/microsoft-8217-s-support-statement-around-replicated-user/ba-p/398230.
- To understand why DFSR does not support distributed file locking, see https://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 option 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 replication makes it suitable for maintaining a disaster recovery site, for example. It 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 might be modified infrequently.
  Important: Active-active DFSR is not supported.

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

At various points in its operation, Profile Management requires certain files to be locked in the NUS to coordinate updates to the (shared) user store. Typically these updates take place when a session starts and ends, and in the middle of a session if active write-back is enabled. Since distributed file locking is not supported by DFS Replication, Profile Management can only select one target as an NUS. This set 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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

replication) is suitable for Profile Management only as part of a disaster recovery system. Other uses are not supported.

Scenario 3 - Disaster recovery

September 7, 2025

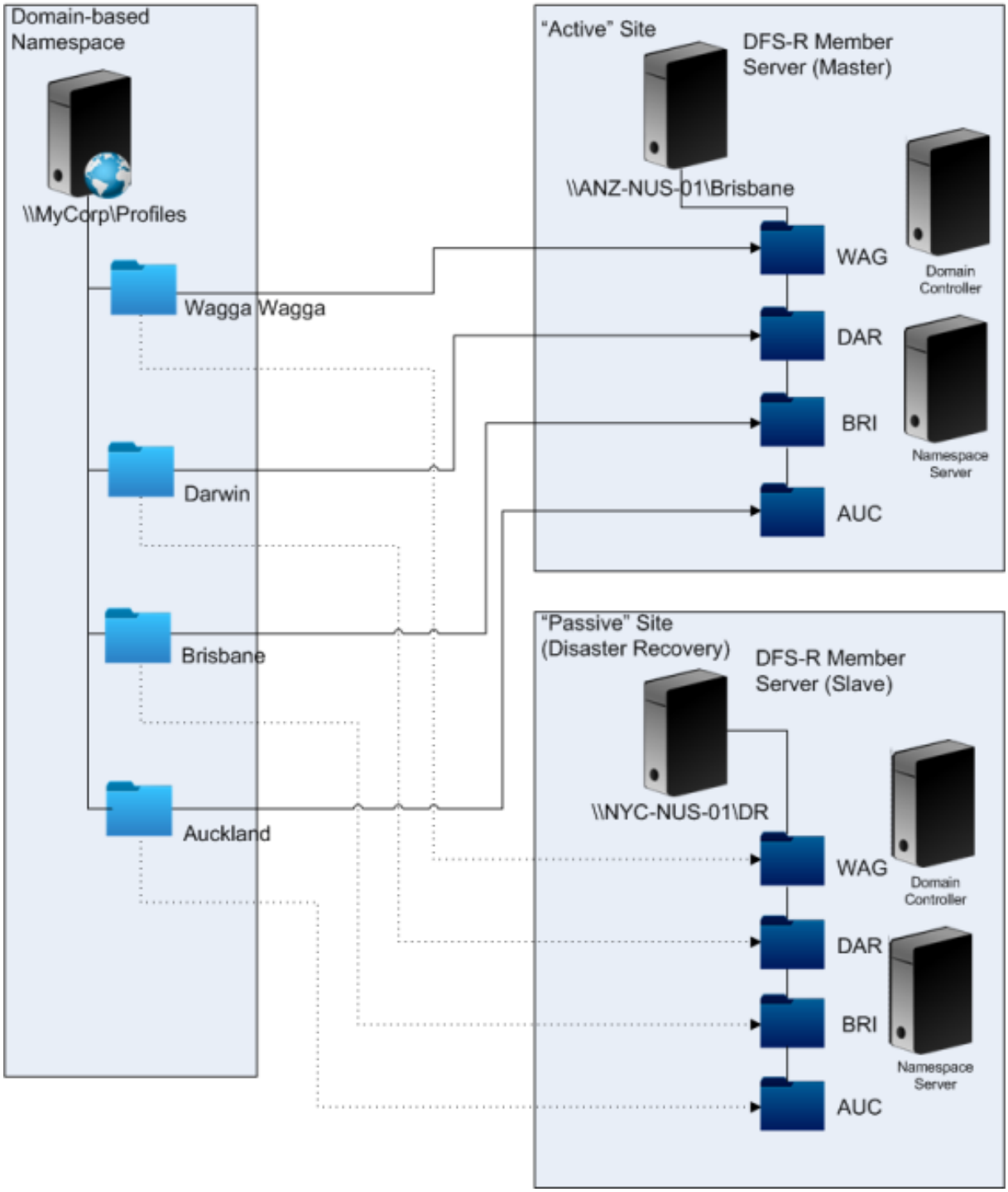
"How do I set up a full disaster recovery site to handle Citrix® user profiles?"

Profile Management supports key features required for disaster recovery (DR):

- **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**. 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.) You can include a namespace server in each site, including the DR site. The servers all support the same view of the namespace.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

September 7, 2025

"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 might be aggregated from multiple locations. They typically roam their desktop session from one site to another. But many of their applications are hosted on back-end servers that have no awareness of the current location of the user's desktop.

Furthermore, the user might reconnect to disconnected sessions, probably hosted at their home location. 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

September 7, 2025

"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, see DFS Namespaces overview.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

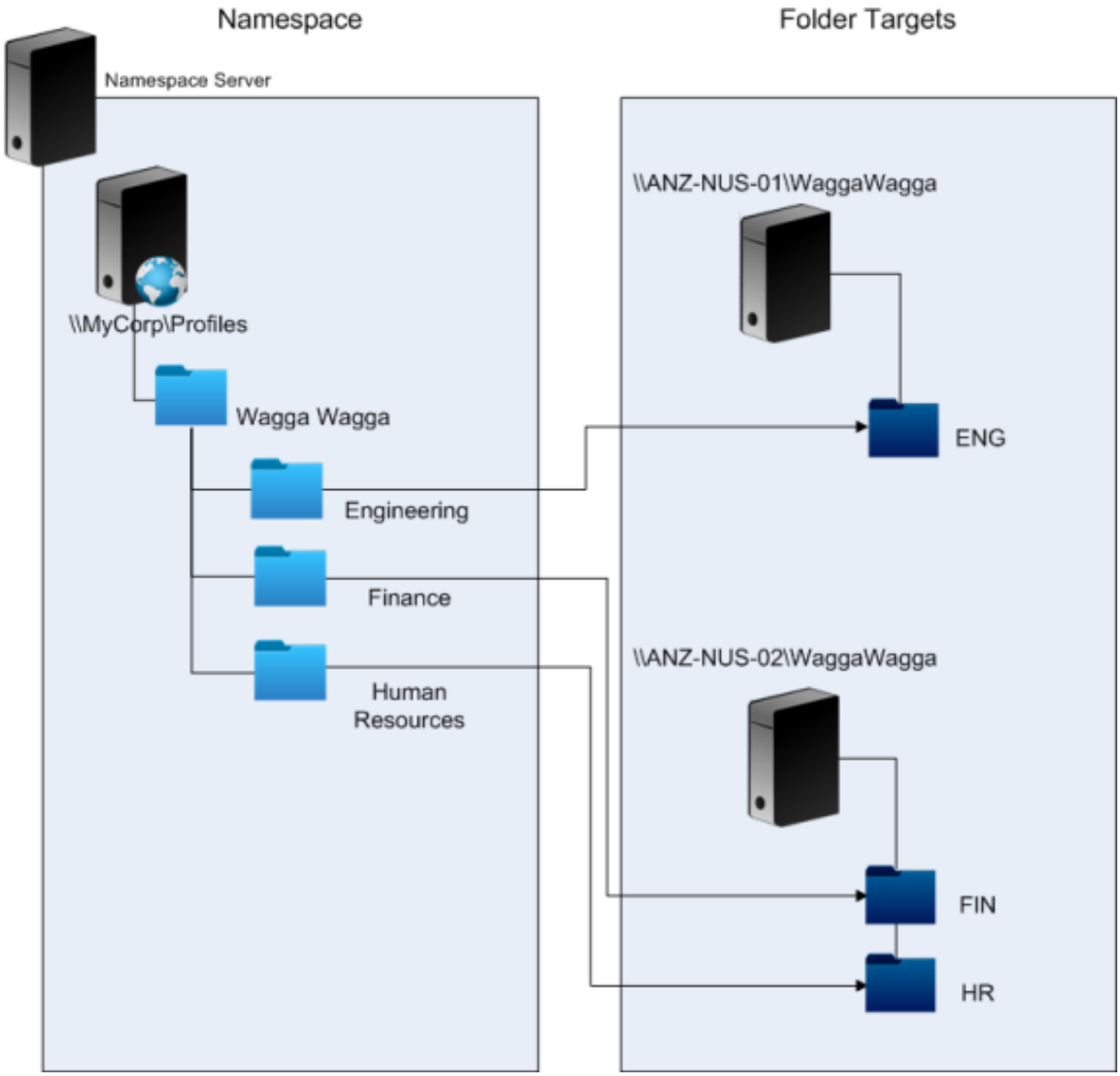
Unlike Scenario 1, this scenario has a single site that is large enough to require multiple NUSs. Using DFS namespaces, we can improve on the solution in Scenario 1.

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.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Once you complete the setup, you configure the Path to user store setting as:

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

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

Plan folder redirection with Profile Management

September 7, 2025

Profile Management supports folder redirection and its use is encouraged.

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

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

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

Important information about folder redirection

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

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Third-party directory, authentication, and file services

September 7, 2025

This article 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 services 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. The reason is that, like the Profile Management Service, they can interact with winlogon.exe and cause problems with the user logon process. For example, the authentication service from Novell allows users to access Novell resources, such as printers and file shares, but is not supported.

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

FAQs about profiles on multiple platforms and Profile Management migration

September 7, 2025

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.

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

Balance 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. You manage the different systems by adjusting the user profiles as follows. When profiles roam, any issues must be handled properly or, if necessary, settings must be ignored completely and not tracked at all. This is the basis of many third-party software solutions.

To minimize troubleshooting, try and roam profiles across 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 does 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 base profile for each platform. This is not necessarily the same as one profile per operating system. For more information on this recommendation, see Plan for multiple platforms. This minimizes the number of settings that might not work 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

How does Profile management enable settings across multiple versions or platforms?

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

How does Microsoft support roaming profiles across platforms and versions?

For relevant information, see Deploying Roaming User Profiles.

For Office 2007 toolbar settings, see Customize the Quick Access Toolbar.

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

There are several reasons. For example, one reason is that per-use file associations are stored in `HKEY_CURRENT_USER\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. If you want to explore how a single profile behaves across multiple platforms, the following information might be helpful.

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

Items that work across platforms:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

Items that might not work:

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

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, Citrix Virtual Apps, or Citrix Virtual Desktops™, 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 Citrix Virtual Apps™ session. This setting overrides any existing profile (except for a Citrix user profile) when the user logs on through a Remote Desktop Services session.

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

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.

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.

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Which profiles can be migrated to Citrix user profiles?

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

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

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 for the first time receives the default user profile of the Windows device they log on to. This may be acceptable, but it means any variation in different devices' default user profiles results in differences in the base profile created for the user. Therefore, you can regard the template profile feature as a global default user profile.

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

For more information, see Specify a template or mandatory profile.

Install and set up

September 7, 2025

About Profile Management installations

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

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

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

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 might result when different user store structures (from different versions) exist.

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

To install the .msi file

This procedure installs Profile Management on a single computer.

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

To install the .msi file from the command line

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

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

If you use these exclusions in Group Policy and set OVERWRITEINIFILES=yes in this procedure, ensure that 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 this option is for either deployment type in which configuration settings can be discarded and the default .ini file reinstalled.) 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 that you add the exclusions as described.

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

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

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

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

INSTALLDIR can be user specified.

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

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

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

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

To add the .adm or .admx file

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

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

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

Note: For small pilot projects and evaluations where no separate test deployment of Active Directory (AD) is available, you can also use the installed .ini file instead of the .adm or .admx file. If, after successful testing, you move from the .ini file to an AD deployment, be sure to add to the .adm or .admx

© 1997–2026 Citrix Systems, Inc. All rights reserved.

file any required inclusions and exclusions in addition to the minimum defaults that are documented in
Default inclusions and exclusions.

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

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

To remove Profile Management

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

1. To avoid data loss, ensure that all users are logged off.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. From the list of installed programs in Programs and Features, select Profile Management and click Uninstall.
3. Click Yes.
4. Restart the computer.

You can also remove Profile Management in unattended mode.

Files included in the download

September 7, 2025

The following files are included in this release.

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

In addition to DLLs and other files, be aware of the following files. The installer in the install location (by default, C:\Program Files\Citrix\User Profile Manager) creates these files.

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

Create the user store

September 7, 2025

© 1997–2026 Citrix Systems, Inc. All rights reserved.

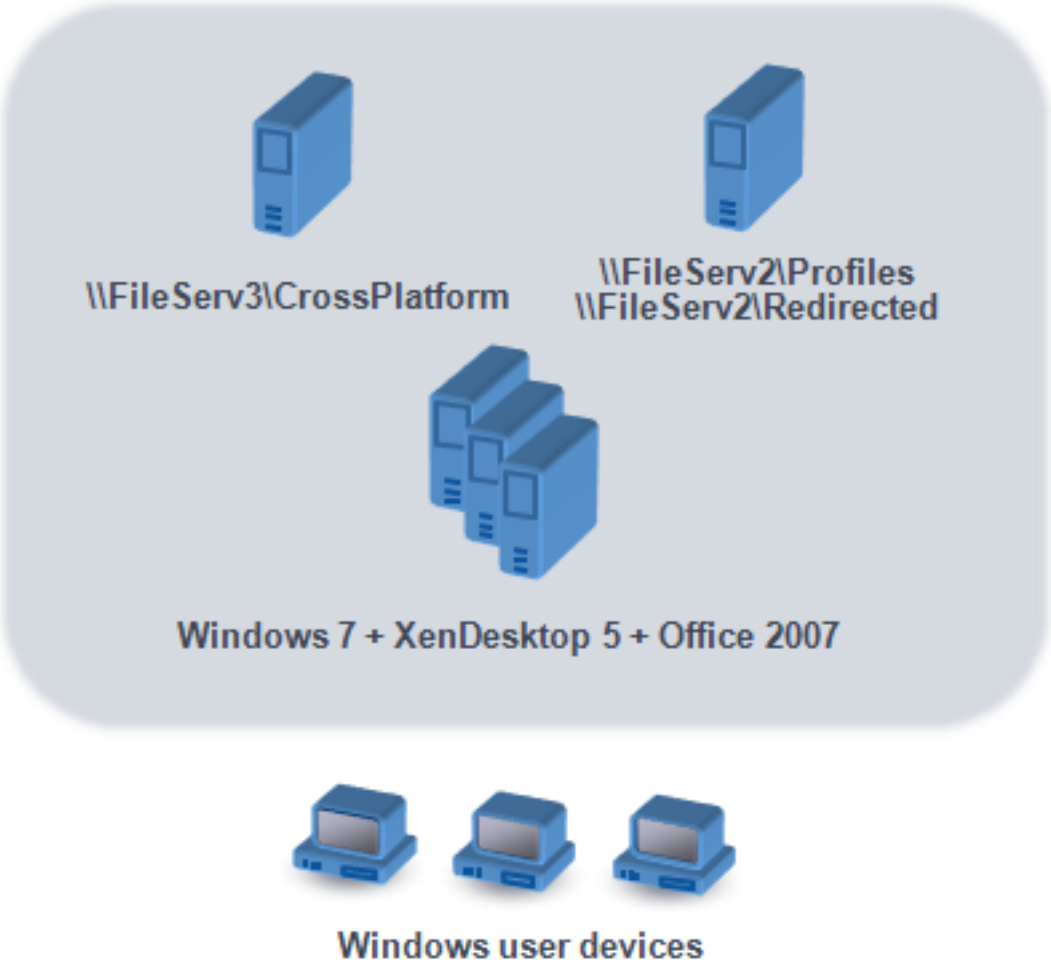
This topic helps you create the user store in a way that best suits your organization. In addition to reviewing the information here, be sure to configure the path to the user store as efficiently as possible. For example, configure the path by the sensible use of variables. For advice and examples on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

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

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

- The share is accessible to the accounts used with Citrix user profiles.
- The share is large enough to store profile data.
- The share is robust in case of disk or network failure.

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



© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

If your deployment includes multiple platforms, review the information on Version 1 and Version 2 profile types in Plan for multiple platforms. As for the structure of the user store, see Profile Management architecture.

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

Test Profile Management with a local GPO

September 7, 2025

Before deploying Profile Management in a production environment, Citrix® recommends using a test environment. You can create this setup on a local machine with the supplied .ini file. 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 adjust 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. The reason is that 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 way introduces complexities into the environment. For example, you must ensure that the Profile Management ADM file is installed and configured on each device. And there might be inability of domain users to maintain settings when accessing multiple devices.

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

If you are testing on Windows 2008 domain controllers, consider using a Windows Management Instrumentation (WMI) filter to restrict your configuration to just one machine in an OU temporarily.

Test the user experience

Minimizing differences in the end user experience when accessing resources from various devices is the goal when implementing a profile solution. Before Profile Management, the contents of users'

© 1997–2026 Citrix Systems, Inc. All rights reserved.

registry and files might vary depending on the physical device, profile configuration, and operating system. For this reason, Profile Management must be configured to address the differences between system installations on computers the users roam between.

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

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

Test operating system variations

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

Upgrade and migrate

September 7, 2025

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

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

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

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Mixed Deployments

For deployments in which different versions of Profile Management coexist, do the following:

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

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

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

Mixed Deployments Involving Profile Management 2.1.1 or Earlier

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

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

Using separate OUs and user stores can be inconvenient. To avoid these constraints, you can use one of the following two strategies. You configure each group in the appropriate version of Profile Management using the Processed groups setting. Strategy 2 is more work than Strategy 1. With the former, you keep updating the Version 5 processed user groups. And you maintain two sets of applications and desktops (but you can automate by exporting application definitions from Citrix Virtual Apps™). The advantage is that you can take your time over the migration.

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

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 5 file. The latter is compatible with the earlier version, so Version 2 computers continue to operate normally.
2. Ensure all Version 5 settings are disabled. Do not rely on the default Not enabled.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Upgrade a few computers (the first batch) to Version 5. Alternatively, install Version 5 on new computers. By default, your Version 5-processed users group contains an empty group, so no user is processed as a Version 5 user. Be aware of the exception described in Strategy 1, which might also apply when you upgrade computers in a phased migration.
4. Publish new applications (using Citrix Virtual Apps) or virtual desktops (using Citrix Virtual Apps or Citrix Virtual Desktops™) from your Version 5 computers. These applications and desktops are identical to the ones previously published from your Version 2 computers, except for their names. These names identify them as for use by Version 5 users.
5. The selected users in this batch log on to the applications or desktops (for example, using Web Interface). They choose the new applications. (Use Web Interface to enforce this step, based on user name or group membership). As a result, their sessions run on the Version 4 computers but they are processed with Version 2 settings.
6. Ensure that you have backed up all users' profiles.
7. Move the users out of the Version 2 processed users group and into the Version 4 group. Wait for the AD Group Policy changes to propagate to the Version 5 computers. Next time they log on, the users' sessions are processed with Version 5 settings.
8. Upgrade the next batch of computers and migrate the next batch of users.

Upgrade Profile Management

September 7, 2025

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

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

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

The upgrade process involves:

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

   - or -

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

To upgrade an existing .adm file

If any earlier version of the Profile Management .adm file exists in Group Policy, you can upgrade it by using the following procedure. All policy settings in the earlier version are preserved when you upgrade.

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

To upgrade the .msi file

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

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

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

To upgrade the .ini file

You edit the .ini file in an earlier version of Profile Management and upgrade to a newer version. The software can detect that the file was edited and, by default, does not overwrite it. To preserve your .ini file settings, and use the new settings in the newer version, you must do one of the following:

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

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

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

More Resources

- Profile Management policies
- Install and set up

Migrate user profiles

September 7, 2025

This article describes instructions on turning Citrix® user profiles into Windows roaming profiles. It also describes how to remove Citrix user profiles from personal vDisks so Profile Management can process them.

For more information on migration strategies, see Upgrade and migrate.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

To migrate to roaming profiles

You can migrate Citrix user profiles to Windows roaming profiles at any time. Move profile data to a network location where the roaming profiles are stored. After migration, Profile Management takes no part in processing user logons or application settings.

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

To migrate from personal vDisks

If you use the Personal vDisk feature in Citrix Virtual Desktops™, by default, user profiles are stored on the Personal vDisk's P: drive not the virtual desktop's C: drive.
If you want Citrix Profile Management to process the profiles, adjust this default when installing the Virtual Delivery Agent. To do so, modify the Registry on the master image used for a new catalog. In this scenario, because the catalog is new, no users have logged on, so no profiles are stored on the P: drive.

Important: An alternative scenario occurs if you enable Profile Management on machines in existing catalogs with Personal vDisks. Because the catalog is already in use, logons have taken place and profiles are present on the P: drive. The profiles remain there after you modify the Registry. Therefore adjust the default differently.

Issues that indicate the presence of profiles on P: drives while Profile Management is enabled include users having to reset their wallpaper, having to reconfigure their applications, or receiving temporary profiles.

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

1. Schedule a maintenance downtime for the virtual machines whose profiles you want to migrate.
2. Create a startup script (or edit your existing script). Include a command to run Delprof.exe, a profile deletion tool for Windows XP from Microsoft, or Delprof2.exe. a similar tool for later operating systems from Sepago. Follow the run command by a shutdown command:

   ```
   pre codeblock \\<share name>\delprof.exe /q /i shutdown /s /t 0
   ```

   You can download Delprof.exe from the Microsoft website. For information on this tool, see https://www.microsoft.com/en-us/download/details.aspx?id=5405.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. On the master image, change the following Registry setting from 1 to 0:

   Caution: Editing the registry incorrectly can cause serious problems that might require you to reinstall your operating system. Citrix cannot guarantee that problems resulting from the incorrect use of the Registry Editor can be solved. Use the Registry Editor at your own risk. Be sure to back up the registry before you edit it.

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\personal vDisk\Config\EnableUserProfile
   ```

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

Note: To migrate profiles in the reverse direction so the Personal vDisk manages them, follow these instructions. But change the Registry setting of EnableUserProfileRedirection from 0 to 1. This change loads the profiles on to the Personal vDisk's P: drive.

Configure

September 7, 2025

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

Manage

September 7, 2025

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Policy: Number of retries when accessing locked files

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

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

Citrix recommends that you do not enable this policy.

Resolve conflicting profiles

September 7, 2025

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

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

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

For your changes to take effect, run the `gpupdate /force` command from the command prompt as documented at https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/gpupdate.

Specify a template or mandatory profile

September 7, 2025

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 profiles. The template can be a standard roaming, local, or mandatory profile that resides on any network file share.

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

As prerequisites:

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

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

1. Under Profile Management, open the Profile handling folder.
2. Double-click the Template profile policy.
3. Select Enabled.
4. In Path to the template profile, enter the location of the profile you want to use as a template or mandatory profile. This path is the full path to the folder containing the NTUSER.DAT registry file and any other folders and files required for the template.

   Important: If the path consists only of NTUSER.DAT, ensure that you do not include the file name in the path. For example, with the file \\myservername\myprofiles\template\ntuser.dat, set the location as \\myservername\myprofiles\template.

   Use absolute paths, which can be UNC paths or paths on the local machine. You can use the latter, for example, to specify a template profile permanently on a Citrix Provisioning™ Services image. Relative paths are not supported.

   This policy does not support the expansion of Active Directory attributes, system environment variables, or the %USERNAME% and %USERDOMAIN% variables.
5. Optionally, select a check box to override any existing Windows user profiles. If a user has no Citrix user profile, but a local or roaming Windows user profile exists, by default the local profile is used. And this file is migrated to the user store, if this is not disabled. You can change the setting by enabling the check box Template profile overrides local profile or Template profile overrides roaming profile. Also, identify the template as a Citrix mandatory profile. Like Windows mandatory profiles, changes cannot be saved to Citrix mandatory profiles.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

If the **Template profile** 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 or mandatory profile is used.

For your changes to take effect, run the `gpupdate /force` command from the command prompt as documented at https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/gpupdate.

Choose a migration policy

September 7, 2025

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

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

1. Under Profile Management, open the Profile handling folder.
2. Double-click the Migration of existing profiles policy.
3. Select Enabled.
4. Select one of the following options from the drop-down list:

    - Local. Use this setting if you are migrating local profiles.
    - Local and Roaming. Use this setting if you are migrating local and roaming profiles (including Remote Desktop Services profiles, formerly known as Terminal Services profiles).
    - Roaming. Use this setting if you are migrating roaming profiles or Remote Desktop Services profiles.

If
Migration of existing profiles is not configured here, the value from the .ini file is used. If this setting is not configured here or in the .ini file, existing local and roaming profiles are migrated. If this setting is disabled, no profile is migrated. If this setting is disabled and no Citrix user profile exists in the user store, the existing Windows mechanism for creating 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 https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/gpupdate.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Enable Profile Management

April 27, 2026

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

To enable Profile Management using Group Policy, follow these steps:

1. Open the **Group Policy Management Editor**.
2. Under **Computer Configuration > Policies > Administrative Templates: Policy definitions (ADMX files) > Citrix Components > Profile Management**, double-click the **Enable Profile management** policy.
3. Select **Enabled**.

You can also enable Profile Management using the UPMPolicyDefaults_all.ini file. To do so, follow these steps:

1. On the machine where Profile Management is installed, navigate to `C:\Program Files\Citrix\User Profile Manager\UPMPolicyDefaults_all.ini`.
2. Open UPMPolicyDefaults_all.ini using Notepad.
3. Edit the configurations to reflect your specifics.

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

You can also choose to enable Profile Management using:

- Citrix Studio. For instructions on enabling Profile Management using Citrix Studio, see Knowledge Center article CTX222893.
- Workspace Environment Management (WEM). For instructions on enabling Profile Management using WEM, see Knowledge Center article CTX229258.

For your changes to take effect, run the `gpupdate /force` command from the command prompt as documented at https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/gpupdate.

Configuration precedence

September 7, 2025

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

1. Settings defined by Group Policies take precedence. The .ini file is queried only if a policy setting is set to **Not Configured**.

   Note: If you apply a Group Policy Object selectively to sites and domains within an Organizational Unit, a further precedence applies. See Group Policy: Filtering and Permission. Domain and OU Group Policies take precedence over local policies.

2. Where a setting is not defined by a policy, Profile Management tries to read the setting from the .ini file.
3. If a setting is not configured by a group policy or in the .ini file, the default setting is used.

In XenDesktop 7 deployments, be aware of the additional precedence introduced by Citrix Virtual Desktops policies. For more information, see the topic User profiles in the Citrix Virtual Desktops documentation.

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

About the Profile Management .ini file

September 7, 2025

Default configuration

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

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

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Modify the .ini file

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

Flags (on/off indicators) must be of this form:

```
<variable>=<value>
```

A value of 1 enables a setting and any other value or no value disables it. For example, the following entry enables the `ServiceActive` setting:

```
ServiceActive=1
```

Any of the following entries disable the setting:

```
ServiceActive=ON
ServiceActive=OFF
ServiceActive=TRUE
ServiceActive=FALSE
ServiceActive=
```

List entries must be of this form:

```
<value>=
```

The following entry specifies Microsoft Office files to be synchronized:

```
[SyncFileList]
AppData\Local\Microsoft\Office\*.OfficeUI
```

Changes to Group Policy settings take effect when a manual or automatic policy refresh occurs on the target computers. Changes to the .ini file take effect when you issue the command `gpupdate /force`, which is recommended. Or the changes take effect when you restart the Profile Management Service on the target computers.

Include and exclude items

September 7, 2025

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

For example, you might include Microsoft Word because it is a highly customizable and frequently used application that can present the same experience to roaming users however it is accessed. Con-

© 1997–2026 Citrix Systems, Inc. All rights reserved.

versely, you might exclude an enterprise application because it is infrequently used by some groups so its profile data does not need to be downloaded at each logon and logoff.

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

You can include and exclude:

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

Before including and excluding items

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 might 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.

Files and folders

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.

The registry

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

If you have a template profile that contains unwanted keys, use a tool such as Profile Nurse from Sepago to eliminate them from the user store.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

About exclusions

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

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

Do not add redirected folders as exclusions.

Important: Citrix recommends excluding the `AppData\LocalLow` folder from synchronization. In the default configuration, the exclusion list already contains `AppData\LocalLow`. You can also choose to exclude partial content from the `AppData\Local` folder. If you do not exclude `AppData\LocalLow` or `AppData\Local`, a large amount of data can be transferred over the network and users can experience logon delays. The folders are not synchronized by standard Windows roaming profiles.

Inclusion and exclusion rules

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

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

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

Default inclusions and exclusions

September 7, 2025

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

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

Registry inclusion list

Default Value

Registry exclusion list

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

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

Folder inclusion list

Default Value

All folders in the profile are included by default.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Folder exclusion list

Folders in this table are excluded from synchronization.

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Default Value
!ctx_roamingappdata!\Sun\Java\Deployment\tmp=
$Recycle.Bin=
AppData\LocalLow=
Tracing=

File inclusion list

Default Value

All files in the profile are included by default.

File exclusion list

Default Value

No files in the profile are excluded by default.

Include and exclude items

November 12, 2021

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

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

To exclude items

1. Under **Profile Management** > **Registry**, click the **Exclusion list** policy.
2. Select **Enabled**.
3. Click **Show** and add any registry keys in the HKCU hive that you do not want Profile Management to synchronize during logoff. Example: Software\Policies.
4. Under **Profile Management** > **File system**, double-click the **Exclusion list - directories** policy.
5. Select **Enabled**.
6. Click **Show** and add any folders that you do not want Profile Management to synchronize.

   Be aware of the following:

   - Specify the folders using paths relative to the user profile (%USERPROFILE%) and omit initial backslashes from paths.

     Examples:

     - `Desktop`. Does not synchronize the `Desktop` folder in the user profile.
     - `MyApp\tmp`. Does not synchronize the `%USERPROFILE%\MyApp\tmp` folder.

   - Use the variable %USERPROFILE% to locate the profile but do not enter the variable itself in this policy.

7. Under **Profile Management** > **File system**, double-click the **Exclusion list - files** policy.
8. Select **Enabled**.
9. Click **Show** and add any files that you do not want Profile Management to synchronize.

   Be aware of the following:

   - Specify the file names with paths relative to the user profile (%USERPROFILE%). Do not enter the variable (%USERPROFILE%) in this policy.
   - Wildcards are allowed but only for file names. Wildcards are applied recursively. As of Profile Management 7.15, you can use the vertical bar | to restrict the policy only to the current folder so that the policy does not apply to the subfolders.

     Examples:

     - `Desktop\Desktop.ini`. Ignores Desktop.ini in the Desktop folder.
     - `AppData\*.tmp`. Ignores all files with the extension .tmp in the folder `AppData` and its subfolders.
     - `AppData\*.tmp|`. Ignores all files with the extension .tmp in the folder `AppData`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

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

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

For your changes to take effect, run the `gpupdate /force` command from the command prompt as documented at https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/gpupdate.

To include items

> **Tip:**
>
> You can include specific top-level folders. In a collaborative environment, this step has the advantage of flagging critical folders to other administrators.

1. Under **Profile Management** > **Registry**, double-click the **Inclusion list** policy.
2. Select **Enabled**.
3. Click **Show** and add any profile-related registry keys in the HKEY_CURRENT_USER hive that you want Profile Management to process during logoff. Example: Software\Adobe.
4. Under **Profile Management** > **File system** > **Synchronization**, double-click the **Directories to synchronize** policy.
5. Select **Enabled**.
6. Click **Show** and add folders that are inside excluded folders but that you want Profile Management to synchronize. Example: `Desktop\exclude\include` ensures that the subfolder `include` is synchronized even if the folder `Desktop\exclude` is not.

   Be aware of the following:

   - Specify the folders using paths relative to the user profile.
   - 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.

7. Under **Profile Management** > **File system** > **Synchronization**, double-click the **Files to synchronize** policy.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

8. Select **Enabled**.
9. Click **Show** and add files that are inside excluded folders but that you want Profile Management to synchronize.

   Be aware of the following:

   - Specify the files with paths relative to the user profile.
   - Wildcards can be used but are allowed only for file names. Wildcards cannot be nested and are applied recursively. As of Profile Management 7.15, you can use the vertical bar `|` to restrict the policy only to the current folder so that the policy does not apply to the subfolders.

     Examples:

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

If **Inclusion list** is not configured here, the value from the .ini file is used. If this setting is not configured here or in the .ini file, the entire HKEY_CURRENT_USER hive is processed.

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

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

For your changes to take effect, run the `gpupdate /force` command from the command prompt as documented at https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/gpupdate.

Use wildcards

September 7, 2025

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

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

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

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

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.

Configuring policies in profile root folder:
`*.txt` specifies all files with the extension .txt in the root folder and subfolders.

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

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

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

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

Configuring policies in profile non-root folders:

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

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

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

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

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

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

Enable logon exclusion check

September 25, 2020

The **Enable Logon exclusion check** feature controls what Profile Management does if a profile in the user store contains excluded files and folders when a user logs on. By default, the feature is disabled.

To use this feature, do the following:

1. Open the Group Policy Management Editor.
2. Under **Computer Configuration > Policies > Administrative Templates: Policy definitions (ADMX files) > Citrix Components > Profile Management > File system**, double-click the **Logon Exclusion Check** policy.
3. Select **Enabled**.
4. Select an option from the drop-down menu. By default, **Delete excluded files or folders** is selected.
5. Click **OK**.

This feature provides the following three options:

- **Delete excluded files or folders**. Deletes the excluded files and folders from the user store when a user logs on.
- **Ignore excluded files or folders**. Ignores the excluded files and folders from the user store when a user logs on.
- **Synchronize excluded files or folders**. Synchronizes the excluded files and folders from the user store to a local profile when a user logs on.

> **Warning:**
>
> If you select **Delete excluded files or folders**, Profile Management deletes your excluded files and folders from the user store permanently. If you include the excluded files and folders again, Profile Management still deletes them from the cached local profile when you log on.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

For your changes to take effect, run the `gpupdate /force` command from the command prompt. Log off and log back on. For more information about the `gpupdate /force` command, see https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/gpupdate.

If the **Enable logon exclusion check** setting is not configured in Group Policy objects, the value from the .ini file is used. If this setting is not configured anywhere, it is disabled by default.

To enable logon exclusion check using the .ini file, do the following:

1. Open the Profile Management .ini file. For more information about the .ini file, see About the Profile Management .ini file.
2. Add the EnableLogonExclusionCheck item in the [General Settings] section.
3. Set a value for the EnableLogonExclusionCheck item as follows:
    - To ignore the excluded files and folders specified in the exclusion list from the user store, set the value to 1; for example, EnableLogonExclusionCheck=1.
    - To delete the excluded files and folders specified in the exclusion list from the user store, set the value to 2; for example, EnableLogonExclusionCheck=2.
    - To disable the check, set the value to 0; for example, EnableLogonExclusionCheck=0.
4. Save and close the Profile Management .ini file.
5. Run the `gpupdate /force` command to make your changes take effect.

Define which groups'profiles are processed

September 7, 2025

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

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

1. Under Profile Management, double-click the Processed groups policy.
2. Select **Enabled**.
3. Click **Show**.
4. Add the groups containing the users whose profiles you want Profile Management to process. Use Enter to separate multiple entries.

    If this setting is not configured here, the value from the .ini file is used. If this setting is not configured here or in the .ini file, members of all user groups are processed unless you exclude them using the Excluded groups policy.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. Under Profile Management, double-click the Excluded groups policy.
6. Select **Enabled**.
7. Click **Show**.
8. Add the groups containing the users you do not want Profile Management to process. Use **Enter** to separate multiple entries.

   If this setting is not configured here, the value from the .ini file is used. If this setting is not configured here or in the .ini file, no members of any groups are excluded.
9. To manage the profiles of local administrators, under Profile Management, double-click the Process logons of local administrators policy and click **Enabled**.

   Important: By default, Profile Management recognizes which operating system is in use, and processes the accounts of local administrators on desktop, not server, operating systems. The reason is that users are typically members of the Local Administrators group only on desktops, and excluding local administrators from processing in server environments assists with troubleshooting. Therefore only enable this policy if you want to modify the default behavior.

   The Excluded groups policy takes precedence over the Process logons of local administrators policy. If an account appears in both policies, it is not processed by Profile Management.

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

For your changes to take effect, run the `gpupdate /force` command from the command prompt as documented at https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/gpupdate.

Specify the path to the user store

September 7, 2025

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

- Storing multilingual profiles
- Combining inclusions and exclusions

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

The path can be:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **A relative path**. This path must be relative to the home directory, which is typically configured as the #homeDirectory# attribute for a user in Active Directory (AD).
- **A UNC path**. This path 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%). System environment variables generally require extra setup. For more information, see Administer profiles within and across OUs.
- Attributes of the AD user object enclosed in hashes (for example, #sAMAccountName#).
- Profile Management variables. For more information, see Profile Management policies.

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

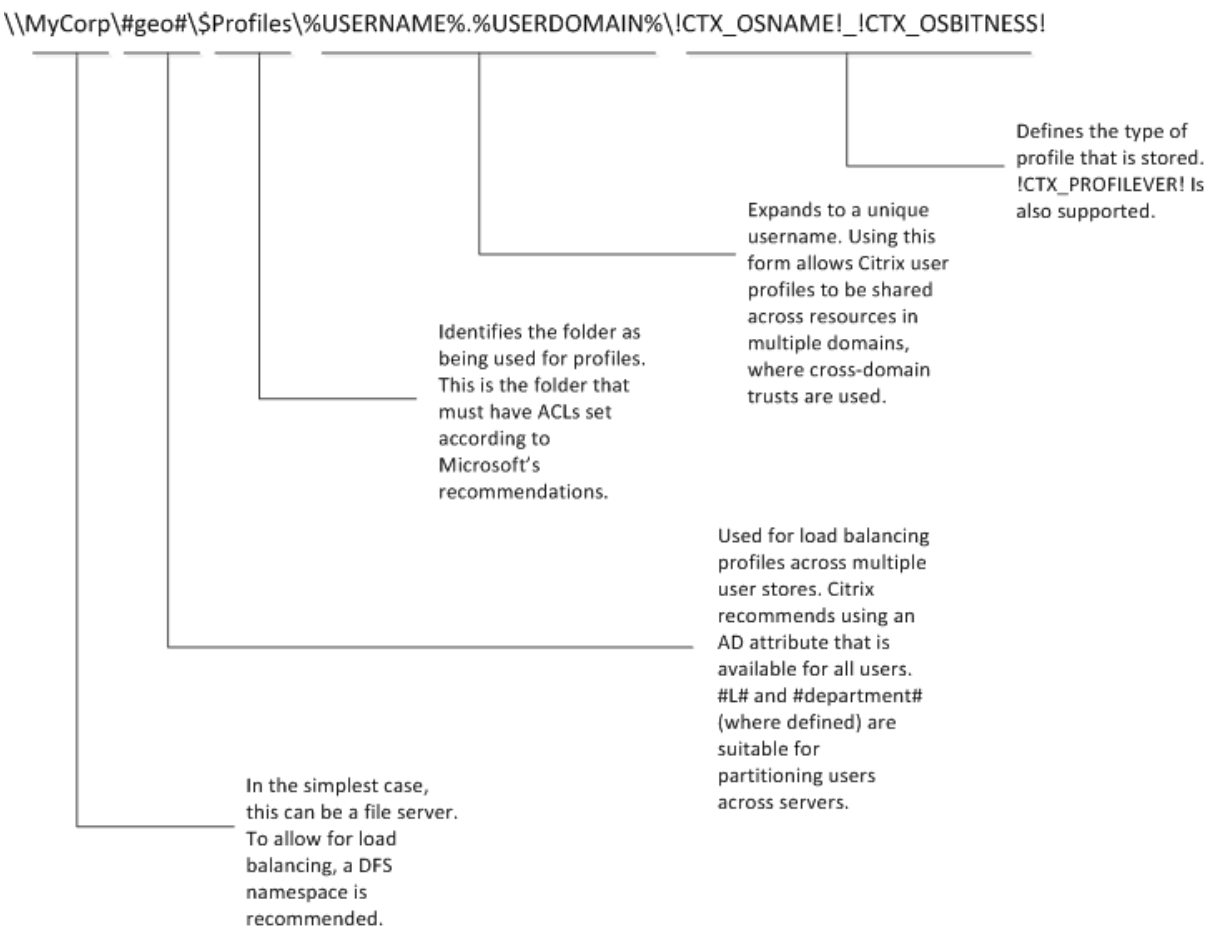
Examples:

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

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

This diagram illustrates the components of a typical path to the user store that incorporates AD attributes, environment variables, and Profile Management variables.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



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

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

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

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

For your changes to take effect, run the `gpupdate /force` command from the command prompt as documented at https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/gpupdate.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Migrate user store

November 15, 2022

Profile Management provides a solution to migrate your user store without losing any data. This feature can be useful in cases where you want to migrate your user store to a more scalable file server.

To migrate your user store, use the Migrate user store policy along with the Path to user store policy. The Migrate user store policy lets you specify the path to the folder where the user settings (registry changes and synchronized files) were previously saved (the user store path that you previously used).

The path can be an absolute UNC path or a path relative to the home directory. In both cases, you can use the following types of variables:

- System environment variables (enclosed in percent signs)
- Attributes of the Active Directory user object (enclosed in hash signs)

Examples:

- The folder `Windows\\%ProfileVer%` stores the user settings in a subfolder called `Windows\W2K3` of the user store (if %ProfileVer% is a system environment variable that resolves to W2K3).
- `\\server\share\\#SAMAccountName#` stores the user settings to the UNC path `\\server\share\<JohnSmith>` (if `#SAMAccountName#` resolves to JohnSmith for the current user).

In the path, you can't use user environment variables except `%username%` and `%userdomain%`.

If this setting is disabled, the user settings are saved in the current user store.

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

If this setting is not configured here or in the .ini file, the user settings are saved in the current user store.

After the changes to the policy settings take effect, the user settings stored in the previous user store are migrated to the current user store specified in the **Path to user store** policy.

To configure the migration of the user store in Group Policy, complete the following steps:

1. Open the Group Policy Management Editor.
2. Under **Policies > Administrative Templates: Policy definitions (ADMX files) > Citrix Components > Profile Management**, double-click the **Migrate user store** policy.
3. Select **Enabled**.
4. In the **Options** pane, type the user store path that you previously used.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. Click **OK**.

For your changes to take effect, run the `gpupdate /force` command from the command prompt. Log off from all sessions and then log on again. For details, see https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/gpupdate.

You can also choose to configure the Profile Management policies in Citrix Studio. To do so, complete the following steps:

1. In the left pane of Citrix Studio, click **Policies**.
2. In the **Create Policy** window, type the policy in the search box. For example, type "Migrate user store."
3. Click **Select** to open the **Migrate user store** policy.
4. Select **Enabled** and then type the user store path that you previously used.
5. Click **OK**.

Automatic migration of existing application profiles

September 7, 2025

Profile Management provides a solution that can automatically migrate existing application profiles. The application profiles include both the application data in the **AppData** folder and the registry entries under `HKEY_CURRENT_USER\SOFTWARE`.

This feature can be useful in cases where you want to migrate your application profiles across different operating systems (OSs). For example, suppose you upgrade your OS from Windows 10 version 1803 to Windows 10 version 1809. If this feature is enabled, Profile Management automatically migrates the existing application settings to Windows 10 version 1809 the first time each user logs on. As a result, the application data in the **AppData** folder and the registry entries under `HKEY_CURRENT_USER\SOFTWARE` are migrated. Users no longer need to configure the applications again.

This feature is disabled by default. To enable it in Group Policy, complete the following steps:

1. Open the Group Policy Management Editor.
2. Under **Policies > Administrative Templates: Policy definitions (ADMX files) > Citrix Components > Profile Management > Profile handling**, double-click the **Automatic migration of existing application profiles** policy.
3. Select **Enabled** and then click **OK**.

For your changes to take effect, run the `gpupdate /force` command from the command prompt. Log off from all sessions and then log on again. For more information, see https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/gpupdate.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

You can also choose to configure the Profile Management policies in Citrix Studio. To do so, complete the following steps:

1. In the left pane of Citrix Studio, click **Policies**.
2. In the **Create Policy** window, type the policy in the search box. For example, type "Automatic migration of existing application profiles."
3. Click **Select** to open the **Automatic migration of existing application profiles** policy.
4. Select **Enabled** and then click **OK**.

How it works

Profile Management performs the migration when a user logs on and there are no user profiles in the user store. Before the migration starts, Profile Management locates the application profiles to be migrated. It does so through automatic discovery. It automatically locates and migrates the following:

- Application settings under %userprofile%\Appdata\Local\ and %userprofile%\Appdata\Roaming. The following Microsoft folders that contain the current OS platform information are ignored:

```
- %userprofile%\AppData\Local\Temp
- %userprofile%\AppData\Local\Packages
- %userprofile%\AppData\Local\TileDataLayer
- %userprofile%\AppData\Local\Microsoft\Temp
- %userprofile%\AppData\Local\Microsoft\Credentials
- %userprofile%\AppData\Local\Microsoft\Windows
- %userprofile%\AppData\Local\Microsoft\Windows\
   InputPersonalization
- %userprofile%\AppData\Local\Microsoft\Windows\Side bars
- %userprofile%\AppData\Local\Microsoft\WindowsApps
- %userprofile%\Appdata\Roaming\Microsoft\Credentials
- %userprofile%\Appdata\Roaming\Microsoft\SystemCertificates
- %userprofile%\Appdata\Roaming\Microsoft\Crypto
- %userprofile%\Appdata\Roaming\Microsoft\Vault
- %userprofile%\Appdata\Roaming\Microsoft\Windows
```

- Registry keys under `HKEY_CURRENT_USER\SOFTWARE` and `HKEY_CURRENT_USER\SOFTWARE\Wow6432Node` (except for `HKEY_CURRENT_USER\SOFTWARE\Microsoft` and `HKEY_CURRENT_USER\SOFTWARE\Classes`)

If there are multiple existing application profiles, Profile Management performs the migration in the following order of priority:

1. Profiles of the same OS type (single-session OS to single-session OS and multi-session OS to multi-session OS).
2. Profiles of the same Windows OS family; for example, Windows 10 to Windows 10, or Windows Server 2016 to Windows Server 2016).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Profiles of an earlier version of the OS; for example, Windows 7 to Windows 10, or Windows Server 2012 to Windows 2016.
4. Profiles of the closest OS.

> **Note:**
>
> You must specify the short name of the OS by including the variable "!CTX_OSNAME!"in the user store path. Doing so lets Profile Management locate the existing application profiles.

Suppose you configure the user store path as `\\fileserver\userstore\\%username%\!CTX_OSNAME!!CTX_OSBITNESS!` and your OS is Windows 10 version 1803 64-bit (Win10RS4x64). Profile Management first locates the previous profile folder and then migrates it to the application profile folder in the user store in the following order:

1. \fileserver\userstore\user1\Win10RS3x64
2. \fileserver\userstore\user1\Win10RS2x64
3. \fileserver\userstore\user1\Win10RS1x64
4. \fileserver\userstore\user1\Win10x64
5. \fileserver\userstore\user1\Win10RS5x64
6. \fileserver\userstore\user1\Win10RS6x64
7. \fileserver\userstore\user1\Win8x64
8. \fileserver\userstore\user1\Win7x64
9. \fileserver\userstore\user1\Win2016
10. \fileserver\userstore\user1\Win2012R2
11. \fileserver\userstore\user1\Win2012
12. \fileserver\userstore\user1\Win2008
13. \fileserver\userstore\user1\Win2019

If none of them is available, Profile Management ends the migration process and returns an error.

Store certificates

September 7, 2025

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 setting **Directories to synchronize**. 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/gpupdate.

Stream user profiles

September 7, 2025

With the Citrix® streamed user profiles feature, files and folders contained in a profile are fetched from the user store to the local computer only when they are accessed by users after they have logged on. Registry entries and any files in the pending area are exceptions. They are fetched immediately. For more information on the pending area, see Pending area in Profile Management architecture.

Streaming is not required and does not support the Personal vDisk feature of Citrix Virtual Desktops.

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 MB. Any files and folders that exceed the limit are fetched as soon as possible after logon.
   - To turn on the cache entire profile feature, set the limit to zero. After logon, this fetches all files in the user store as a background system task, without any feedback to users.
     If large files are present, the Always cache policy can improve performance by reducing logon times.
5. Click **OK**.
6. Optionally, double-click Timeout for pending area lock files, select **Enabled**, and enter a time-out period (days) that frees up files so they are written back to the user store from the pending area if the user store remains locked when a server becomes unresponsive. Use this setting to prevent bloat in the pending area and to ensure that the user store always contains the most up-to-date files.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

7. Click **OK**.
8. Optionally, if you want only a subset of user profiles in the OU to be streamed, double-click **Streamed user profile groups**, select **Enabled**, and enter a list of groups. Use Enter to separate multiple entries. The profiles of users in all other groups are not streamed.
9. Click **OK**.

If the **Profile streaming** setting is not configured in the policy or in the .ini file, Profile Streaming is disabled.

If the **Always cache** 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.

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

If the **Streamed user profile groups** 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.

For your changes to take effect, run the `gpupdate /force` command from the command prompt as documented at https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/gpupdate.

To enable profile streaming exclusion

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

To enable profile streaming exclusion, do the following:

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

For example:

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

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

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

For your changes to take effect, run the `gpupdate /force` command. For more information, see https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/gpupdate.

Note:

- This policy only takes effect when Profile Streaming is enabled.
- The policy does not support wildcards * and ?.
- Use Enter to separate multiple entries.
- When manually editing the profile streaming exclusion list, you must add the preceding default excluded folders to avoid logons hanging.

Configure folder redirection

September 7, 2025

Folder redirection is a feature of Microsoft Windows and can be used with Profile Management.

> **Important:**
>
> Configure folder redirection using only one of these methods: Microsoft Active Directory (AD) GPOs or Citrix® policies. Using multiple methods to configure folder redirection might cause unpredictable results.

To configure folder redirection, complete the following steps:

1. Move applicable users to an OU that Profile Management manages.
2. Create a GPO and then open it for editing.
3. Navigate to **User Configuration > Administrative Templates > Citrix Components > Profile Management > Folder Redirection** and then select the folder you want to redirect.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. Enable the Redirect the <folder name> folder policy and then type the redirected path. Do not add redirected folders as exclusions. Do not add user names or folder names to the path. For example, if you set the path to the **Desktop** folder as \\server\share\, the folder in the user environment is redirected as \\server\share\<user name>\Desktop.
5. For your changes to take effect, run the gpupdate /force command from the command prompt. For details, see https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/gpupdate.

The following folders can be redirected:

- AppData(Roaming)
- Desktop
- Start Menu
- Documents
- Pictures
- Music
- Videos
- Favorites
- Contacts
- Downloads
- Links
- Searches
- Saved Games

When redirecting folders, keep the following in mind:

- The **Documents** folder. You can redirect it to the user's home directory.
- The **Music**, **Pictures**, and **Videos** folders. You can redirect them to folders relative to the **Documents** folder.

How to verify that folder redirection works

To verify that folder redirection works, complete the following steps:

1. In a session, navigate to a folder you directed, right-click the folder, and then select **Properties**.
2. In the properties window, navigate to the **Shortcut** tab and then check the **Target** field. If the field displays a redirected path, folder redirection works. Otherwise, folder redirection does not work.

Folder redirection logs

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> Profile Management writes information to the Windows Event Log only when folder redirection fails.

Profile Management writes information to the Windows event logs. You can view the events in the **Application** pane of the Windows Event Viewer. The information helps you troubleshoot issues you experience when using the folder redirection feature.

Manage cookie folders and other transactional folders

September 7, 2025

This article 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 step 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). These folders contain interdependent files, where one file references others. Mirroring folders allows Profile Management to process a transactional folder and its contents as a single entity, therefore avoiding profile bloat.

For example, consider how Index.dat references cookies while a user browses the Internet. 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. The user logs off from the first session (or in the middle of a session, if the active write-back feature is configured). Then the cookies from the second session replace the cookies 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. With this feature, Profile Management overwrites the cookies with those cookies from the last session each time the user logs off. Therefore, Index.dat stays up-to-date.

The cookie folder can become bloated in the following situations:

- Multiple sessions are involved
- Websites 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

CONFIGURE: Add the following folders under Mirroring:

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

Note:

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

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

To mirror folders

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

The **Folders to mirror** policy does not support scenarios where certain files in a folder or certain subfolders are mirrored. As a workaround, use the **Folders to mirror** policy with the **Exclusion list** – **directories** policy or the **Exclusion list** –**files** policy.

For example, in the case of Google Chrome, the bookmark-related files or subfolders in `AppData\Local\Google\Chrome\User Data\Default` are interdependent. As a result, they must be synchronized as a single entity. To avoid profile bloat, follow these steps:

1. Add `AppData\Local\Google\Chrome\User Data\Default` to the list of folders to mirror.
2. Add the files or subfolders unrelated to bookmarks in that folder to the exclusion list.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Caution:**
>
> Mirroring transactional folders can mean that the "last write wins."Files that are modified in more than one session are overwritten by the last update. Changes to the user profile might be lost.

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

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

For your changes to take effect, run the `gpupdate /force` command from the command prompt as documented at https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/gpupdate.

To delete stale cookies

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

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

If **Process Internet cookie files on logoff** is not configured here, the value from the .ini file is used. If this setting is not configured here or in the .ini file, no processing of Index.dat takes place.

For your changes to take effect, run the `gpupdate /force` command from the command prompt as documented at https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/gpupdate.

Enabling Process Internet cookie files on logoff increases logoff times. Nevertheless, 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/gpupdate.

Configure offline profiles

April 24, 2026

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

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

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

You can configure offline profiles in these ways:

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

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Using Group Policy

1. Create an OU containing all computers managed by Profile Management. Include the laptops and mobile devices that use offline profiles, your Citrix Virtual Apps™ servers, and your virtual desktops.
2. Create a child OU containing only the laptops and mobile devices.
3. In Group Policy Management, create a baseline Group Policy Object (GPO) that enforces your site-wide policies, and link it to both OUs.
4. Configure the baseline GPO with the Profile Management settings common to all computers.
5. Create a second, offline GPO and link it to the child OU.
6. Configure the offline GPO as follows:

    a) Under Profile Management, double-click Offline profile support.
    b) Select Enabled and click OK.
    c) Configure any other settings that you want to apply only to laptops and mobile devices.

For your changes to take effect, run the `gpupdate /force` command from the command prompt as documented at https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/gpupdate.

Using the .ini file

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

1. On each laptop or mobile device, locate the .ini file created by the Profile Management installer. To locate the .ini file, see Files included in the download.
2. Uncomment this line (by removing the semi-colon from it):

    ```
    pre codeblock ;OfflineSupport=
    ```

3. Save the .ini file.

    For your changes to take effect, run the `gpupdate /force` command from the command prompt as documented at https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/gpupdate.

Configure the Customer Experience Improvement Program (CEIP)

September 7, 2025

To configure the CEIP, follow these steps:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Open the Group Policy Management Editor.
2. Under **Computer Configuration > Policies > Administrative Templates: Policy definitions (ADMX files) > Citrix Components > Profile Management > Advanced settings**, double-click **Customer Experience Improvement Program**.
3. Select **Enabled** or **Disabled**, then click **OK**.
4. For your changes to take effect, run the `gpupdate /force` command from the command prompt as documented at https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/gpupdate.

Note: If the CEIP is not configured in Group Policy objects and HDX™, the value from the .ini file is used. If this setting is not configured anywhere, it is enabled by default.

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

Configure active write back

September 7, 2025

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

If you start a second session (at a second computer, for example), modifications made to a file in the first session are available in the second if it was started before you log off from the first.

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

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

For your changes to take effect, run the `gpupdate /force` command from the command prompt as documented at https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/gpupdate.

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configure cross-platform settings

September 7, 2025

Important: Note the following important information for this feature:

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

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

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

1. For the settings that are common to all platforms, create a common Group Policy Object (common GPO), link it to the Profile Management .adm or .admx file, and configure the settings as required. This setup is best practice because it minimizes duplicate settings that can make any later troubleshooting awkward. Depending on your requirements, all Profile Management settings work on multiple platforms except Path to user store. Configure Path to user store separately for each platform due to the different user store structures of Version 1 and Version 2 profiles. In the common GPO, leave this setting unconfigured.
2. Create separate OUs for your different platforms. For example, if you are migrating from Windows 7 to Windows 8, create separate OUs for these operating systems), and set Path to user store appropriately in each OU.
3. Locate the definition (.xml) files for the supported applications whose personalizations you

© 1997–2026 Citrix Systems, Inc. All rights reserved.

want to work across the platforms. These files are located in the CrossPlatform folder in the download package. You can create your own application definition files. For details, see Create a definition file.

4. Copy the .xml files to a suitable location on your network.
5. Edit the common GPO in Group Policy Management Editor. Under Profile Management open the Cross-platform settings folder and configure these settings:

    - Cross-platform settings user groups. Restricts the users who experience cross-platform settings. This setting is optional. It is useful when testing this feature or rolling it out in stages.
    - Path to cross-platform definitions. Identifies the network location of the definition files that you copied from the download package. This path must be a UNC path. Users must have read access to this location, and administrators must have write access to it. The location must be a Server Message Block (SMB) or Common Internet File System (CIFS) file share.
    - Path to cross-platform settings store. It is the common area of the user store where profile data shared by multiple platforms is located. Users must have write access to this area. The path can be an absolute UNC path or a path relative to the home directory. You can use the same variables as for Path to user store.

6. Specify a base platform by ensuring Source for creating cross-platform settings is set to Enabled in that platform's OU. This setting migrates data from the base platform's profiles to the cross-platform settings store. In the other platforms'OUs, set this policy to Disabled or Unconfigured. Each platform's own set of profiles are stored in a separate OU. You must decide which platform's profile data to use to seed the cross-platform settings store. This is referred to as the base platform. If the cross-platform settings store contains a definition file with no data, or the cached data in a single-platform profile is newer than the definition's data in the store, Profile Management migrates the data from the single-platform profile to the store unless you disable this setting.
   Important: If
   Source for creating cross-platform settings is enabled in multiple OUs, the platform that the first user logs on to becomes the base profile.
7. Set Enable cross-platform settings to Enabled. By default, to facilitate deployment, cross-platform settings is disabled until you turn on this setting.
8. Run a Group Policy update.
9. If you are migrating profiles across platforms but not supporting roaming of them, when the migration is complete, set Enable cross-platform settings to **Disabled**.

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

If Path to cross-platform settings store is disabled, the default path Windows\PM_CP is used. If this

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

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

Example: Roaming Microsoft Office settings between Windows Server 2008 and Windows 7

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

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

Operating systems and applications supported by cross-platform settings

September 7, 2025

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

About definition files

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

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

Important: Without a thorough analysis of an application's behavior across all OSs and a full understanding of this feature's operation, editing of definition files can result in unexpected changes to users' profiles that can be difficult to troubleshoot. For this reason, Citrix® does not support the editing of the supplied definition files or the creation of new ones. In addition, some application settings cannot be duplicated across OSs due to the nature of Windows user profiles.

In addition note that, although this feature is suitable for registry and application settings, it is not suitable for files or folders, or objects typically used with folder redirection (for example, browser favorites, and desktop and Start menu settings).

Supported operating systems

You can roam profiles between any of the supported single-session OSs, and between any of the supported multi-session OSs.

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

- **Single-session OSs**. Windows XP, Windows 7, and Windows Vista.
- **Multi-session OSs**. Windows Server 2003, Windows Server 2008, and Windows Server 2008 R2.

Supported Citrix products

The cross-platform settings feature supports the following Citrix products:

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Supported applications

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

- **Internet Explorer 7 Plus.xml**. This file supports the roaming of Versions 7, 8, and 9 of Internet Explorer (except favorites) across platforms. The roaming of favorites and feeds is not supported.
- **Office 2007.xml**.
- **Office 2010.xml**.
- **Wallpaper.xml**. This file supports the roaming of desktop wallpaper across platforms. The roaming of themes across platforms is not supported.

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

Create a definition file

September 7, 2025

Definition files define the folders, files, or registries to be synchronized. You can create your own application definition files.

Use the Microsoft UE-V template generator to create a UE-V template file.

1. Download the **Windows Assessment and Deployment Kit** (Windows ADK) for Windows 10 from Microsoft website.
2. Install Windows ADK. Select **Microsoft User Experience Virtualization (UE-V) Template Generator**. Click **Install**. Click **Finish** to close the wizard after the installation completes.
3. Click **Start**, click **Microsoft User Experience Virtualization**, and then click **Microsoft User Experience Virtualization Generator**.
4. Click **Create a settings location template**.
5. Follow the wizard to specify application related parameters. Click **Next** to continue.
   Take Notepad as an example. Specify the file path as **C:\Windows\System32\notepad.exe**.
6. After the specified application starts, close it.
7. After the process completes, click **Next** to continue.
8. Choose **Review Locations** in the left pane. Select all the check boxes in the lists for standard and nonstandard registry/files.
9. Click **Create** to save the template XML file.
   Take Notepad as the example. Save the template XML file as **Notepad.xml**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Note**
>
> You might have multiple applications defined in a single UE-V template file.

To convert the UE-V template file to a cross-platform definition file, do the following:

1. Download the conversion tool here.
2. From a command prompt, run the command **convert show filename** to display all application names in the definition file.
3. Run the following command to convert the UE-V template file to a definition file.
   convert source destination [/Index] [/V]

   [/Index]: Convert only the application specified by index number.

   By default, this tool converts all applications in the UE-V template.

   [/V]: Display verbose information for the conversion.

For cross-platform settings, you must repeat the preceding steps for other operating systems and merge the definition files into one. You can use the **Platform** element with the **OSVersionNumber** attribute to merge the files. On Windows 7, a setting folder is at **AppData\Application\Win7\folder**. On Windows 10, at **AppData\Application\Win10\folder**.

On Windows 7, the definition file you created looks as follows:

```
<?xml version="1.0" encoding="utf-8"?>

<GroupDefinitions Version="4.0.0.0" GUID="93E41C6E-2091-1B9B-36BC-7CE94EDC677E">

    <Group Name="Common Settings" GUID="32D83BB6-F3AD-985F-D4BC-655B3D9ACBE2">

        <Object Name="!CTX_ROAMINGAPPDATA!\Application\Win7\folder" GUID="1B43DE3F-EC9C-463c-AC19-CD01D00219B6">

            <Platform>

                <Folder>

                    <Path>!CTX_ROAMINGAPPDATA!\Application\Win7\folder</Path>

                    <Recurse/>

                </Folder>

            </Platform>

        </Object>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
22
23      </Group>
24
25  </GroupDefinitions>
```

On Windows 10, the definition file you created looks as follows:

```
1  <?xml version="1.0" encoding="utf-8"?>
2
3  <GroupDefinitions Version="4.0.0.0" GUID="93E41C6E-2091-1B9B-36BC-7
       CE94EDC677E">
4
5      <Group Name="Common Settings" GUID="32D83BB6-F3AD-985F-D4BC-655
           B3D9ACBE2">
6
7          <Object Name="!CTX_ROAMINGAPPDATA!\Application\Win10\folder"
               GUID="1B43DE3F-EC9C-463c-AC19-CD01D00219B6">
8
9              <Platform>
10
11                 <Folder>
12
13                     <Path>!CTX_ROAMINGAPPDATA!\Application\Win10\folder
                           </Path>
14
15                     <Recurse/>
16
17                 </Folder>
18
19             </Platform>
20
21         </Object>
22
23     </Group>
24
25 </GroupDefinitions>
```

After merging, the contents of the definition file look as follows:

```
1  <?xml version="1.0" encoding="utf-8"?>
2
3  <GroupDefinitions Version="4.0.0.0" GUID="93E41C6E-2091-1B9B-36BC-7
       CE94EDC677E">
4
5      <Group Name="Common Settings" GUID="32D83BB6-F3AD-985F-D4BC-655
           B3D9ACBE2">
6
7          <Object Name="!CTX_ROAMINGAPPDATA!\Application\%osname%\folder"
               GUID="1B43DE3F-EC9C-463c-AC19-CD01D00219B6">
8
9              <!-- Assuming that the folder locates differently when in
                   different platforms -->
10
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
11              <Platform OSVersionNumber="6.1"> <!-- Win7 -->
12
13                  <Folder>
14
15                      <Path>!CTX_ROAMINGAPPDATA!\Application\Win7\folder
                            </Path>
16
17                      <Recurse/>
18
19                  </Folder>
20
21              </Platform>
22
23              <Platform OSVersionNumber="10.0"> <!-- Win10 -->
24
25                  <Folder>
26
27                      <Path>!CTX_ROAMINGAPPDATA!\Application\Win10\folder
                            </Path>
28
29                      <Recurse/>
30
31                  </Folder>
32
33              </Platform>
34
35          </Object>
36
37      </Group>
38
39  </GroupDefinitions>
```

For information about configuring cross-platform settings, see Configure cross-platform settings.

For information about the architecture of definition files, see Application definition file structure.

For information about enabling application profiler, see Enable application profiler.

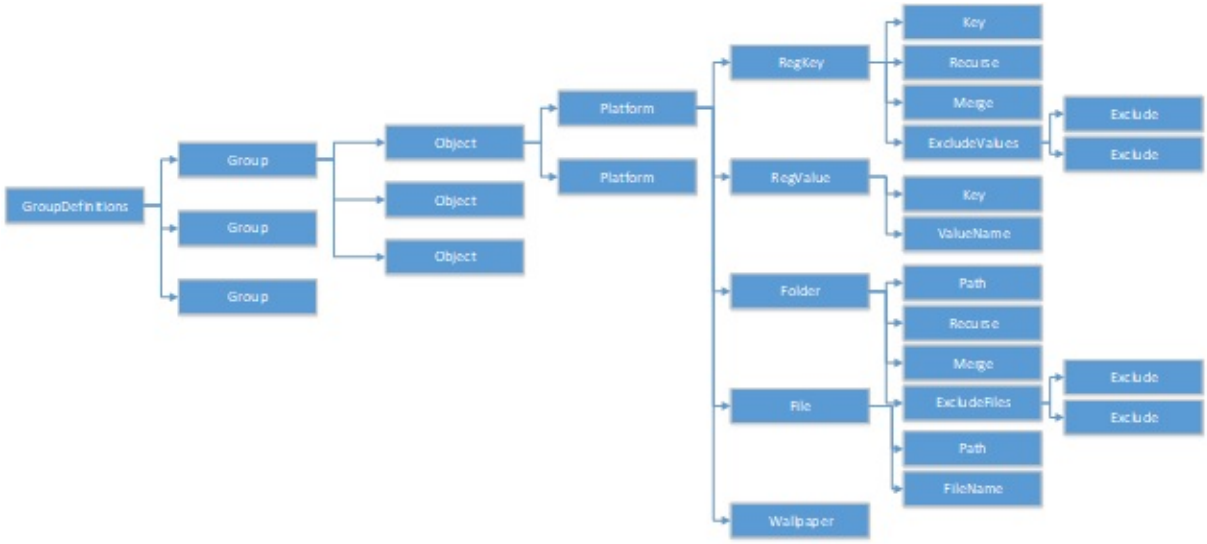
Application definition file structure

September 7, 2025

This article describes the XML structure of Profile Management application definition files. The structure applies to both application profiler and cross-platform settings.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Architecture Chart



- XML Declaration and Encoding Attribute

  The XML declaration must specify the attribute, <?xml version=”1.0”>.

  Encoding=”UTF-8”is a recommended attribute.

- GroupDefinitions

  A container of collections of groups. It acts as the root element of the XML document. Its attributes include version and GUID. They are mandatory attributes.

- Group

  Defines settings of a subapplication. Its attributes are name and GUID. They are mandatory attributes.

- Object

  Defines one setting of a subapplication. Its attributes are name and GUID. They are mandatory attributes.

- Platform

  Platform provides different definitions in different operating systems. It can use an optional attribute OSVersionNumber to specify the operating system. When there is no attribute, all platforms accept the inner definition of the setting. Platform must contain one of the following elements: RegKey, RegValue, File, Folder, and Wallpaper.

- RegKey

  Defines a setting as a key in the registry. It must contain the Key element. It includes two optional subelements, Recurse and Merge. Recurse and Merge define the performance when Pro-

© 1997–2026 Citrix Systems, Inc. All rights reserved.

file Management roams the key. Another optional subelement is ExcludeValues. ExcludeValues defines the registry values that can be excluded.

- RegValue

  Defines a setting as a value in the registry. It must contain Key to specify the path of its parent key.

- Folder

  Defines a setting as a folder. It must contain `Path` to specify the path of the folder. It has optional subelements, `Recurse` and `Merge`. `Recurse` and `Merge` define the performance when Profile Management roams the folder. Another optional subelement is `ExcludeFiles`, which defines the files that can be excluded.

- File

  Defines a setting as a file. It must contain `Path` to specify the path of its parent folder, and `FileName` to specify the name of a file.

- Wallpaper

  Defines all wallpaper settings. No attributes or subelements are required. Profile Management roams these settings automatically.

- Key

  Specifies the path of the registry key or the path of the parent registry key. Key is the subelement of RegKey and RegValue.

- ValueName

  Specifies the name of the registry value. It is a subelement of RegValue.

- Path

  Specifies the path of the folder or the path of the parent folder. It is a subelement of Folder and File. Profile Management variables can be adopted.

- FileName

  Specifies the name of a file. It is s subelement of File.

- Recurse

  Optional subelement of RegKey and Folder. If this element exists, Profile Management roams the key and the folder recursively.

- Merge

  Optional subelement of RegKey and Folder. If this element exists, Profile Management merges (but does not substitute) the key and the folder.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- ExcludeValues

  Optional subelement of RegKey. Specifies the values that can be excluded when roaming the key.

- ExcludeFiles

  Optional subelement of Folder. Specifies the files that can be excluded when roaming the folder.

- Exclude

  Subelement of ExcludeValues and ExcludeFiles. Specifies the excluded items of files or registry values.

> **Note**
>
> Make sure that your document contains a correct syntax format. Profile Management checks these files by using the CPSValidationSchema.xsd validation file when these files load. You can find the validation file under the installation path of Profile Management. Profile Management ignores incorrect files and record error messages in the log.

Sample

```
<?xml version="1.0" encoding="UTF-8"?>

<!-- Copyright 2011 Citrix Systems, Inc. All Rights Reserved. -->

<GroupDefinitions GUID="748E63D3-426E-4796-9C32-420B25DB2D9F" Version="
   4.0.0.0">

<!-- Application Settings -->

<Group GUID="0FCCCF29-0A0E-482d-A77E-3F39A8A854A6" Name="Application
   Settings">

<!-- Registry Key Setting Example -->

<Object GUID="637EC13C-2D47-4142-A8EB-3CEA6D53522A" Name="Software\
   Application\certain key">

<Platform>

<RegKey>

<Key>Software\Microsoft\Office\certain key</Key>

<Merge/>

<Recurse/>

<ExcludeValues>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
26
27 <Exclude>excluded value 1</Exclude>
28
29 <Exclude>excluded value 2</Exclude>
30
31 <Exclude>excluded value 3</Exclude>
32
33 </ExcludeValues>
34
35 </RegKey>
36
37 </Platform>
38
39 </Object>
40
41 <!-- Registry Value Setting Example -->
42
43 <Object GUID="3C896310-10C4-4e5f-90C7-A79F4E653F81" Name="Software\
      Application\certain value">
44
45 <!-- Folder Setting Example -->
46
47 <Object GUID="7F8615D0-5E63-4bd0-982D-B7740559C6F9" Name="!
      CTX_ROAMINGAPPDATA!\Application\setting folder">
48
49 <Platform>
50
51 <Folder>
52
53 <!-- We can use Citrix variable if necessary -->
54
55 <Path>!CTX_ROAMINGAPPDATA!\Application\setting folder</Path>
56
57 <Merge/>
58
59 <Recurse/>
60
61 <ExcludeFiles>
62
63 <Exclude>excluded file 1</Exclude>
64
65 <Exclude>excluded file 2</Exclude>
66
67 <Exclude>excluded file 3</Exclude>
68
69 </ExcludeFiles>
70
71 </Folder>
72
73 </Platform>
74
75 </Object>
76
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
<!-- File Setting Example -->

<Object GUID="7F8615D0-5E63-4bd0-982D-B7740559C6F9" Name="!
   CTX_ROAMINGAPPDATA!\Application\file.txt">

<Platform>

<File>

<!-- We can use Citrix variable if necessary -->

<Path>!CTX_ROAMINGAPPDATA!\Application</Path>

<FileName>file.txt</FileName>

</File>

</Platform>

</Object>

<!-- Setting based on different OS -->

<Object GUID="1B43DE3F-EC9C-463c-AC19-CD01D00219B6" Name="!
   CTX_ROAMINGAPPDATA!\Application\%osname%\folder">

<!-- Assuming that the folder locates differently when in different
   platforms -->

<Platform OSVersionNumber="6.1">

<!-- Win7 -->

<Folder>

<Path>!CTX_ROAMINGAPPDATA!\Application\Win7\folder</Path>

<Recurse/>

</Folder>

</Platform>

<Platform OSVersionNumber="10.0">

<!-- Win10 -->

<Folder>

<Path>!CTX_ROAMINGAPPDATA!\Application\Win10\folder</Path>

<Recurse/>

```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
</Folder>

</Platform>

</Object>

</Group>

</GroupDefinitions>
```

Cross-platform settings - Case study

September 7, 2025

The cross-platform settings feature is primarily used for migrating from Windows 7 and Windows Server 2008 to Windows 8 and Windows Server 2012. This migration might also move from Microsoft Office 2003 or Office 2007 to Office 2010. Given the typical investment in Windows 2003 systems, a significant coexistence phase is expected. The feature is expected to support both migration and sustained coexistence.

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

The case study consists of:

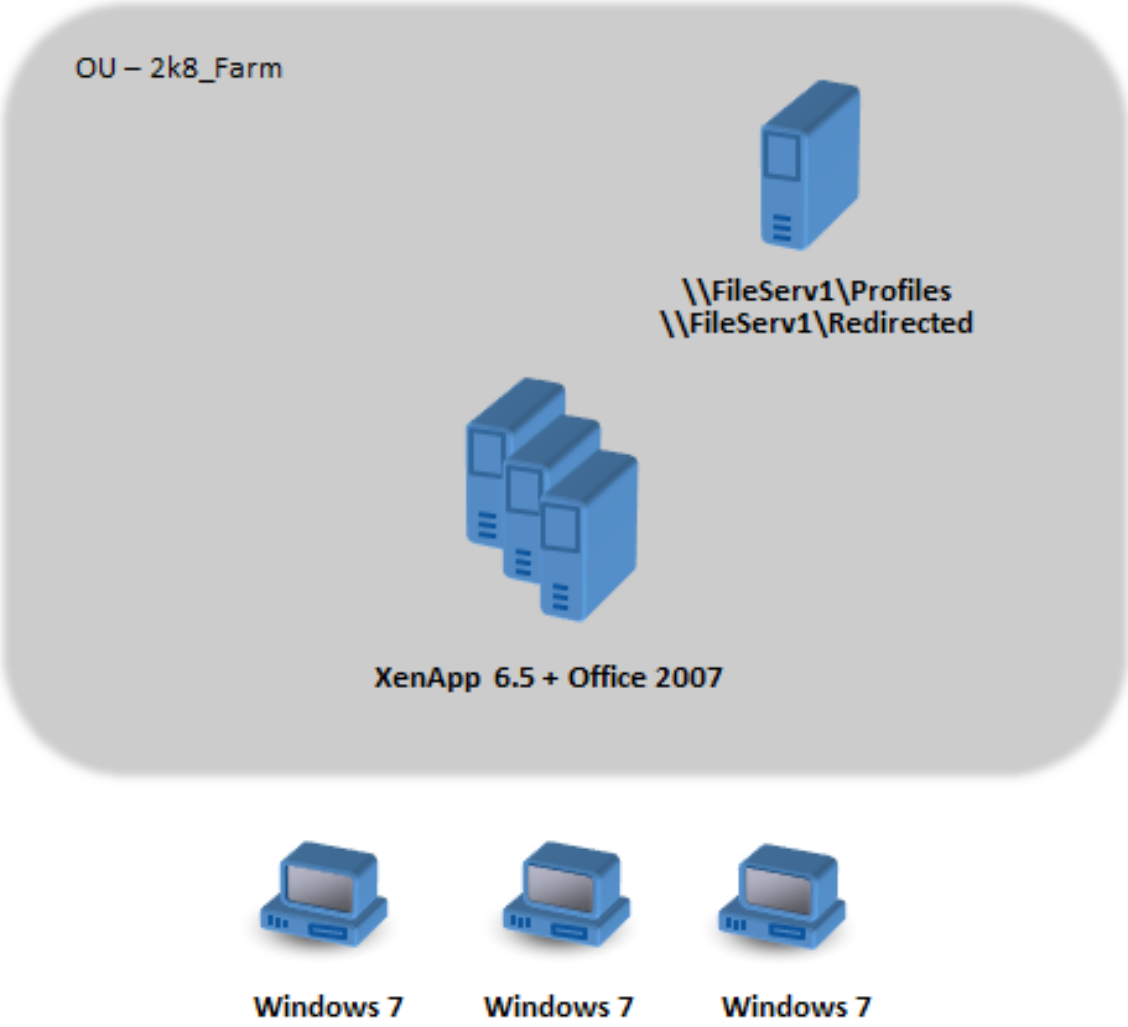
- Initial configuration
- Plan the new site
- Execute the plan
- Other considerations

Initial configuration

September 7, 2025

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.



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

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

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

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

So, for example, user john.smith has a profile at \\FileServ1\Profiles\john.smith\Win7 for the Windows 7 desktop and at \\FileServ1\Profiles\john.smith\Win2008 for the Citrix Virtual Apps servers. Separate profiles are maintained for desktops and servers. The administrator is aware that issues exist when profiles roam between workstation and multi-session operating systems and is being cautious.

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

Plan the new site

September 7, 2025

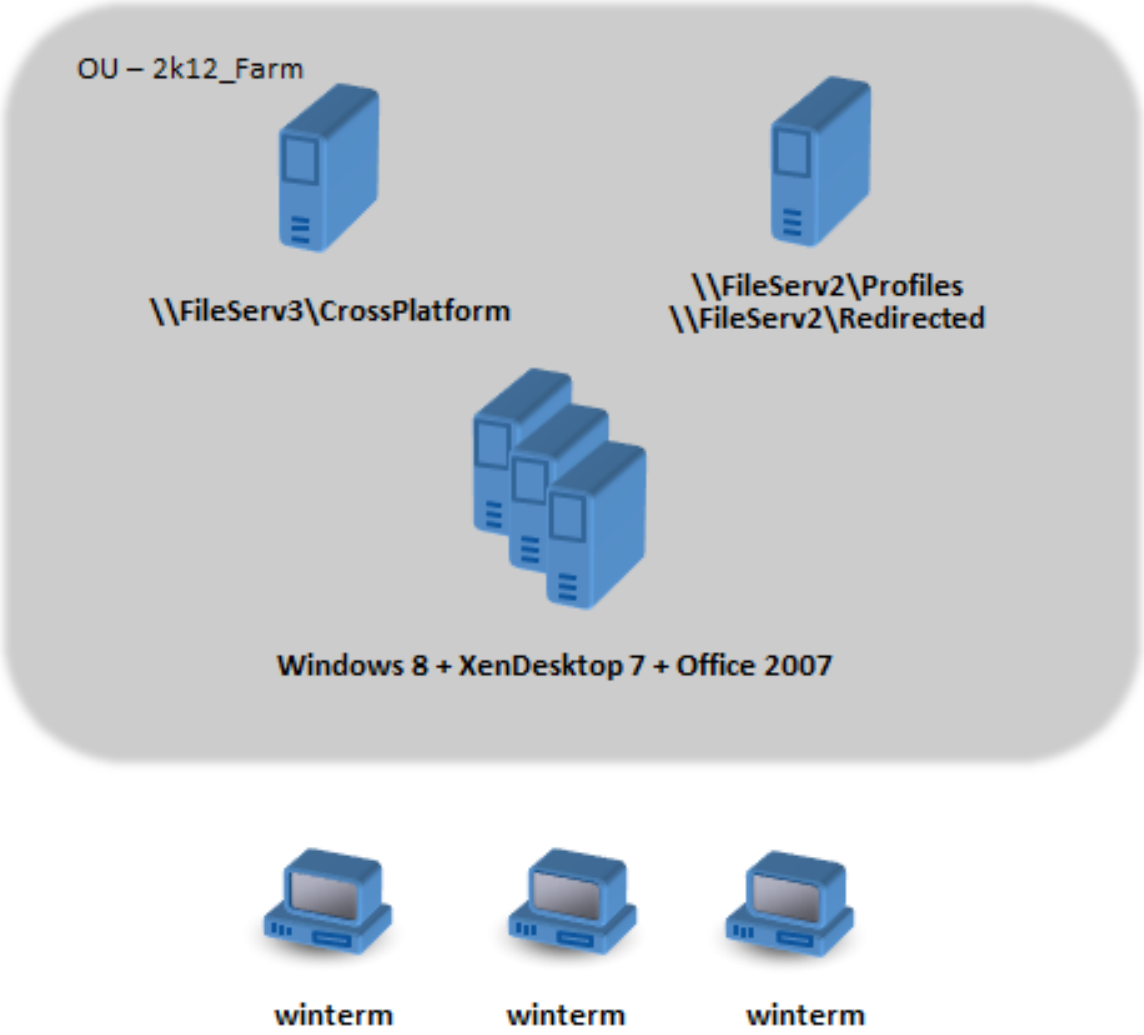
The network administrators have decided to set up a new domain for the new environment, based on Windows Server 2012 domain controllers and Active Directory 2012. Ultimately, a new Citrix Virtual Apps farm is planned, based on Windows Server 2012 running Citrix Virtual Apps. But for now, the new domain is used only for the Windows 7 Citrix Virtual Desktops™ site.

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

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

The following graphic illustrates the configuration of the new Citrix Virtual Desktops site.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Execute the plan

September 7, 2025

Phase 1: Configure the new file servers

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

In this case, we choose to set up separate file servers for the profiles and for the cross-platform settings. This way is not strictly necessary, but it is an easy way of making the cross-platform settings server

© 1997–2026 Citrix Systems, Inc. All rights reserved.

available. The profile server might be designed differently, using DFS namespaces for example, and so take longer to implement.

In both cases, set up the server shares according to the security recommendations for roaming user profiles on shared folders. For more information, see https://docs.microsoft.com/en-us/windows-server/storage/folder-redirection/deploy-roaming-user-profiles.

Phase 2: Upgrade the machines in 2k8_Farm to Profile Management 5.0

For instructions, see Upgrade Profile Management.

Phase 3: Choose which definition files to deploy

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

Important: Do not update these files unless instructed to by Citrix® personnel.

Choose the configuration files that are relevant to your deployment, and copy only these files to \\FileServ3\CrossPlatform\Definitions. In this example, copy just Office 2007.xml.

Phase 4: Configure the machines in 2k8_Farm for Profile Management 5.0

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

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

No changes are required to the machine logon script.

No changes are required to the folder redirection policy.

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

Phase 5: Prepare the machines in 2k12_Farm

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

Policy	Value	Notes
Path to user store	\FileServ2\Profiles\%USERNAME%.%USERDOMAIN%\%ProfVer%	As this file share is used by users from both domains, it is important also to include domain information.
Active write back	Disabled	
Enable cross-platform settings	Enabled	
Cross-platform settings user groups	Disabled	All user groups are processed.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Policy	Value	Notes
Path to cross-platform definitions	\FileServ3\CrossPlatform\Definitions	This path is where the definition files are located. This setting must match the setting in 2k8_Farm.
Path to cross-platform settings store	\FileServ3\CrossPlatform\Store\%USERNAME%.%USERDOMAIN%	Use roaming and mandatory settings store is shared by users of both domains, so both %USERNAME% and %USERDOMAIN% must be specified in the path. This setting must match the setting in 2k8_Farm.
Source for creating cross-platform settings	Disabled	Prevents settings from NewDomain being used for the initial setup of the profile data in the cross-platform settings store. It ensures that settings from OldDomain take precedence.

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

Machine Type	%ProfVer%	Notes
XenApp server on Windows 2012	Win2012x64	It is required when your planned 64-bit servers become available. See Other considerations for more information.
Windows 7 desktops	Win7	If both 32-bit and 64-bit versions of Windows 7 are deployed, it is recommended that they have separate profiles. So %ProfVer% must be configured differently on each platform.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

So the OldDomain user john.smith has a profile at \\FileServ2\Profiles\ john.smith.OldDomain\Win7 for the Windows 7 desktop and at \\FileServ2\Profiles\john.smith.OldDomain\Win2012x64 for the Citrix Virtual Apps servers.

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

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

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

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

Phase 6: Live testing

You perform testing in two stages:

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Other considerations

September 7, 2025

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

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

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

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

Force user logoffs

September 25, 2020

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

Synchronize file security attributes

September 7, 2025

Security attributes can be synchronized when Profile Management copies files and folders in a user profile between the system on which the profile is installed and the user store. This feature aims to prevent inconsistencies among security attributes. It requires Windows 10 and later, and in Windows Server 2016.

This feature is enabled by default. To disable it, do the following:

1. In the **UPMPolicyDefaults_all.ini** file, add **SecurityPreserveEnabled=0** in the **General Settings** section.
2. From a command line, run the command `gpupdate /force`.

Note: Profile Management synchronizes profile changes based on the latest modification time of the profile. Profile Management does not synchronize a file if the changes are made only to the file's security attributes.

Enable large file handling

September 7, 2025

Large files existing in a profile are a common reason for a slow logon or logoff. Citrix® provides an option to redirect large files to the user store. This option eliminates the need to synchronize those files over the network.

To enable large file handling in group policy, do the following:

1. Under **Profile Management**, open the **File system** folder.
2. Double-click the **Large File Handling - Files to be created as symbolic links** policy.
3. Specify files to be handled.

To enable large file handling in the UPMPolicyDefaults_all.ini file, do the following:

1. Add the **[LargeFileHandlingList]** section in the .ini file.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Specify files to be handled under that section.

You can use wildcards in policies that refer to files. For example, !ctx_localappdata!\Microsoft\Outlook*.ost

Make sure that these files are not added to the exclusion list from Citrix Profile Management.

> **Note**
>
> Some applications do not allow concurrent file access. Citrix recommends that you take application behavior into consideration when you define your large file handling policy.
>
> We recommend that you apply Microsoft security update MS15-090. As a general security practice, keep your Microsoft Windows systems updated.

Enable application profiler

September 7, 2025

This feature defines application-based profile handling. When you enable this feature, only the settings defined in the definition file are synchronized.

To enable the application profiler feature, do the following:

1. Under **Profile Management**, open the **Citrix Virtual Apps™ Optimization settings** folder.
2. Enable the **Enable Citrix Virtual Apps Optimization** policy.
3. Enable the **Path to Citrix Virtual Apps optimization definitions** policy.
4. Specify a folder where the Citrix Virtual Apps optimization definition files are located.
5. Run the command `gpupdate /force` to enforce policy deployment.

> **Note:**
>
> For information about creating definition files, see Create a definition file.
>
> During logoff, only settings in the definition file are synchronized, all other settings are discarded. Use folder redirection in case you want to view or update user documents in the session. For more information, see Configure folder redirection.

Enable native Outlook search experience

September 25, 2020

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The **Enable search index roaming for Outlook** feature provides native Outlook search experience. With this feature, the Microsoft Outlook offline folder file (`.ost`) and the search database specific to a user are roamed along with the user profile.

Before being able to use the **Enable search index roaming for Outlook** feature, enable the Microsoft Windows Search Service. By default, the Microsoft Windows Search Service is enabled on Windows desktops. To enable the Microsoft Windows Search Service on Windows servers, perform the following steps:

1. Open **Server Manager** from the **Start** menu.
2. In the upper-right corner of the interface, click **Manage** and then select **Add Roles and Features**.
3. In the **Add Roles and Features Wizard**, the **Before You Begin** page appears by default. Click **Next**.
4. On the **Installation Type** page, select **Role-based or feature-based installation** and then click **Next**.
5. On the **Server Selection** page, select the server to install the Microsoft Windows Search Service on and then click **Next**. If you have only one server, the server is automatically selected.
6. On the **Server Roles** page, click **Next**.
7. On the **Features** page, select **Windows Search Service** and then click **Next**.
8. On the **Confirmation** page, click **Install**. It might take a few minutes to install the Windows Search Service.
9. After the installation completes, on the **Results** page, click **Close**.
10. Click **Search** from the **Start** menu, type **services** in the search box, and then press **Enter**.
11. In the **Services** window, double-click **Windows Search**, set the startup type to **Automatic**, click **Apply**, and then click **OK**.
12. Close the **Services** and the **Server Manager** windows.

After enabling the Microsoft Windows Search Service, perform the following steps to configure **Enable search index roaming for Outlook** in Group Policy Objects.

1. Open the Group Policy Management Editor.
2. Under **Policies > Administrative Templates: Policy definitions (ADMX files) > Citrix Components > Profile Management > Advanced settings**, double-click the **Enable search index roaming for Outlook** policy.
3. Select **Enabled**. Click **OK**.

If search index roaming is not configured in Group Policy Objects, the value from the .ini file is used. If search index roaming is not configured anywhere, it is disabled by default.

For your changes to take effect, run the `gpupdate /force` command from the command prompt, log off from all sessions, and then log on again. For details, see https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/gpupdate.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> To make the search index roaming feature work on Microsoft Windows 10 1809 and later, and on Windows Server 2019 and later, add a DWORD value `EnablePerUserCatalog = 0` under `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Search`. Restart the VDA to make your registry setting take effect.

VHDX files

The VHDX (Virtual Hard Disk) is a disk file format that is used to provision virtual and logical disk storage space to virtual machines. The Enable search index roaming for Outlook feature relies on VHDX files to work. VHDX files are created for each user that uses the feature. VHDX files store a user-specific profile on a separate virtual disk that is dedicated to that user's profile. Profile Management mounts VHDX files on logon and unmounts them on logoff. There are two VHDX files:

- OutlookOST.vhdx file, containing the Microsoft Outlook offline folder file (`.ost`)
- OutlookSearchIndex.vhdx file, containing the search index database for the offline folder file stored in the OutlookOST.vhdx file

> **Note:**
>
> Profile Management mounts VHDX files only when users log on. It does not remount the VHDX files *after* logon, even if the VHDX files are unmounted.
> Profile Management provides a default VHDX capacity of 50 GB. Plan your storage quota accordingly. If the actual usage of your VHDX exceeds the quota you configured earlier, your VHDX file is unmounted.

Quick creation of VHDX files

As an enhancement to the **Enable search index roaming for Outlook** feature, Profile Management accelerates the creation of user-specific VHDX files. It does so by generating user-specific VHDX files as copies of the template VHDX file (UpmParentVhd.vhdx). The template VHDX file is created automatically when the first user logs on.

For example, if the **Enable search index roaming for Outlook** feature is enabled, the following VHDX folder files are available after logon:

- A folder `UpmVhd` in the user store. This folder is located in the root folder of the user store. For example, if the user store is configured as `\\Fileshare\UpmStore$\\%USERNAME%.%USERDOMAIN%\!CTX_OSNAME!_!CTX_OSBITNESS!`, the `UpmVhd folder` is created at `\\Fileshare\UpmStore$\`.
- A file `UpmParentVhd.vhdx` in the `UpmVhd` folder.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

When other users log on, Profile Management generates the VHDX files specific to those users' profiles as copies of the template VHDX file.

Automatic backup and restore of Outlook search index database

Profile Management can automatically save a backup of the last known good copy of the search index database and revert to the copy if corruption occurs. To achieve this purpose, enable search index roaming for Outlook and then enable the Outlook search index database –backup and restore policy. For more information, see Automatic backup and restore of Outlook search index database.

Prerequisites

Software requirements:

- Microsoft Windows 10 1709 or later
- Windows Server 2016 or later
- Microsoft Outlook 2016 (32-bit or 64-bit) or Microsoft Office 365

The following versions of the Microsoft Windows Search Service (SearchIndexer.exe) have been tested and are supported:

- 7.0.17134.376
- 7.0.17134.285
- 7.0.17134.228
- 7.0.17134.1
- 7.0.16299.402
- 7.0.16299.248
- 7.0.16299.15
- 7.0.15063.413
- 7.0.14393.2457
- 7.0.14393.2430
- 7.0.14393.2368
- 7.0.14393.2312
- 7.0.14393.2273
- 7.0.14393.2248

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 7.0.14393.1884
- 7.0.10240.17443
- 7.0.9600.18722
- 7.0.1493.1593
- 7.0.1393.2125
- 7.0.1393.1884
- 7.0.1393.1770

> **Note:**
>
> - Concurrent sessions on multiple machines are not supported.
> - This feature is expected to support the future versions of the Microsoft Windows Search Service. If you find that the feature does not support specific future versions of the Microsoft Windows Search Service, contact Citrix Technical Support.

Automatic backup and restore of Outlook search index database

September 7, 2025

Profile Management provides a solution to ensure the stability of the Enable search index roaming for Outlook feature. It does so by automatically saving a backup of the last known good copy of the search index database and then reverting to the copy in case of corruption. As a result, you no longer need to manually reindex the database when it becomes corrupted.

This feature is disabled by default. To use it, you must enable search index roaming for Outlook first. For more information about search index roaming for Outlook, see Enable native Outlook search experience.

After enabling search index roaming for Outlook, complete the following steps to enable this feature:

1. Open the Group Policy Management Editor.
2. Under **Policies > Administrative Templates: Policy definitions (ADM) > Classic Administrative Templates (ADM) > Citrix® > Profile Management > Advanced settings**, double-click the **Outlook search index database –backup and restore** policy.
3. Select **Enabled** and then click **OK**.

For your changes to take effect, run the `gpupdate /force` command from the command prompt. Log off from all sessions and then log on again. For more information, see https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/gpupdate.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

You can also choose to configure the Profile Management policies in Citrix Studio. To do so, complete the following steps:

1. In the left pane of Citrix Studio, click **Policies**.
2. In the **Create Policy** window, type the policy in the search box. For example, type "Outlook search index database –backup and restore."
3. Click **Select** to open the **Outlook search index database –backup and restore** policy.
4. Select **Enabled** and then click **OK**.

How it works

If this feature is enabled, Profile Management saves a backup of the search index database each time the database is mounted successfully on logon. Profile Management deletes the previously saved backup after a new backup is saved successfully. Profile Management treats the backup as the good copy of the search index database. When an attempt to mount the search index database fails, Profile Management automatically reverts the search index database to the last known good copy.

> **Important:**
>
> - Profile Management does not save a backup of the search index database after the policy takes effect the first time the search index database is created.
> - Profile Management deletes the previously saved backup after a new backup is saved successfully. The backup consumes more of the available storage space of the VHDX files.

Profile container

September 7, 2025

> **Important:**
>
> This feature does not work on Windows 7.

Large folders associated with a user profile result in a slow logon. Profile Management provides a VHDX-based profile solution that lets you specify the folders to be contained in the profile disk (VHDX files). This solution reduces logon times by mapping the specified folders to the profile disk that is stored on the network. The profile container attaches the profile disk containing those folders during logon, thus eliminating the need to save a copy of the folders to the local profile. Doing so decreases logon times.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> - The maximum permitted size for the VHDX files is 50 GB. You cannot modify this value.
> - Profile Management automatically grants permissions to the folder where the VHDX files are stored. Doing so allows the Profile Management service to access and mount VHDX files.
> - The VHDX files do not shrink automatically, even if you manually delete files from them. If you want to reduce the size of the VHDX files, go to Disk Management, right-click the applicable volume, and then select **Shrink Volume**.

There are two scenarios to be aware of:

- The profile container does not support simultaneous access by multiple sessions.
- The profile container does not support containing the entire profile.

The profile disk is stored at a user's user store path. For example, if you configure your user store path as `\\myprofileserver\profiles$\\%username%.%domain%\!ctx_osname!.!ctx_osbitness!`, the profile disk is located at `\\myprofileserver\profiles$\\%username%.%domain%\!ctx_osname!.!ctx_osbitness!\ProfileContainer\!ctx_osname!`.

To understand how a profile container works, you can regard it as a secondary user store that is designed for storing profile-related large folders such as cache folders. Even if the folders are present in the exclusion list, they are still stored in the profile disk after you enable the profile container feature and add the folders to the profile container list.

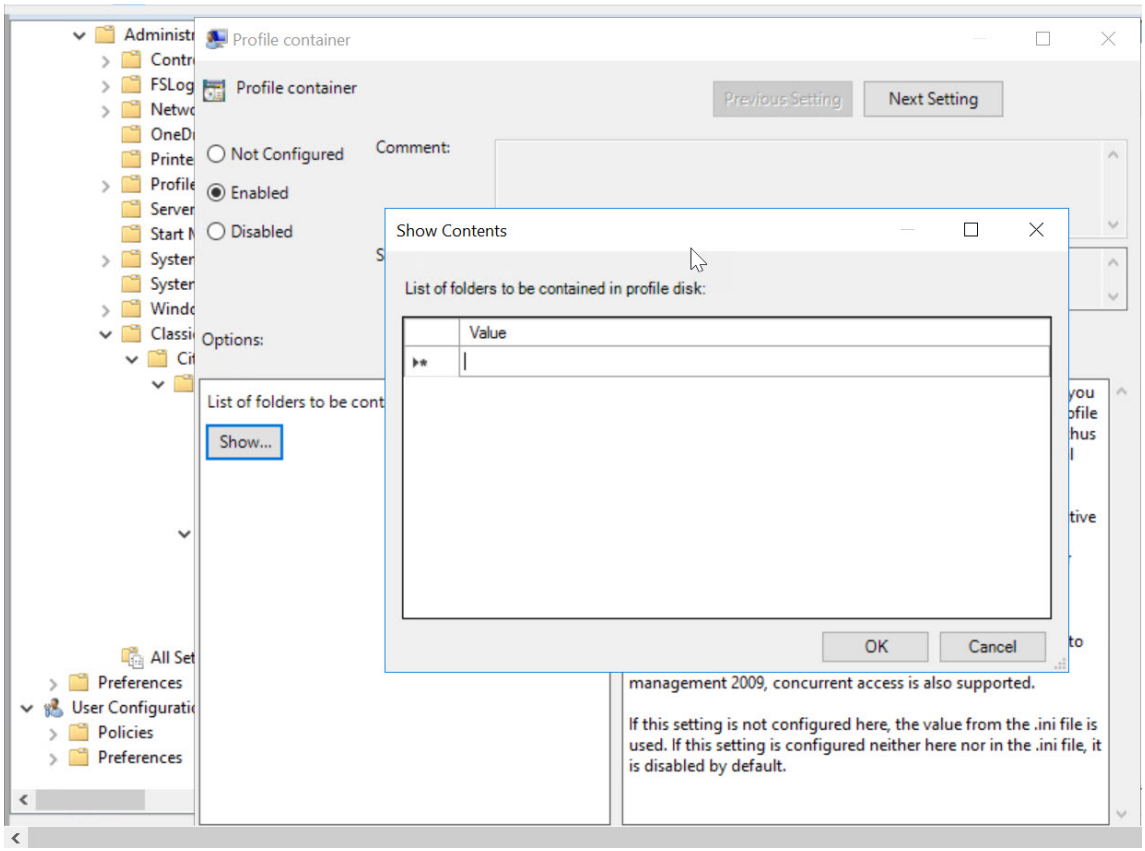
Suppose you enable the profile container feature and then you disable it. To ensure a consistent user profile, Profile Management synchronizes the user store profile with a profile container. This synchronization occurs during user logon. Folders in the exclusion list are not copied to the user store.

To enable the profile container feature, do the following:

1. Open the Group Policy Management Editor.
2. Under **Computer Configuration > Policies > Administrative Templates: Policy definitions (ADMX files) > Citrix Components > Profile Management > File system > Synchronization**, double-click the Profile container policy.
3. Select **Enabled**.
4. Click **Show** to add the relative paths of the folders to contain in the profile container. We recommend that you add folders that contain large cache files. For example, add the Citrix Files content cache folder to the list: `AppData\Local\Citrix\Citrix Files\PartCache`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> The folders you add to the profile container also exist in the user store. After you enable the profile container feature, Profile Management keeps the folders synchronized between the profile container and the user store.



5. Click **OK**.

> **Note:**
>
> To delete the folders contained in the profile disk for a specific user, you can perform the profile reset from Citrix Director. For more information, see Reset a user profile.

Policies

September 7, 2025

This topic provides:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Profile Management policies - describing policies by version and variables available for use in both Group Policy and the .ini file
- Profile Management policy descriptions and defaults - providing reference information on each policy, including policy default settings

Profile Management policies

September 13, 2025

This article describes important aspects of the policies in the .adm and .admx files.

Profile Management variables

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

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

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

For policies that are used to build paths, the `\!ctx\\_osbitness\!` variable expands to x86 or x64 depending on the operating system. The following variables also expand:

- !ctx_osname! expands to the short name as follows depending on the operating system.
- !ctx_profilever! expands to the profile version as follows depending on the operating system.

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Long Name	Short Name	Profile Version
Windows 10 Redstone 6	Win10RS6	v6
Windows 10 Redstone 5	Win10RS5	v6
Windows 10 Redstone 4	Win10RS4	v6
Windows 10 Redstone 3	Win10RS3	v6
Windows 10 Redstone 2	Win10RS2	v6
Windows 10 Redstone 1	Win10RS1	v6
Windows 10	Win10	v5
Windows 8.1	Win8.1	v4 or v2
Windows 8	Win8	v3 or v2
Windows 7	Win7	v2
Windows Server 2019	Win2019	v6
Windows Server 2016	Win2016	v6
Windows Server 2012 R2	Win2012R2	v4 or v2
Windows Server 2012	Win2012	v3 or v2
Windows Server 2008 R2	Win2008	v1
Windows Server 2008	Win2008	v1

> **Note:**
>
> For Windows 8, Windows 8.1, Windows Server 2012, and Windows Server 2012R2, the actual profile version might change. If the `UseProfilePathExtensionVersion` registry key under `HLKM\System\CurrentControlset\Services\ProfSvc\Parameters` is set to 1, the profile version is v3 or v4 depending on the operating system. If it is not set or is set to 0, the profile version is v2.

Policies by version

As an aid to migration, the following tables show the policies that are available in different versions of Profile Management, the location of each policy in the .adm (or .admx) file and in the .ini file, and the feature each policy is designed for (or whether it is part of the base configuration of all deployments).

The location in the .adm or .admx file is relative to `Citrix > Profile Management`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Policies available from Version 1909

Policy in .adm or .admx file	Location in .adm or .admx file	Policy in .ini file	Feature
MigrateUserStore	\	MigrateUserStore	Migrate UserStore
OutlookEdbBackupEnabled	\AdvancedSettings	OutlookEdbBackupEnabled	Outlook search index database - backup and restore
ApplicationProfilesAutoMigration	\AdvancedSettings	ApplicationProfilesAutoMigration	Automatic migration of existing application profiles

Policy available from Version 1903

Policy in .adm or .admx file	Location in .adm or .admx file	Policy in .ini file	Feature
ProfileContainer	**Before Version 2009:** \FileSystemSet-tings\FSSynchronization **Version 2009 and later:** \ProfileContainer	ProfileContainer	Profile Container

Policy available from Version 7.18

Policy in .adm or .admx file	Location in .adm or .admx file	Policy in .ini file	Feature
OutlookSearchRoamingEnabled	\AdvancedSettings	OutlookSearchRoamingEnabled	Outlook search roaming

Policies available from Version 7.16

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Policy in .adm or .admx file	Location in .adm or .admx file	Policy in .ini file	Feature
XenAppOptimizationSettings	\XenAppOptimizationSettings	XenAppOptimizationSettings	CVAD application optimization
XenAppOptimizationDefinitionPaths	\XenAppOptimizationSettings	XenAppOptimizationDefinitionPaths	CVAD application optimization
LargeFileHandlingList	\FileSystemSettings	LargeFileHandlingList	Large file handling

Policies available from Version 7.15

Policy in .adm or .admx file	Location in .adm or .admx file	Policy in .ini file	Feature
LogonExclusionCheck	\FileSystemSettings	LogonExclusionCheck	Logon exclusion check

Policy available from Version 5.8

Policy in .adm or .admx file	Location in .adm or .admx file	Policy in .ini file	Feature
StreamingExclusionList	\PsSettings	StreamingExclusionList	Profile streaming exclusion list

Policies available from Version 5.6

Policy in .adm or .admx file	Location in .adm or .admx file	Policy in .ini file	Feature
CEIPEnabled	\AdvancedSettings	CEIPEnabled	CEIP
PSMidSessionWriteBackReg	\	PSMidSessionWriteBackReg	Active write back registry

Policies available from Version 5.5

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Policy in .adm or .admx file	Location in .adm or .admx file	Policy in .ini file	Feature
Default Exclusion list	\Registry	DefaultExclusionListRegistry	Base
NTUSER.DAT	\Registry	LastKnownGoodRegistry	Backup NTUSER.DAT
Default Exclusion list - directories	\File system	DefaultSyncExclusionListDir	Base

Policies available from Version 5.0 to 5.4

Policy in .adm or .admx file	Location in .adm or .admx file	Policy in .ini file	Feature
Excluded groups	\	ExcludedGroups	Excluded Groups
Disable automatic configuration	\Advanced Settings	DisableDynamicConfig	Automatic Configuration
Redirect the AppData (Roaming) folder, Redirect the Desktop folder, …	\Folder Redirection (in User Configuration)	Note: Not applicable	Integration with XenDesktop
Delay before deleting cached profiles	\Profile handling	ProfileDeleteDelay	Base

Policies available from Version 4.x

Policy in .adm or .admx file	Location in .adm or .admx file	Policy in .ini file	Feature
Cross-platform settings user groups	\Cross-platform settings	CPUserGroupList	Cross-platform settings
Enable cross-platform settings	\Cross-platform settings	CPEnabled	Cross-platform settings
Source for creating cross- platform settings	\Cross-platform settings	CPMigrationFromBaseProfileToCPStore	Cross-platform settings
Path to cross-platform definitions	\Cross-platform settings	CPSchemaPath	Cross-platform settings

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Policy in .adm or .admx file	Location in .adm or .admx file	Policy in .ini file	Feature
Path to cross-platform settings store	\Cross-platform settings	CPPath	Cross-platform settings
Offline profile support	\Cross-platform settings	OfflineSupport	Offline profiles
Log off user if a problem is encountered	\Advanced Settings	LogoffRatherThanTempProfile	Improved Troubleshooting

Policies available from Version 3.x

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Policies available from Version 2.x

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Policy in .adm or .admx file	Location in .adm or .admx file	Policy in .ini file	Feature
Log settings	\Log settings	LogLevel	Logging
Maximum size of the log file	\Log settings	MaxLogSize	Logging
Path to log file (available from Version 2.1)	\Log settings	PathToLogFile	Logging

Profile Management policy descriptions and defaults

September 7, 2025

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

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

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

Sections in the .adm and .admx files

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

Profile Management

Profile Management\Folder Redirection (User Configuration)

Profile Management\Profile handling

Profile Management\Advanced settings

Profile Management\Log settings

Profile Management\Registry

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Profile Management\File system

Profile Management\File system\Synchronization

Profile Management\Streamed user profiles

Profile Management\Cross-platform settings

Profile Management

Enable Profile Management

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

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

Processed groups

Both computer local groups and domain groups (local, global, and universal) can be used. Specify domain groups in the format: DOMAIN NAME\GROUP NAME.

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

Excluded groups

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

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Process logons of local administrators

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

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

Path to user store

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

The path can be:

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

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

- System environment variables enclosed in percent signs (for example, %ProfVer%). System environment variables generally require extra setup.
- Attributes of the Active Directory user object enclosed in hashes (for example, #sAMAccountName#).
- Profile Management variables. For more information, see the Profile Management variables product document.

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

Examples:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

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

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

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

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

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

Migrate user store

Specifies the path to the folder where the user settings (registry changes and synchronized files) were previously saved (the user store path that you previously used).

If this setting is configured, the user settings stored in the previous user store are migrated to the current user store specified in the Path to user store policy.

The path can be an absolute UNC path or a path relative to the home directory.

In both cases, you can use the following types of variables: system environment variables enclosed in percent signs and attributes of the Active Directory user object enclosed in hash signs.

Examples:

- The folder `Windows\\%ProfileVer%` stores the user settings in a subfolder called `Windows\W2K3` of the user store (if %ProfileVer% is a system environment variable that resolves to W2K3).
- `\\server\share\\#SAMAccountName#` stores the user settings to the UNC path `\\server\share\<JohnSmith>` (if `#SAMAccountName#` resolves to JohnSmith for the current user).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

In the path, you can use user environment variables except %username% and %userdomain%.

If this setting is disabled, the user settings are saved in the current user store.

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

If this setting is not configured here or in the .ini file, the user settings are saved in the current user store.

Active write back

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

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

Offline profile support

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

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

Active write back registry

Use this policy along with "Active write back."Registry entries that are modified can be synchronized to the user store in the middle of a session.

If you do not configure this setting here, the value from the .ini file is used.

If you do not configure this setting here or in the .ini file, the active write back registry is disabled.

Offline profile support

Enables the offline profiles feature. This setting is intended for computers that are commonly removed from networks, typically laptops or mobile devices, not servers or desktops.

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, offline profile support is disabled.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Profile Management\Folder Redirection (User Configuration)

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

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

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

The Redirect <folder-name> folder policy lets you specify how to redirect the <folder-name> folder. To do so, select **Enabled** and then type the redirected path.

Caution: Potential data loss might occur.

You might want to modify the path after the policy takes effect. However, consider potential data loss before you do so. The data contained in the redirected folder might be deleted if the modified path points to the same location as the previous path.

For example, suppose you specify the Contacts path as path1. Later, you change path1 to path2. If path1 and path2 point to the same location, all data contained in the redirected folder is deleted after the policy takes effect.

To avoid potential data loss, complete the following steps:

1. Apply Microsoft policy to machines where Profile Management is running through Active Directory Group Policy Objects. To do so, open the Group Policy Management Console, navigate to **Computer Configuration > Administrative Templates > Windows Components > File Explorer**, and then enable **Verify old and new Folder Redirection targets point to the same share before redirecting**.
2. If applicable, apply hotfixes to machines where Profile Management is running. For details, see https://support.microsoft.com/en-us/help/977229 and https://support.microsoft.com/en-us/help/2799904.

Profile Management\Profile handling

Delete locally cached profiles on logoff

Specifies whether locally cached profiles are deleted after logoff.

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

Delay before deleting cached profiles

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

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

Migration of existing profiles

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

The following event takes place during logons. 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 profiles is used as in a setup without Profile Management.

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

Automatic migration of existing application profiles

This setting enables or disables the automatic migration of existing application profiles across different operating systems. The application profiles include both the application data in the **AppData**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

folder and the registry entries under HKEY_CURRENT_USER\SOFTWARE. This setting can be useful in cases where you want to migrate your application profiles across different operating systems.

For example, suppose you upgrade your operating system (OS) from Windows 10 version 1803 to Windows 10 version 1809. If this setting is enabled, Profile Management automatically migrates the existing application settings to Windows 10 version 1809 the first time each user logs on. As a result, the application data in the **AppData** folder and the registry entries under HKEY_CURRENT_USER\SOFTWARE are migrated.

If there are multiple existing application profiles, Profile Management performs the migration in the following order of priority:

1. Profiles of the same OS type (single-session OS to single-session OS and multi-session OS to multi-session OS).
2. Profiles of the same Windows OS family; for example, Windows 10 to Windows 10, or Windows Server 2016 to Windows Server 2016).
3. Profiles of an earlier version of the OS; for example, Windows 7 to Windows 10, or Windows Server 2012 to Windows 2016.
4. Profiles of the closest OS.

Note: You must specify the short name of the OS by including the variable "!CTX_OSNAME!"in the user store path. Doing so lets Profile Management locate the existing application profiles.

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, it is disabled by default.

Local profile conflict handling

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

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

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

Template profile

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

file.

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

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

If this policy is disabled, templates are not used. If this policy is enabled, Profile Management uses the template instead of the local default profile when creating 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 the local profile is migrated to the user store, if this policy is not disabled. This setup can be changed by enabling the **Template profile overrides local profile** or **Template profile overrides roaming profile** check box. Also, identifying the template as a Citrix mandatory profile means that, like Windows mandatory profiles, changes are not saved.

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

Profile Management\Advanced settings

Number of retries when accessing locked files

Sets the number of retries when accessing locked files.

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

Process Internet cookie files on logoff

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

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Disable automatic configuration

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

You can regard automatic configuration as a dynamic configuration checker that automatically configures the default policy settings according to environments at runtime. It eliminates the need to configure the settings manually. Runtime environments include:

- Windows OS
- Windows OS versions
- Presence of Citrix Virtual Desktops
- Presence of personal vDisks

Automatic configuration might change the following policies if the environment changes:

- Active write back
- Always cache
- Delete locally cached profiles on logoff
- Delay before deleting cached profiles
- Profile streaming

See the following table for the default status of the preceding policies on different OSs:

	Multi-session OS	Single-session OS
Active write back	Enabled	*Disabled* if Personal vDisk is in use; otherwise, enabled.
Always cache	Disabled	*Disabled* if Personal vDisk is in use; otherwise, enabled.
Delete locally cached profiles on logoff	Enabled	*Disabled* if Personal vDisk is in use or if Citrix Virtual Desktops is assigned or if Citrix Virtual Desktops is not installed; otherwise, enabled.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

	Multi-session OS	Single-session OS
Delay before deleting cached profiles	0 seconds	60 seconds if user changes are not persistent; otherwise, 0 seconds.
Profile streaming	Enabled	*Disabled* if Personal vDisk is in use; otherwise, enabled.

However, with automatic configuration disabled, all policies above default to **Disabled**.

Starting with Profile Management 1909, you can have an improved experience with the Start menu on Windows 10 (version 1607 and later) and Windows Server 2016 and later. This is achieved through automatic configuration of the following policies:

- Add `Appdata\Local\Microsoft\Windows\Caches` and `Appdata\Local\Packages` to **Folders to Mirror**
- Add `Appdata\Local\Microsoft\Windows\UsrClass.Dat*` to **Files to synchronize**

> **Note:**
>
> Starting with Citrix Profile Management 1912, a folder added to the exclusion list cannot be synchronized even if you add it to **Folders to mirror**. As a workaround, remove the `appdata\local\packages` folder from the exclusion list before you add it to **Folders to mirror**.

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

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

Log off user if a problem is encountered

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

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

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

Customer Experience Improvement Program

By default, the Customer Experience Improvement Program is enabled to help improve the quality and performance of Citrix products by sending anonymous statistics and usage information.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

Enable search index roaming for Outlook

Allow user-based Outlook search experience by automatically roaming Outlook search data along with user profile. This requires extra spaces in the user store to store search index for Outlook.

Log off and then log on again for this policy to take effect.

Outlook search index database –backup and restore

This setting configures what Profile Management does during logon when the Enable search index roaming for Outlook is enabled.

If this setting is enabled, Profile Management saves a backup of the search index database each time the database is mounted successfully on logon. Profile Management treats the backup as the good copy of the search index database. When an attempt to mount the search index database fails because the database becomes corrupted, Profile Management automatically reverts the search index database to the last known good copy.

Note: Profile Management deletes the previously saved backup after a new backup is saved successfully. The backup consumes the available storage space of the VHDX files.

Profile Management\Log settings

Enable logging

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

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

Log settings

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

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

The check boxes for these policies correspond to the following settings in the .ini file: LogLevelWarnings, LogLevelInformation, LogLevelFileSystemNotification, LogLevelFileSystemActions,

© 1997–2026 Citrix Systems, Inc. All rights reserved.

LogLevelRegistryActions, LogLevelRegistryDifference, LogLevelActiveDirectoryActions, LogLevelPolicyUserLogon, LogLevelLogon, LogLevelLogoff, and LogLevelUserName.

Maximum size of the log file

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

If this policy is disabled, the default value of 10 MB is used. If this policy is not configured here, the value from the .ini file is used. If this policy is not configured here or in the .ini file, the default value is used.

Path to log file

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

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

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

Examples:

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

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Profile Management\Registry

Exclusion list

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

Example: Software\Policies

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

Inclusion list

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

Example: Software\Adobe.

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

Enable Default Exclusion List - Profile Management 5.5

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

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

NTUSER.DAT backup

Enables a backup of the last known good copy of NTUSER.DAT and rollback if there is corruption.

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Profile Management\File system

Exclusion list - files

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

Examples:

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

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

Enable Default Exclusion List - directories

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

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

Exclusion list - directories

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

Example:

- Desktop ignores the Desktop folder in the user profile

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

Logon Exclusion Check

This setting configures what Profile Management does if a profile in the user store contains excluded files or folders.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

If this setting is disabled or set to the default value of "Synchronize excluded files or folders on logon," Profile Management synchronizes these excluded files or folders from the user store to the local profile when a user logs on.

If this setting is set to "Ignore excluded files or folders on logon,"Profile Management ignores the excluded files or folders in the user store when a user logs on.

If this setting is set to "Delete excluded files or folder on logon,"Profile Management deletes the excluded files or folders in the user store when a user 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 excluded files or folders are synchronized from the user store to the local profile when a user logs on.

Large File Handling - Files to be created as symbolic links

To improve logon performance and to process large-size files, a symbolic link is created instead of copying files in this list.

You can use wildcards in policies that refer to files; for example, `!ctx_localappdata!\Microsoft\Outlook*.OST`.

To process the offline folder file (`*.ost`) of Microsoft Outlook, make sure that the **Outlook** folder is not excluded for Profile Management.

Those files cannot be accessed in multiple sessions simultaneously.

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.

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

Example:

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

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

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Files to synchronize

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

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

Examples:

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

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

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

Folders to mirror

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

For example, consider how Index.dat references cookies while a user browses the Internet. If a user has two Internet Explorer sessions, each on a different server, and they visit different sites in each session, cookies from each site are added to the appropriate server. When the user logs off from the first session (or in the middle of a session, if the active write back feature is configured), the cookies from the second session must replace those cookies 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 cookies from the last session each time the user logs off. So Index.dat stays up-to-date.

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Profile container

A profile container is a VHDX-based profile solution that lets you specify the folders to be contained in the profile disk. The profile container attaches the profile disk containing those folders, thus eliminating the need to save a copy of the folders to the local profile. Doing so decreases logon times.

To use a profile container, enable this policy and add the relative paths of the folders to the list. We recommend that you include the folders containing large cache files to the list. For example, add the Citrix Files content cache folder to the list: `AppData\Local\Citrix\Citrix Files\PartCache`.

There are two scenarios to be aware of:

- Profile container does not support simultaneous access by multiple sessions.
- Profile container does not support containing the entire profile.

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

Profile Management\Streamed user profiles

Profile streaming

Files and folders contained in a profile are fetched from the user store to the local computer only when they are accessed by users after they have logged on. Registry entries and any files in the pending area are exceptions. They are fetched immediately.

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

Always cache

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

This setting 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 the profile contents as a background task).

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Timeout for pending area lock files

You can set a timeout period (days) that frees up users'files. So the files are written back to the user store from the pending area if the user store remains locked when a server becomes unresponsive. Use this policy to prevent bloat in the pending area and to ensure that the user store always contains the most up-to-date files.

If this policy is not configured here, the value from the .ini file is used. If this policy is not configured here or in the .ini file, the default value of one day is used.

Streamed user profile groups

This policy streams the profiles of a subset of Windows user groups in the OU. The profiles of users in all other groups are not streamed.

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

Profile Streaming Exclusion list - directories

This policy lets you configure a list of directories that are ignored by Profile Streaming. Folder names must be specified as paths relative to the user profile.

Examples:
Entering "Desktop"(without quotes) ignores the Desktop directory in the user profile.

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.

> **Note:**
>
> Profile Streaming exclusions do not indicate that the configured folders are excluded from profile handling. They are still processed by Citrix Profile Management.

Profile Management\Cross-platform settings

Enable cross-platform settings

By default, to facilitate deployment, cross-platform settings are disabled. Turn on processing by enabling this policy but only after thorough planning and testing of this feature.

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Cross-platform settings user groups

Enter one or more Windows user groups. For example, you might use this policy to process only the profiles from a test user group. If this policy is configured, the cross-platform settings feature of Profile Management processes only members of these user groups. If this policy is disabled, the feature processes all the users specified by the **Processed groups** policy.

If this policy is not configured here, the value from the .ini file is used. If this policy is not configured here or in the .ini file, all user groups are processed.

Path to cross-platform definitions

Identifies the network location of the definition files that you copied from the download package. This path must be a UNC path. Users must have read access to this location, and administrators must have write access to it. The location must be a Server Message Block (SMB) or Common Internet File System (CIFS) file share.

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

Path to cross-platform settings store

Sets the path to the cross-platform settings store, the folder in which users'cross-platform settings are saved. Users must have write access to this area. The path can be an absolute UNC path or a path relative to the home directory.

This area is the common area of the user store where profile data shared by multiple platforms is located. Users must have write access to this area. The path can be an absolute UNC path or a path relative to the home directory. You can use the same variables as for the Path to user store.

If this policy is disabled, the path Windows\PM_CP is used. If this policy is not configured here, the value from the .ini file is used. If this policy is not configured here or in the .ini file, the default value is used.

Source for creating cross-platform settings

Specifies a platform as the base platform if this policy is enabled in that platform's OU. This policy migrates data from the base platform's profiles to the cross-platform settings store.

Each platform's own set of profiles are stored in a separate OU. You must decide which platform's profile data to use to seed the cross-platform settings store. It is referred to as the base platform. If

© 1997–2026 Citrix Systems, Inc. All rights reserved.

the cross-platform settings store contains a definition file with no data, or the cached data in a single-platform profile is newer than the definition's data in the store, Profile Management migrates the data from the single-platform profile to the store unless you disable this policy.

> **Important:**
>
> If this policy is enabled in multiple OUs, or multiple user or machine objects, the platform that the first user logs on to become the base profile.
> By default this policy is Enabled.

Profile Management\Citrix Virtual Apps Optimization settings

Enable Citrix Virtual Apps™ Optimization

When you enable this feature, only the settings specific to the published applications a user launches or exits are synchronized.

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 Citrix Virtual Apps optimization settings are applied.

Path to Citrix Virtual Apps optimization definitions

This policy lets you specify a folder where the Citrix Virtual Apps optimization definition files are located.

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 Citrix Virtual Apps optimization settings are applied.

> **Note:**
>
> The folder can be local or it can reside on an SMB file share.

Integrate

September 7, 2025

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

in the Profile Management documentation. For example, for solutions to common issues with Profile Management in such deployments, see Troubleshoot.

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

Profile Management and Citrix Virtual Apps™

September 7, 2025

Use of this version of Profile Management on Citrix Virtual Apps servers is subject to the Profile Management EULA. You can also install Profile Management on local desktops, allowing users to share their local profile with published resources.

Note: Profile Management automatically configures itself in Citrix Virtual Desktops™ but not Citrix Virtual Apps environments. Use Group Policy or the .ini file to adjust Profile Management settings for your Citrix Virtual Apps deployment.

Profile Management works in Citrix Virtual Apps environments that employ Remote Desktop Services (formerly known as Terminal Services). In these environments, you must set up an OU for each supported operating system. For more information, see your Microsoft documentation.

In farms that contain different versions of Citrix Virtual Apps or that run different operating systems, Citrix recommends using a separate OU for each server that runs each version or operating system.

Important: Including and excluding folders that are shared by multiple users (for example, folders containing shared application data published with Citrix Virtual Apps) is not supported.

Streamed applications

Profile Management can be used in environments where applications are streamed to either user devices directly or streamed to Citrix Virtual Apps servers and, from there, published to users.

Client-side application virtualization technology in Citrix Virtual Apps is based on application streaming which automatically isolates the application. The application streaming feature enables applications to be delivered to Citrix Virtual Apps 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 might be installed locally and Office 2007 might be streamed to users' devices. Failure to isolate user settings creates conflicts, and might severely affect the functionality of both applications (local and streamed).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

For requirements relating to the use of Profile Management with streamed applications, see System requirements.

Profile Management and Citrix Virtual Desktops™

September 7, 2025

Important: We recommend using the Profile Management capabilities integrated into Citrix Virtual Desktops. For more information, see the Citrix Virtual Desktops documentation. The information in this topic applies to a different deployment - the use of Citrix Virtual Desktops with the Profile Management component that has been separately installed and configured.

Install and upgrade Profile Management in Citrix Virtual Desktops deployments

Use of this version of Profile Management with Citrix Virtual Desktops is subject to the Profile Management EULA. Subject to the terms in the EULA, you can also use Profile Management with Citrix Virtual Apps™ in a Citrix Virtual Desktops environment.

If you upgrade Profile Management in a Citrix Virtual Desktops deployment, consider the effect on the log file locations as described in Upgrade Profile Management.

For Citrix Virtual Desktops in Quick Deploy setups, see the recommendations in Decide on a configuration.

Configure Profile Management in Citrix Virtual Desktops deployments

If Profile Management has not been configured correctly on the images before they are rolled out, the Profile Management Service starts before Group Policy is applied. To avoid this, perform the configuration using the documented procedures before you put the images into a production environment.

Important: Including and excluding folders that are shared by multiple users (for example, folders containing data that can be shared by multiple virtual desktops) is not supported.

Configure Profile Management in Personal vDisk deployments

If you use the Personal vDisk feature of Citrix Virtual Desktops, Citrix user profiles are stored on virtual desktops' personal vDisks by default, typically the P: drives. The profiles are not stored on users' C: drives. However, this is where Profile Management expects to find the profiles. So you must modify

© 1997–2026 Citrix Systems, Inc. All rights reserved.

the Registry on the master image while installing or upgrading the VDA. In addition, because you have freed up space on the Personal vDisk, it is also good practice to increase the default allocation of disk space for applications on the master image. For instructions on these modifications, see Managing Citrix Virtual Desktops documentation.

Do not delete the copy of a profile in the user store while a copy remains on the Personal vDisk. Doing so creates a Profile Management error, and causes a temporary profile to be used for logons to the virtual desktop. For more information, see Users Receive New or Temporary Profiles in Troubleshooting common issues.

Windows Apps - Microsoft Store

In Citrix Virtual Desktops environments, applications on the Microsoft Store (also known as UWP apps) are supported. To use Microsoft Store applications on a pooled machine (pooled-random, static, or RDS), open the Group Policy Management Editor and then configure the following settings at **Policies > Administrative Templates > Classic Administrative Templates (ADM) > Citrix > Profile Management > File System > Synchronization**:

- Enable Folders to mirror and then add `appdata\local\packages` to the list of folders to mirror
- Enable Files to synchronize and then add `!ctx_localappdata!\Microsoft\Windows\UsrClass.dat*` to the list of files to synchronize

Microsoft Store applications might not work if users access a dedicated desktop with a Personal vDisk (the recommended solution) when their profile was already created on another desktop.

Example Settings for Citrix Virtual Desktops

This topic lists Profile Management policy settings used in a typical Citrix Virtual Desktops deployment. Windows 7 virtual desktops are created with Citrix Provisioning™ Services and are shared by multiple users. In this example, the desktops, which are created from a pooled-random catalog and are deleted at logoff, are intended for use on static workstations (not mobile laptops) and personal vDisks are not used.

Where no policy is listed, no selection or entry was made in Group Policy, and the default setting applies.

Note the following:

- **Path to user store** - You can incorporate Profile Management variables into the path to the user store. This example uses !CTX_OSNAME! and !CTX_OSBITNESS!, which expand to Win7 and x86 respectively when the path is interpreted. The AD attribute #sAMAccountName# is also used to specify user names.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Delete locally cached profiles on logoff** - Disabling this policy is safe because the desktops do not include personal vDisks and get deleted when users log off. Preserving locally cached profiles is therefore unnecessary. (If the desktops were not discarded at logoff, enable this policy.)
- **Profile streaming** - Enabling this setting improves logon times in this deployment.
- **Active write back** - This policy is enabled because the pooled desktops in this deployment are only temporarily allocated to users. The users might therefore change their profile but might forget (or not bother) to close their desktop session. With this setting enabled, local file changes in the profile are mirrored in the user store before logoff.

Note: If you enable the Active write back policy, performing a significant number of file operations in a session - such as file creation, file copy, and file deletion –can cause high system I/O activity and result in temporary performance issues while Profile Management synchronizes the file changes to the user store.

- **Process logons of local administrators** - Enabling this setting is recommended for Citrix Virtual Desktops deployments, in which most users are local administrators.
- **Processed groups** - All domain users' profiles are managed by Profile Management.
- **Exclusion list - directories** (file system) and **Exclusion list** (registry) - These settings prevent the listed temporary or cached files, and the listed registry entries, from being processed. These files and entries are commonly stored in user profiles.
- **Directories to synchronize** and **Files to synchronize** - Knowledge of where users' application data is stored helped define these settings.

Important: Citrix Virtual Desktops deployments vary, so the Profile Management policy settings you decide on are probably different to those in this example. To plan your settings, follow the advice in Decide on a configuration.

Citrix/Profile Management

- Enable Profile Management

  Enabled

- Processed groups

  MyDomainName\Domain Users

- Path to user store

  \\MyServer.MyDomain\MyUserStore\#sAMAccountName#\!CTX_OSNAME!_!CTX_OSBITNESS!

- Active write back

  Enabled

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Process logons of local administrators

  Enabled

Citrix/Profile Management/Profile handling

- Delete locally cached profiles on logoff

  Disabled

Citrix/Profile Management/Advanced settings

- Process Internet cookie files on logoff

  Enabled

Citrix/Profile Management/File system

- Exclusion list - directories

  $Recycle.Bin

  AppData\Local\Microsoft\Windows\Temporary Internet Files

  AppData\Local\Microsoft\Outlook

  AppData\Local\Temp

  AppData\LocalLow

  AppData\Roaming\Microsoft\Windows\Start Menu

  AppData\Roaming\Sun\Java\Deployment\cache

  AppData\Roaming\Sun\Java\Deployment\log

  AppData\Roaming\Sun\Java\Deployment\tmp

Citrix/Profile Management/File system/Synchronization

- Directories to synchronize

  AppData\Microsoft\Windows\Start Menu\Programs\Dazzle Apps

- Folders to mirror

  AppData\Roaming\Microsoft\Windows\Cookies

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix/Profile Management/Streamed user profiles

- Profile streaming

  Enabled

Profile Management and VDI-in-a-Box

September 7, 2025

> **Important:**
>
> Citrix VDI-in-a-box reached End of Life (EOL) in 2018. You can still use Profile Management on desktops created with VDI-in-a-box, but technical support is no longer provided.

You can use Profile Management on desktops created with Citrix VDI-in-a-Box.

Use of this version of Profile Management with VDI-in-a-Box is subject to the Profile Management EULA. Subject to the terms in the EULA, you can also use Profile Management with Citrix Virtual Apps in a VDI-in-a-Box environment. For more information, see Profile Management and Citrix Virtual Apps.

Profile Management and UE-V

September 7, 2025

Profile Management 5.x and Microsoft User Experience Virtualization (UE-V) 2.0 can co-exist in the same environment. UE-V is useful when multiple profile versions are present (for example, Version 1 and Version 2 profiles). For this reason, do not use the cross-platform settings feature of Citrix Profile Management when UE-V is present. UE-V might be preferred over that feature because it supports more applications, synchronization during user sessions, and XML configuration and generation for applications.

When Profile Management co-exists with UE-V, no matter whether the cross-platform settings feature is enabled:

- Exclude the AppData\Local\Microsoft\UEV folder. Profile settings captured by UE-V then overwrite profile settings captured by Profile Management.
- Do not share profiles controlled by UE-V with those controlled by Profile Management alone. If you do, the "last write wins."In other words, the last component to synchronize the profile (UE-V or Profile Management) determines which data is saved, which can lead to data loss.

Note: UE-V requires the Microsoft Desktop Optimization Pack (MDOP).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Profile Management and Citrix Content Collaboration™

September 7, 2025

The information in this article applies to the use of Profile Management in Citrix Content Collaboration deployments. Some of it may also be useful for other internet-based file-sharing systems.

You can use Citrix Content Collaboration with Profile Management 4.1.2 and later. Citrix Content Collaboration is only supported in On-Demand mode.

Installation

If you use ShareFile 2.7, to avoid a compatibility issue install this version first before installing Profile Management. This installation dependency does not exist with ShareFile 2.6.

Exclusions

Citrix Content Collaboration stores configuration data locally in the **\AppData\Roaming\ShareFile** folder. For users with Citrix user profiles, this data must roam with the user profile so that the user-specific Citrix Content Collaboration configuration is persisted. Since this ShareFile folder is part of the profile, no Profile Management configuration is required. The configuration data roams by default.

However, user data that is managed by Citrix Content Collaboration is contained in the **ShareFile** folder that is in the root of the profile (%USERPROFILE%\ShareFile). This data must not roam with the profile because it is managed by, and synchronizes with, the Citrix Content Collaboration server. You must therefore add this folder as a Profile Management exclusion. For instructions on setting exclusions, see Include and exclude items.

Personal vDisks

If you create virtual desktops with Personal vDisks (using Citrix Virtual Desktops), configure Citrix Content Collaboration with the location of the user data on the vDisks. This ensures that file synchronization can take place between the desktops and the Citrix Content Collaboration server. By default, Personal vDisks are mapped as P: drives on the desktops so the data might be located in P:\Users\<user name>. In this case, you would set the location using the LocalSyncFolder policy in Citrix Content Collaboration.

Important: To prevent unnecessary synchronizations, which can adversely affect the performance of Profile Management and Personal vDisks, we recommend using the Folder-ID setting on folders

© 1997–2026 Citrix Systems, Inc. All rights reserved.

that contain large files unless they need to be synchronized on the virtual desktop. This is a ShareFile setting.

Profile Management and App-V

September 7, 2025

You can use Profile Management in the same environment as Microsoft Application Virtualization 5.x (App-V 5.x).

> **Note:**
>
> Profile Management supports only globally published App-V.

Exclude the following items using Profile Management exclusions:

- Profile Management\File system\Exclusion list\directories:
  - AppData\Local\Microsoft\AppV
  - AppData\Roaming\Microsoft\AppV\Client\Catalog
- Profile Management\registry\Exclusion list:
  - Software\Microsoft\AppV\Client\Integration
  - Software\Microsoft\AppV\Client\Publishing

For instructions on setting exclusions, see Include and exclude items.

If the **UserLogonRefresh** setting is enabled in App-V, disable the Profile streaming policy in Profile Management. This restriction is the result of an incompatibility of **UserLogonRefresh** with Profile streaming.

For an example of how to sequence an App-V application, see https://docs.microsoft.com/en-us/windows/application-management/app-v/appv-sequence-a-new-application.

For information on configuring third-party Profile Management solutions with App-V enabled, see https://docs.microsoft.com/en-us/microsoft-desktop-optimization-pack/appv-v5/performance-guidance-for-application-virtualization-50. Do not include Software\Classes on Microsoft Windows 10 systems.

Profile Management and Provisioning Services

September 7, 2025

© 1997–2026 Citrix Systems, Inc. All rights reserved.

This article contains advice on maintaining Citrix user profiles on virtual disks (vDisks) created with Citrix Provisioning Services. Before following this advice, understand how your vDisk configuration affects your Profile Management configuration as described in Persistent? Provisioned? Dedicated? Shared?

Supported modes

You can use Profile Management on vDisks running in standard image and private image modes but not difference disk image mode.

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

To prevent any non-essential, locally cached profiles being stored, ensure that these profiles are removed from vDisks running in standard image mode before taking the Master Target Device image. But do not remove the currently logged-on local administrator's profile. A good way of achieving this is as follows. During this procedure, error messages might appear.

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

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, take account of the fact that base images can be reset, which results in log files being deleted. You therefore must take some action 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 Citrix Virtual Desktops™ 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 is also not saved there.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

If the Provisioning Services write-cache is stored on the computer running Provisioning Services, this issue does not arise. And the log file is saved back to the user store.

If the write-cache is stored locally, in this procedure you might have to log on from the same device as the user. However, even this might fail if the write-cache is stored locally in RAM.

If the write cache is not on the computer running Provisioning Services, you might have to create a copy of the vDisk image. You assign it to the new virtual machine, and change the write-cache on the image so it is stored on that computer.

1. In Citrix Virtual Desktops, create a 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). 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 Citrix Virtual Desktops 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 are lost.

1. Map a drive to \\<vmhostname>\C$ and, before the user logs off the session, locate the log file. The log file is not 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 Knowledge Center article CTX115601.

Preconfigure Profile Management on provisioned images

September 7, 2025

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 likely capture some Group Policy settings in the registry while you set up the image. For example, it happens while it is in Private Image mode with Provisioning Services. The settings are still present when you deploy the image. For example, when you switch back to standard image mode with Provisioning Services. Ideally, you choose defaults that suit the state of the virtual machine when it starts running and your users requirements when they log on. At a minimum, you ensure that you have suitable defaults for those policies described in Persistent? Provisioned? Dedicated? Shared?

The defaults are used if `gpupdate` is not run before the Citrix Profile Management Service starts. So it is best to ensure that they are sensible defaults for most 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 you transfer the settings to the .adm or .admx file only once your testing proves successful.

1. If you use the .adm or .admx file, change the desired settings using the file in the appropriate GPO. If you use the .ini file, omit this step; you 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 might have set up), and run `gpupdate /force`. This step ensures that the registry is correctly configured.
5. If you use the .ini file, change the desired settings in the file.
6. Stop the Profile Management Service.
7. To avoid confusion with the new log files that are created, delete the old Profile Management log file and the configuration log file. These have file names that use the name of the old image. They are redundant because the updated image has new files (with the name of the new image).
8. Do one of the following:
    - Switch the image back to standard image mode (Citrix Provisioning Services).
    - Save the updated image (Citrix XenServer or VMware ESX).
9. Start the operating system on the image.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Profile Management and Self-service Plug-in

September 7, 2025

By default, Profile Management excludes the Windows **Start Menu** folder. Citrix Self-service Plug-in users cannot see their subscribed applications in the **Start Menu**. Adjust this default behavior by removing the folder %APPDATA%\Microsoft\Windows\Start Menu from the **Exclusion list - directories** policy. In addition, when using GPOs for configuration, it is a best practice to delete the Profile Management .ini file. These actions ensure that the **Start Menu** folder containing subscribed applications (and any user-created subfolders) are processed by Profile Management.

Note: If you are using the Profile Management .ini file rather than Group Policy, remove this entry from the default exclusion list in that file.

Profile Management and VMware

September 7, 2025

> **Note:**
>
> This article applies only to Windows XP and Windows 7.

This article 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 Citrix Virtual Desktops™ or Citrix Virtual Apps deployment) 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 thus 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 might 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
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

`Settings\Application Data\VMware> failed with: The directory is not empty.`

To work around this issue in a Citrix Virtual Apps™ deployment on Windows Server 2008:

1. Log on as Administrator to the Citrix Virtual Apps server.
2. In Citrix Virtual Apps deployments, log off all users from the server.
3. In the 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. Under **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.

Profile Management and Outlook

September 7, 2025

This article describes best practices for integrating Microsoft Outlook with roaming profiles.

It is a 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, except for one folder, `%UserProfile%`\Local Settings. This exception affects Outlook users because a Microsoft recommendation means that, by default, some Outlook data (for example, `.ost`, `.pst`, and `.pab` files) is created in this non-roaming folder.

Important: Files in this location are typically large and hinder the performance of roaming profiles.

The following practices can reduce troubleshooting of roaming profiles with Outlook and encourage good email management by users and administrators:

- If possible, use an ADM template for Microsoft Office that prohibits the use of `.pst` files.
- If users need more space, increase storage on your Microsoft Exchange servers rather than a network share.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 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 must 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. The **Enable search index roaming for Outlook** feature is not designed for `.pst` files.

Using Windows profiles with Password Manager and single sign-on

September 7, 2025

This article does not contain any information specific to Profile Management. It tells you how to configure certain Windows options so that Citrix Single Sign-on operates optimally with local profiles, roaming profiles, mandatory profiles, or hybrid profiles. This topic applies to Citrix Single Sign-on 4.8 or 5.0.

Local profiles

Local profiles are stored on the local server to which the user has logged on. Password Manager and single sign-on save registry information in the `HKEY_CURRENT_USER\SOFTWARE\Citrix\MetaFrame Password Manager` hive of the User Registry at:

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

Files are also saved in:

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

On Windows 7, single sign-on uses:

%APPDATA%\Roaming\Citrix\MetaFrame Password Manager

Important: It is critical that single sign-on has Full Control Access to the following files:

File Name	Description
%username%.mmf	User's credential information file with pointers to aelist.ini.
entlist.ini	Application definition file created at enterprise level in the synchronization point or Active Directory.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

File Name	Description
aelist.ini	Application definition file created by merging the 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) might become corrupted.
- When roaming profiles are used with multiple concurrent sessions, they share the back-end MMF. All active sessions share some common session data such as retry lock counters, last used data counters, and event log entries.

Mandatory or hybrid profiles

Mandatory profiles are by definition user read-only profiles. Single sign-on needs write permission to the profile folder under **Application Data**. With mandatory profiles, a user might make changes but the changes are not saved back to the profile at logoff. For single sign-on to work correctly with mandatory profiles, the **Application Data** folder must be redirected.

The registry changes are written each time the user logs on. Credential information is synchronized with the synchronization point but the changes are not saved back to the profile.

Beginning with Windows 2000, Microsoft provides a mechanism for redirecting the **Application Data** folder. However, using Windows NT4 domains requires logon scripts capable of modifying the location of the **Application Data** folder. You can achieve this using tools such as `Kix` or `VBScript` to define a writeable location for the **Application Data** folder.

The following example uses `Kix` to redirect the **Application Data** folder during user logon:

Important: This sample script is for informational purposes only. Do not use it in your environment before first testing it.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

“‘ pre codeblock

```
$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`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

`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 single sign-on. In Windows 2000, you must reference the share that stores application data using the `%username%` variable (for example \\servername\sharename\%username%).

Folder redirection is global for the user and it affects all of their applications. 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 approach 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.

Firefox browser

September 28, 2021

© 1997–2026 Citrix Systems, Inc. All rights reserved.

For a seamless user experience, Profile Management synchronizes each user's entire profile between the system it is installed on and the user store. As a result, Firefox users might experience slow logons or logoffs. The issue occurs because some files associated with Firefox can grow large.

We recommend you customize a logoff script to delete the following files and folders and thus to exclude them from synchronization:

- Appdata\Roaming\Mozilla\Firefox\profiles*\sessionstore.bak
- AppData\Roaming\Mozilla\Firefox\Profiles*\sessionstore-backups

The general workflow is as follows:

1. Write the logoff script using the Windows PowerShell or any other languages supported by the user computers. You can also use Windows Script Host (WSH)–supported languages and command files, including VBScript and Jscript.
2. Copy the script to the **Netlogon** shared folder on the domain controller.
3. In the **Group Policy Management Console**, associate the script to the user logoff event. For more information, see the Microsoft article.

Google Chrome browser

September 9, 2025

To provide a seamless user experience, Profile Management synchronizes each user's entire profile between the system it is installed on and the user store. As a result, Google Chrome users might experience slow logons or logoffs. This issue occurs because some files associated with Google Chrome can grow large.

To improve the user experience with Google Chrome, follow the steps below.

1. Add the following folder to the list of folders to mirror:
    - AppData\Local\Google\Chrome\User Data\Default
2. Exclude the following folders from synchronizing:
    - Appdata\Local\Google\Chrome\User Data\Default\Cache
    - Appdata\Local\Google\Chrome\User Data\Default\JumpListIconsMostVisited
    - Appdata\Local\Google\Chrome\User Data\Default\JumpListIconsRecentClosed
    - AppData\Local\Google\Chrome\User Data\Default\Media Cache
3. Exclude the following files from synchronizing:
    - AppData\Local\Google\Chrome\User Data\Default\Favicons

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- AppData\Local\Google\Chrome\User Data\Default\History
- The files unrelated to bookmarks in the `AppData\Local\Google\Chrome\User Data\Default` folder

We recommend that you use the Profile streaming feature if you experience slow logons or logoffs. For more information, see Stream user profiles.

Secure

September 7, 2025

This topic contains recommended best practice for securing Profile Management. In general, secure the servers on which the user store is located to prevent unwanted access to Citrix® user profile data.

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

Permissions

Citrix tests and recommends the following permissions for the user store and the cross-platform settings store:

- Share Permissions: Full control of the user store root folder
- The following NTFS permissions, as currently recommended by Microsoft:

Group or User Name	Permission	Apply To
Creator Owner	Full Control	Subfolders and files only
The group of accounts under Profile Management control	List Folder / Read Data and Create Folders / Append Data	This folder only
Local System	Full Control	This folder, subfolders, and files

Assuming inheritance is not disabled, these permissions allow the accounts to access the stores. And allow the accounts to create subfolders for users'profiles and perform the necessary read and write operations.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Beyond this minimum, you can also simplify administration by creating a group of administrators with full control of subfolders and files only. Then deleting profiles (a common troubleshooting task) becomes easier for members of that group.

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

Access control list (ACL)

If you use the cross-platform settings feature, set ACLs on the folder that stores the definition files as follows: read access for authenticated users, and read-write access for administrators.

Windows roaming profiles automatically removes administrator privileges from the folders containing profile data on the network. Profile Management does not automatically remove these privileges from folders in the user store. Depending on your organization's security policies, you can do so manually.

Note: If an application modifies the ACL of a file in the user's profile, Profile Management does not replicate those changes in the user store. It is consistent with the behavior of Windows roaming profiles.

Profile streaming and enterprise antivirus products

The streamed user profiles feature of Citrix Profile Management uses advanced NTFS features to simulate the presence of files missing from users' profiles. In that respect, the feature is similar to a class of products known as Hierarchical Storage Managers (HSMs). HSMs 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, configure antivirus products to be aware of HSM drivers, and the streamed user profiles driver is no different. 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 written with the possibility of sophisticated storage products, such as HSMs, in mind. And they can be configured to delay their scanning until the HSM has done its work. Home antivirus products are 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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**. 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**. Configures the antivirus product to scan only a file when data is accessed (for example, when a file is executed or created). Other types of file access (for example, when a file is opened or its status checked) are ignored by the antivirus product. HSMs generally activate in response to file-open and file-status-check operations, so disabling virus scans on these operations eliminates potential conflicts.

Citrix tests streamed user profiles with versions of the leading enterprise antivirus products to ensure that they are compatible with Profile Management. These versions include:

- McAfee Virus Scan Enterprise 8.7
- Symantec Endpoint Protection 11.0
- Trend Micro OfficeScan 10

Earlier versions of these products are not tested.

If you are using an enterprise antivirus product from other vendors, ensure that it is HSM-aware. It can be configured to allow HSM operations to complete before performing scans.

Some antivirus products allow administrators to choose to scan-on-read or scan-on-write. This choice balances performance against security. The streamed user profiles feature is unaffected by the choice.

Troubleshoot Profile Management in streaming and antivirus deployments

If you encounter issues, such as logons hanging or taking a long time, there might 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 might 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 might 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 it works, re-enable the feature and disable your enterprise antivirus product. If it also works, gather Profile Management diagnostics for the non-working case and contact Citrix Technical Support. They need to know the exact version of enterprise antivirus product.

To continue using Profile Management, do not forget to re-enable the enterprise antivirus and turn off streamed user profiles. Other features of Profile Management continue to function in this configuration. Only the streaming of profiles is disabled.

Troubleshoot

April 24, 2026

This section provides guidance on how to troubleshoot Profile Management.

The general troubleshooting workflow is as follows:

1. Check Profile Management settings.
2. Check Profile Management log file.
3. Check Windows events logged by Profile Management.
4. Troubleshoot common issues.
5. Perform advanced troubleshooting.
6. If you can't resolve the issues after trying the preceding procedures, collect as much diagnostic information as possible and contact Citrix Technical Support.

Check Profile Management settings

April 27, 2026

As a first step in troubleshooting an issue, check the current Profile Management settings as follows:

1. Start troubleshooting in Citrix Director. This console displays properties of profiles that can help you diagnose and correct problems.
2. Use the UPMConfigCheck tool to examine a live Profile Management deployment and determine whether it's optimally configured.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

For more information about installing and using this tool, see Knowledge Center article CTX132805.

3. If a Profile Management .ini file is in use, check its configuration on the affected machine.
4. To deactivate any Profile Management policy that you enter as lists (for example, exclusion lists and inclusion lists), set the policy to Disabled. Do not set the policy to Not Configured.
5. Check the `HKEY_LOCAL_MACHINE\SOFTWARE\Policies` registry entry on the affected machine. If there are any stale policies because of GP tattooing issues, delete them. Tattooing occurs when policies are deleted from GP but remain in the registry.
6. Check the UPMSettings.ini file, which contains the Profile Management settings that have been applied for each user. This file is present in the root folder of each Citrix user profile in the user store.

Check Profile Management log files

September 7, 2025

Log files are useful when troubleshooting system behaviors. After checking Profile Management settings, enable Profile Management logging and reproduce the issue to check the log files.

Detailed steps are as follows:

1. Enable Profile Management logging for all events and actions.
2. Reproduce the issue on the machine.
3. Check the Profile Management log file (for example, #computername#.#domainname#_pm.log) in the `%SystemRoot%\system32\LogFiles\UserProfileManager` folder for errors and warnings. Locate them by searching for the word ERROR or WARNINGS respectively.

   For more information about log files, see Reference, later in this article.
4. Check that the path to the user store is correct.
5. Check that all information from Active Directory was read correctly.
6. Check the time stamps to see whether there's an action that takes too long.

> **Tip:**
>
> You can use Microsoft Excel to review Profile Management log files. For more information, see Knowledge Center article CTX200674.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Enable Profile Management logging

Enable Profile Management logging for all events and actions only when troubleshooting an issue in your Profile Management deployment. When you have the issue resolved, disable logging and delete the log files because they might include sensitive information.

This section guides you through using GPOs and `UPMPolicyDefaults_all.ini` to enable logging for all events and actions.

You can also achieve this goal using Citrix Studio and Workspace Environment Management (WEM). For more information, see Decide on where to configure Profile Management.

Enable logging using GPOs

To enable Profile Management logging for all events and actions using a GPO, follow these steps:

1. Open the Group Policy Management Editor, and then create a Group Policy Object.
2. Access **Policies > Administrative Templates: Policy definitions (ADMX files) > Citrix Components > Profile Management > Log settings**.
3. Enable Profile Management logging as follows:
    a) Double-click **Enable logging**.
    b) Click **Enabled**.
    c) Click **OK**.
4. Enable Profile Management to log all events and actions:
    a) Double-click **Log settings**.
    b) Select all events and actions. For more information about their descriptions, see Events and actions.
    c) Click **OK**.
5. To change the default maximum size of the log file, follow these steps:
    a) Double-click **Maximum size of the log file**.
    b) Click **Enable**, and then enter a size in the **Maximum size in bytes** field.
    c) Click **OK**.

> **Tip:**
>
> When the maximum size is reached, Profile Management retains one backup file (for example, Logfilename.log.bak).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

6. Run the `gpupdate /force` command on the machine.

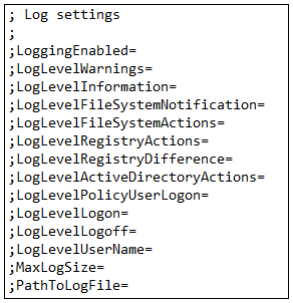
   These policies take effect on the machine.

For more information about these policies, see Profile Management policy descriptions and defaults.

Enable logging using the .ini file

To enable Profile Management logging for all events and actions using `UPMPolicyDefaults_all.ini`, follow these steps:

1. Open `UPMPolicyDefaults_all.ini` in the Profile Management installation folder (by default, C:\Program Files\Citrix\User Profile Manager).
2. Search for **Log settings** to locate the settings.



```
; Log settings
;
;LoggingEnabled=
;LogLevelWarnings=
;LogLevelInformation=
;LogLevelFileSystemNotification=
;LogLevelFileSystemActions=
;LogLevelRegistryActions=
;LogLevelRegistryDifference=
;LogLevelActiveDirectoryActions=
;LogLevelPolicyUserLogon=
;LogLevelLogon=
;LogLevelLogoff=
;LogLevelUserName=
;MaxLogSize=
;PathToLogFile=
```

3. Enter 1 for `LoggingEnabled`.
4. Enter 1 for each parameter from `LogLevelWarnings` through `LogLevelUserName`. For more information about those parameters, see Events and actions.
5. To change the default maximum size for the log file, enter a size for `MaxLogSize` as needed.
6. To change the default folder for the log file, enter a path for `PathToLogFile` as needed.

Reference

This section provides the following information:

- Log types
- Events and actions
- Fields in the Profile Management log file

Log types

This table lists logs that you can use to troubleshoot Profile Management.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Informal Name	Log File Name	Location	Type of Log Information
Profile Management log file	#computername#.#domainname#_pm.log	%SystemRoot%\system32\Logfiles\UserProfileManager	If logging is enabled, messages, warnings, and errors, are written to the Profile Management log file. The domain name is the computer's domain. If the computer name cannot be determined, this log file is called UserProfileManager.log. If the domain cannot be determined while the computer name is available, the log file is called #computername#_pm.log.
Profile Management configuration log file	#computername#.#domainname#_pm_config.log	%SystemRoot%\system32\Logfiles\UserProfileManager	This file captures the GPO and .ini file settings even if logging is turned off. If the computer name cannot be determined it is called UserProfileManager_pm_config. If the domain cannot be determined while the computer name is available, the log file is called #computername#_pm_config.log.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Informal Name	Log File Name	Location	Type of Log Information
Windows event log	Application.evtx	%SystemRoot%\System32\winevt\Logs	The Windows event log, which you view with the Microsoft Event Viewer, is used primarily for error reporting. Only errors are written to it.

Events and actions

This table lists events and actions that Profile Management can log.

Type	Description	Parameter in .ini
Common warnings	All common warnings.	LogLevelWarnings
Common information	All common information.	LogLevelInformation
File system notifications	One log entry is created each time a processed file or folder is changed.	LogLevelFileSystemNotification
File system actions	File system operations performed by Profile Management.	LogLevelFileSystemActions
Registry actions	Registry actions performed by Profile Management.	LogLevelRegistryActions
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.	LogLevelRegistryDifference
Active Directory actions	Each time Profile Management queries the Active Directory, an entry is written to the log file.	LogLevelActiveDirectoryActions
Policy values	When the Profile Management service starts or a policy refresh occurs, policy values are written to the log file.	LogLevelPolicyUserLogon

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Type	Description	Parameter in .ini
Logon	The series of actions during logon are written to the log file.	LogLevelLogon
Logoff	The series of actions during logoff are written to the log file.	LogLevelLogoff
Personalized user information	Where applicable, user and domain names are logged to dedicated columns of the log file.	LogLevelUserName

Log file fields

Each line in the Profile Management log file has several fields, separated by semicolons. This table lists the log file fields.

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 running at the time, and the log message

Check Windows events

September 7, 2025

Windows events logged by Profile Management also provide diagnostic information for troubleshooting. Windows events are stored in the Application.evtx file under the `%SystemRoot%\System32\winevt\Logs\` folder.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

To view the events using Windows Event Viewer, follow these steps:

1. Start **Event Viewer** on the Windows machine.
2. Select the **Windows Logs > Application** node in the left pane.

   The events appear in the right pane.

List of events

Events logged by Profile Management are not all sequentially numbered and not all are used in this version of Profile Management. However, they might be logged if you upgrade from an earlier version.

Event ID	Description	Cause	Action
6	The Citrix Profile Management service has started.	The Citrix Profile Management service has started. It might 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 might 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Event ID	Description	Cause	Action
8	The profile for user 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 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 that the installation path contains no spaces, or the 8.3 file name 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 file name support on the volume where Profile Management is installed.
10	User 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Event ID	Description	Cause	Action
12	StartMonitoringProfile: A problem was detected in the Windows change journal management during logon…	The Citrix Profile Management Service was unable to monitor the profile or a folder configured for extended synchronization. A problem was detected in the Windows change journal event management, preventing the Service from monitoring changes. Citrix Profile Management does not process this folder. A Windows user profile is used instead.	Ensure that change journal processing is configured and operational for all volumes managed by Profile Management. Ensure that the computer has adequate system resources. Check the event log for errors and take any corrective action indicated, including Profile Management troubleshooting procedures.
13	StopMonitoringProfile: A problem was detected in the Windows change journal management during logoff…	The Citrix Profile Management Service was unable to stop monitoring the profile or a folder configured for extended synchronization. A problem was detected in the Windows change journal management, preventing the Service from monitoring changes. Citrix Profile Management does not process this folder. File and registry changes are not synchronized for the user.	Ensure that change journal processing is configured and operational for all volumes managed by Profile Management. Ensure that the computer has adequate system resources. Check the event log for errors and take any corrective action indicated, including Profile Management troubleshooting procedures.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Event ID	Description	Cause	Action
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 does not process this folder. A Windows user profile is 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 does not process this folder. A Windows user profile is 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Event ID	Description	Cause	Action
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 does not process this folder. A Windows user profile is 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Event ID	Description	Cause	Action
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 processes this directory as normal.	Although this error does not prevent the operation of Profile Management, check for errors anyway. Make sure that change journal processing is configured and operational for all volumes managed by Profile Management. Make sure that the computer has adequate system resources. Check the event log for errors and take any corrective action indicated, including Profile Management troubleshooting procedures.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Event ID	Description	Cause	Action
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 does not complete processing on this folder. Back up critical data manually.	The Citrix Profile Management Service was unable to monitor the profile or a folder configured for extended synchronization. A problem was detected in the Windows change journal event management, preventing the Service from monitoring changes. Citrix Profile Management does not process this folder. A Windows user profile is used instead.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Event ID	Description	Cause	Action
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 does not complete processing on this directory. Back up critical data manually.	The Citrix Profile Management Service was unable to monitor the profile or a folder configured for extended synchronization. A problem was detected in the Windows change journal event management, preventing the Service from monitoring changes. Citrix Profile Management does not process this folder. A Windows user profile is used instead.
20	CADUser::Init: Determining the DNS domain and ADsPath failed…	A problem occurred while querying Active Directory for information about the logged-on user. Citrix Profile Management does not process this folder. A Windows user profile is 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Event ID	Description	Cause	Action
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 experienced a delay while file 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 error might result from 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 might be denied. The user experienced a long delay while a file 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 might be denied. The user received an error message. This error might result from 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Event ID	Description	Cause	Action
24	RevertToSelf failed with error code 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 failed to be called. So, for security reasons, the Profile Management software was shut down. The user received an error message.	If you suspect a security breach, follow your organization's procedures to address it, and then restart Profile Management.
25	The profile for user is managed by Citrix Profile Management, but the user store cannot be reached…	The Citrix Profile Management Service on this computer cannot reach the specified user store. This is normally because of a network issue or because the server hosting the user store is unavailable.	Ensure the server hosting the user store is available and the network between this computer and the server is operational.
26	The default profile location is invalid. Profiles in this location cannot be monitored correctly…	Profiles on this computer must be on a disk mounted on a drive letter (for example, C:).	Move the profiles on this computer to a disk mounted on a drive letter, and restart Profile Management.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Event ID	Description	Cause	Action
27	The profile folder for the user is not present under the default profile location …	In the registry, the location of this user's profile and of the default profile do not match. This can occur, for example, if profiles are moved between different volumes on the machine running the Profile Management Service.	Ensure that this user's profile is located under the default folder location. Use appropriate tools if necessary so that the profile data in the file system matches the profile's registry settings.
28	An error occurred while trying to reset security permissions on the registry hive for user.	It is likely that there are permission issues with the registry in the default or template profile used to create this Citrix user profile.	If appropriate, reset the security permissions on the user's registry hive in the Profile Management user store using a third-party utility such as SetAcl.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Event ID	Description	Cause	Action
29	A template profile path is configured but no profile was found…	The specified folder cannot be used in the template profile setting because it does not contain the file NTUSER.DAT. This issue commonly occurs when the full path of the NTUSER.DAT file is configured instead of the folder containing NTUSER.DAT. The template profile setting does not support the expansion of Active Directory attributes, system environment variables, or the %USERNAME% and %USERDOMAIN% variables.	Check that you have configured a valid path to the folder containing the template profile. Check that the path contains NTUSER.DAT. Make sure that this file is valid, and that access rights are set correctly on the folder to allow read access to all files.
33	Citrix Profile Management created a profile in the user store from a local profile at LOCATION	A profile was created in the user store from the location indicated.	None. This message is for information only.
34	Citrix Profile Management created a profile in the user store from a roaming profile at LOCATION	A profile was created in the user store from the location indicated.	None. This message is for information only.
35	Citrix Profile Management created a profile in the user store from a template profile at LOCATION	A profile was created in the user store from the location indicated.	None. This message is for information only

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Event ID	Description	Cause	Action
36	The existing profile folder for USER cannot be prepared for this user's new Citrix mandatory profile. The user is given a temporary profile if possible.	Citrix mandatory profiles use copies of a template profile for each logon. Any existing profiles are deleted and the Citrix mandatory profiles are copied from the specified template location. This process failed.	Delete any existing profile folder manually. You might have to restart the computer if files are locked by another process that causes the deletion to fail. Ensure that the template folder exists and the user has permissions to read its contents.
37	The user store path for user cannot be reached. A temporary profile is created for this user and no changes are saved to their profile in this user store.	The Citrix Profile Management Service on this computer cannot reach the specified user store. This is normally because of a network issue or because the server hosting the user store is unavailable.	Ensure the server hosting the user store is available and the network between this computer and the server is operational.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Event ID	Description	Cause	Action
38	The profile for user is managed by Citrix Profile Management, but the user store path cannot be found. A temporary profile is created for this user and no changes are saved to their profile in this user store.	The Citrix Profile Management Service on this computer cannot find the profile in the specified user store. This might be because of a network issue or because the server hosting the user store is unavailable. But it might also be because the profile in the user store has been deleted or moved. Or the path to the user store has changed and no longer correctly points to an existing profile in the user store.	Ensure that the server hosting the user store is available. And the network between this computer and the server is operational and the path to the user store points to an existing profile. If the profile in the user store has been deleted, delete the profile on the local machine.
42	An error occurred while trying to update policy settings for user <userdomain>\<username>. Policy settings might not have been applied correctly. Error code:<error code>	Citrix Profile Management failed to update Citrix group policy settings.	Verify that Citrix Group Policy Client-Side Extension is installed and works properly.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Event ID	Description	Cause	Action
3005	Attempts to mount the virtual disk from <path1> to access point <path2> fail.	Citrix Profile Management failed to mount virtual disk to the access point. This issue might occur when the virtual disk is not accessible, the access point is not empty, or the virtual disk is already mounted.	Restart the machine and check whether the issue is resolved. If not, collect CDF trace and contact Citrix Technical Support.
3008	Attempts to mount the search database from <path1> to access point <path2> fail.	Windows Search service failed to mount the search database. This issue might occur when the search database is corrupted.	Collect CDF trace and contact Citrix Technical Support.

Troubleshoot common issues

September 7, 2025

This article describes how to troubleshoot common Profile Management issues.

Slow logons

If your users encounter slow logons, follow these steps to troubleshoot:

1. Check the profile load time in the Logon Duration panel of Citrix Director. If it's substantially longer than expected, the slow logon is caused by loading user profiles.

   See Diagnose user logon issues for details.

2. Check the profile processing time in the Citrix Profile Management log file.

   In the Profile Management log file at `C:\Windows\System32\Log Files\User Profile Manager`, locate the entry starting with `DispatchLogonLogoff`. The following example shows that the logon processing time is 10.22 seconds.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
DispatchLogonLogoff: ---------- Finished logon processing successfully
 in [s]: <10.22>.
```

3. Contact Citrix Technical Support.

   If slow logons persist, contact Citrix Technical Support for further assistance. For more information, see Contact Citrix Technical Support.

Check 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, do the following:

1. Check the following type of entry in the Profile Management log file:

   ```
   pre codeblock 2010-03-16;16:16:35.369;INFORMATION;;;;1140;ReadPolicy
   : Configuration value read from policy: PSEnabled=<1>
   ```

   The last item must be set to PSEnabled=<1> if the feature is enabled.

2. Check the following entry for the user in the Profile Management log file:

   ```
   pre codeblock 2010-03-16;20:17:30.401;INFORMATION;<domain name
   >;<user name>;2;2364;ProcessLogon: User logging on with Streamed
   Profile support enabled.
   ```

   If streamed user profiles aren't being applied, the item reads ProcessLogon: User logging on with Streamed Profile support disabled.

Determine which policies are in force

Use the UPMSettings.ini file to determine the Profile Management policies that are being applied. This file is present in the root folder of each Citrix user profile in the user store. Examining this file might be more convenient than using the Resultant Set of Policy (RSoP). Doing so especially if you use a mixture of GPOs and .ini file settings to determine policies.

Use the UPMFRSettings.ini file to determine which profile folders aren't processed because they are on an exclusion list. The UPMFRSettings.ini file is also present in the root folder.

Exclude corrupt profile data

If a user profile is corrupt and you're confident the problem lies with a particular file or folder, exclude it from the synchronization process. The way is to add the file or folder to the exclusion list.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Clean 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 preservation can result in slow logoffs or incomplete termination of user sessions. The User Profile Hive Cleanup (UPHClean) tool from Microsoft can help resolve these scenarios.

Delete local profiles

Microsoft Delprof.exe and Sepago Delprof2 are tools that help you delete user profiles.

Delete 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.

Identify where profiles are stored

Diagnosing profile issues can involve locating where the files in a user's profiles are stored. The following procedure provides a quick way to identify where profiles are stored.

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.

Check 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 present in the profile's root folder. The last entry in the file is the name of the server from which the user last logged off. For example, if the server runs Profile Management 5.0, the entry would be:

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Roll back

To roll back to earlier versions of Profile Management, run **del /s** from the command line on the file server that hosts the user store. The command deletes the PmCompatibility.ini file from each profile. For example, if the local path to the user store is D:\UpmProfiles, run:

```
del /s D:\UpmProfiles\pmcompatibility.ini
```

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

Excluded folders in user store

Excluded folders appear in the user store. This issue 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've selected all check boxes for the events you want to log.

Tip: You might have to scroll down to enable the last check boxes on the list.

GPO settings inoperative

You change a GPO setting but it isn't operative on the computer running the Citrix Profile Management Service. The issue occurs because GP does not refresh immediately but instead is based on events or intervals specified in your deployment. To refresh GP immediately, run `gpupdate /force` on the computer.

For your changes to take effect, run the `gpupdate /force` command from the command prompt as documented at https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/gpupdate.

Users receive new or temporary profiles

By default, users are given a temporary profile when a problem occurred. For example, the user store is unavailable. Alternatively, you can configure Profile Management to display an error message and then log users off. This approach can help with troubleshooting.

For instructions on configuring this feature, see Force user logoffs.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

In some circumstances, when they log on, users receive a new profile instead of their cached profile.

Users might also receive a temporary profile if a local profile is present after the copy in the user store is removed. This situation can arise if the user store is cleared but local profiles are not deleted at logoff.

Profile Management treats such partial removal of profiles as a network, share, or permissions error, and provides the user with a temporary profile. For this reason, partial removal isn't recommended. To work around this issue, log on to the affected computer and delete the profile manually.

If your deployment includes personal vDisks, users might receive temporary profiles if the default processing of these disks hasn't been correctly adjusted. For more information, see Migrate user profiles.

Profile data lost when virtual desktop sessions become unresponsive

In a Citrix virtual desktops deployment, disconnecting from a Remote Desktop Protocol (RDP) session can cause a virtual desktop to become unresponsive or to restart. The behavior impacts Profile Management because it causes profile data to be lost when the session ends. The issue is fixed in Citrix Virtual Delivery 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 error appears in Windows Application Event Logs (Event ID: 1000, Source: Userenv).

Printing

In Citrix virtual desktops™ environments, a user can select a default printer but sometimes the selection isn't retained between logons. This issue has been observed when a Citrix virtual desktop's policy is used to set printers on pooled virtual desktops based on a Citrix Provisioning Services Personal vDisk in standard image mode.

This issue does not originate with Profile Management. Though the Profile Management log file shows that the registry entry for the printer is copied at logoff (which is expected), NTUSER.dat for the user doesn't contain the entry (which isn't expected). The issue in fact originates with the way Citrix virtual desktops uses the `DefaultPmFlags` registry setting.

Sometimes, unexpected printers are added to profiles. After users remove them, the printers reappear at the next logon. See the Profile Management support forum for more information.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Problems with application settings on multiple platforms

You might experience problems where application settings don't roam correctly across multiple platforms. Typically these problems result from:

- Settings that aren't applicable from one system to another. For example, hardware-specific settings that are not on every system.
- Applications that are installed differently on different systems. Examples:
  - An application that is installed on a C: drive on one system but on a D: drive on another.
  - An application that is installed in C:\Program Files on one system but in C:\Program Files (x86) on another.
  - An Excel add-in installed on one system but not on another.
- Applications that don't store setting information in 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, better standardization of the systems that cause these issues can minimize the issues. However, often the issues result from inherent incompatibilities (with multiple platforms) of the OS or the respective application. If the problematic settings aren't critical, excluding them from the profile might resolve the issue.

Profiles owned by unknown accounts

On rare occasions, a profile can appear to belong to an unknown account. On the **Advanced** tab of the **System Properties** dialog box for a computer, Account Unknown is displayed when you click **Settings** in User Profiles. This issue comes along with an event log entry, *"Profile notification of event Create for component <application ID> failed, error code is???"* In the registry, the application ID points to the SHACCT Profile Notification Handler, a Microsoft component.

To confirm that this issue occurs in your environment, log on as a user whose data Profile Management doesn't process, and check for these symptoms.

It isn't an issue with Profile Management but might be the result of Active Directory interacting badly with virtual machine snapshots. The operation of Citrix user profiles is unaffected. Users can log on and off, and their profile changes are preserved.

Perform advanced troubleshooting

September 7, 2025

© 1997–2026 Citrix Systems, Inc. All rights reserved.

After you check the current Profile Management settings and eliminate the Profile Management logs as sources of useful information, use this checklist to troubleshoot further.

- Check the Resultant Set of Policies (RSoP) report from the machine you're analyzing and ensure all GPOs are applied as expected.

  To generate the report, run the `gpresult` command on the machine.
- Check that you have the latest version of Profile Management installed. For more information, see Check the Profile Management version
- Check the Profile Management support forum for solutions from other users.
- Try to reproduce the issue on a clean machine with the same operating system as the affected machine. Install the software products one by one, and see if you can reproduce the issue after each installation. For more information, see Deploy Profile Management in a test environment.

Check the Profile Management version

To examine the version information, follow these steps:

1. Right-click the UserProfileManager.exe file in Windows Explorer.
2. Click **Properties > Version**.
3. If it's not the latest version, download the latest version from the My Account site. Select your Citrix® product and download Profile Management from the Downloads section.

> **Tip:**
>
> After upgrading, you can enable any later feature if needed.

Deploy Profile Management in a test environment

If logging files can't help with troubleshooting the issue, try the troubleshooting approach used in the following example. You can use this approach to:

- Determine which configuration settings are being read.
- Determine where configuration settings are being read from (when multiple ADM files are present).
- Check that the log file correctly tracks changes made to profiles.

Deployment example

Deployment in this example is as follows:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Citrix virtual apps™ servers are running on Windows Server 2003.
- Users are connecting to their published resources using the Plug-in for Hosted Apps for Windows.
- OU-based GPOs are used instead of the INI file-based configuration.

> **Caution:**
>
> Editing the registry incorrectly can cause serious problems that might require you to reinstall the operating system. We cannot guarantee that problems resulting from improper 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.

Troubleshooting workflow

This example includes a small test OU that comprises only one server. You can edit the profile settings of the server. Then track setting changes in the log file and in the Resultant Set of Policies (RSoP) report.

Detailed steps are as follows:

1. From the production environment, remove one of the Citrix virtual apps servers that host the Citrix user profiles. Next, add the server to a new OU.
2. Remove and reinstall Profile Management on the server. When reinstalling, check that short file names (also known as 8.3 file names) are activated as 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. Doing so enables support for short file names.
   - If the entry isn't set to 1, reinstall Profile Management to a location where each subfolder name is eight characters or less, for example, c:\prof-man.
     For later operating systems, you do not need to adjust this registry entry.
3. Log on as a domain administrator to the server.
4. Examine the local policy and remove the ADM file at this level.
5. Delete any links to GPOs assigned to your new OU.
6. On the server, delete the key and all subkeys from Registry Editor: `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\UserProfileManager\`.
7. Remove any Profile Management .ini file.
8. Using **My Computer > Properties > Advanced**, delete all profiles except those profiles that you want to test. Research any errors that appear.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

9. Grant the Authenticated Users group full control of the file. Doing so enables you to check the Profile Management log file when logging on as a user. The log file is C:\Windows\System32\LogFiles\UserProfileManager\<domainname>#<computername>_pm.log (where <domainname> is the computer's domain and<computername> is its name). If the domain cannot be determined, the log file is UserProfileManager.log.
10. Create a GPO that contains only the following settings, and then link it to your new OU. Make sure that the GPO is assigned to the Authenticated Users group. Enabled and configure these settings:

    a) Enable Profile Management.
    b) Path to user store.
    c) Enable logging.
    d) Log settings. Select all events and actions.
    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.
    h) Disable the *Process logons of local administrators* setting. By doing so, even if Profile Management is misconfigured and prevents user logons, you can still 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 domain test user who has never logged on and isn't a member of any local administrator group on the server.
13. Publish a full desktop to this user and make sure that the user is in the Remote Desktop Users group.
14. If the domain has multiple domain controllers (DCs), force AD replication between all 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 `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\UserProfileManager\` are the ones for your new GPO.
17. Log out as Administrator.
18. Make some setting changes to Internet Explorer, and create a blank test file in your My Docs folder.
19. Create a shortcut to the Profile Management log file. Open it and examine the entries. Research any items that require attention.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

20. Log out and then back in as domain Administrator.
21. Generate a RSoP report for the test user and the server by running `gpresult`.

If the report doesn't include what you expect, research any items that require attention.

Contact Citrix Technical Support

April 24, 2026

If you've checked the troubleshooting advice in this section and believe the problem that you experienced results from Profile Management, contact Citrix Technical Support. Always collect and provide the following files and as much other information as possible.

Collect Profile Management log files

Detailed steps are as follows:

1. Enable Profile Management on the machine to log all events and actions. For more information, see Enable Profile Management logging.
2. Reproduce the problem on the affected machine.
3. Collect the Profile Management log file and its backup file from %SystemRoot%\System32\Logfiles\UserProfi

The log file from the affected machine includes at least the following information:

- Start of the service (including the version and the build number of Profile Management)
- Reading of the configuration by the service
- One full logon process of the affected user
- The activity the user did when the issue occurred
- One full logoff process for the affected user

Collect the Windows event log file

After you reproduce the problem on the affected machine, follow these steps to collect the Windows event log file.

1. Locate the `%SystemRoot%\System32\winevt\Logs` folder.
2. Collect the Application.evtx file.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Collect installed software details

Collect details of the following software installed on the affected machine:

- Operating system, language, and version.
- Citrix products and versions.

Collect .ini files

Follow these steps to collect .ini files associated with Profile Management:

1. Locate the root folder of each Citrix user profile in the user store.
2. Collect the following .ini files:
    - UPMSettings.ini
    - UPMFRSettings.ini
    - PmCompatibility.ini

Collect a diagnostic tracing log using CDFControl

Collect a diagnostic trace log using the CDFControl as follows:

1. Download the CDFControl tool from Knowledge Center article CTX111961.
2. Run the CDFControl executable.
3. In the window that appears, select one or more tracing modules as needed. For more information about their function descriptions, see the following table.
4. Click **Start Tracing**.
5. Reproduce the problem.
6. Click **Stop Tracing**.
7. Find your trace log in the same folder as the CDFControl executable.

This table lists the functions of track modules in CDFControl.

Trace Module	Description
UPM_DLL_GPCSE	Traces the user group policy evaluation request sent from Profile Management to the Citrix Group Policy client-side extension.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Trace Module	Description
UPM_DLL_OUTLOOK_HOOK	Traces the Profile Management hook module in Outlook. Select it to trace issues with the Outlook search index Roaming feature.
UPM_DLL_Perfmon	Traces Windows Performance Monitor counters associated with Profile Management and errors generated by Profile Management.
UPM_DLL_SearchSvc_Hook	Traces the Profile Management hook module in Windows Search Service. Select it to trace issues with the Outlook search index Roaming feature.
UPM_DLL_WfShell	Traces the Profile Management `Wfshell` plug-in, which reports the desktop-ready event for published applications.
UPM_Driver	Traces file-system changes each time the Citrix streamed user profiles driver is used.
UPM_Service	Traces information each time the Profile Management Service is called. Example occasions include at logon, at logoff, or when mid-session synchronization or periodic maintenance takes place.
UPM_SessionLaunchEvaluation	Traces the launch events associated with the unique transaction ID in Profile Management.
UPM_WMI	Traces the Profile Management VDA WMI plug-in events.

Collect other information

Collect the following information if possible:

- The Resultant Set of Policy (RSoP) report for the affected machine and user by running the `gpresult` command.
- Application event logs.
- If available, the **Userenv** debug file. Consult your Microsoft documentation for information on this tool.

> **Notes:**
>
> Data collection can become complex if Citrix Provisioning Services is part of your deployment

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> and the problem occurs when profiles are being initialized. In that scenario, make the preceding configuration updates in the .ini file (and disable the GPO log settings). We recommend you follow the instructions in Preconfigure Profile Management on provisioned images.

Profile Management best practices

November 7, 2025

A Windows user profile is a collection of folders, files, registry and configuration settings defining the environment for a user who logs on with a particular user account. Users can customize these settings depending on the administrative configuration.

Windows 10 compatibility

Citrix Profile Management supports the latest version of Windows 10 available at release time of Profile Management. It also supports all earlier versions of Windows 10. For example, Citrix Profile Management Version 1912 was shipping at a time when the latest version of Windows 10 was 1909 (RS7). Profile Management 1912 supports Windows 1909 (RS7) and all earlier versions of Windows 10.

The following table summarizes the recommended Microsoft Windows 10 operating systems for different versions of Profile Management:

Profile Management version	Windows 10 version	Notes
1912	Windows 10 1909 (RS7)	Citrix Virtual Apps and Desktops™ 7 1912
1909	Windows 10 1903 (RS6)	Citrix Virtual Apps and Desktops 7 1909
1906	Windows 10 1903 (RS6)	Citrix Virtual Apps and Desktops 7 1906
1903	Windows 10 1809 (RS5)	Citrix Virtual Apps and Desktops 7 1903
1811	Windows 10 1809 (RS5)	Citrix Virtual Apps and Desktops 7 1811
1808	Windows 10 1803 (RS4)	Citrix Virtual Apps and Desktops 7 1808
7.18	Windows 10 1803 (RS4)	XenApp and XenDesktop 7.18

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Profile Management version	Windows 10 version	Notes
7.17	Windows 10 1709 (RS3)	XenApp and XenDesktop 7.17
7.16	Windows 10 1703 (RS2)	XenApp and XenDesktop 7.16
7.15 Long Term Service Release	Windows 10 1703 (RS2)	XenApp and XenDesktop 7.15 LTSR with the latest Cumulative Update

> **Note:**
>
> Attempts to upgrade an OS where Citrix user profiles exist might fail. To proceed with the upgrade, remove Citrix user profiles from the local machine.

Windows 10 Start menu customization

We recommend using a partial lockdown customization layout and deploying the customization through Group Policy. For more information about customizing the layout of the Start menu, see https://docs.microsoft.com/en-us/windows-hardware/customize/desktop/customize-start-layout.

Start menu roaming

Applications pinned to the Start menu might disappear on the following operating systems after several logons:

- Windows 10 version 1607 and newer, 32-bit and 64-bit
- Windows Server 2016 Standard and `Datacenter` editions
- Windows Server 2019 Standard and `Datacenter` editions
- Windows 10 Enterprise for Virtual Desktops

To ensure that Start menu roaming works properly on the preceding operating systems, complete the following configuration steps:

1. Enable the **Folders to mirror** policy and then add the following folders to the list of folders to mirror:
   - `Appdata\Local\Packages`
   - `Appdata\Local\Microsoft\Windows\Caches`
   - `!ctx_localappdata!\TileDataLayer` (applicable only to versions earlier than Windows 10 version 1703)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> Starting with Citrix Profile Management 1912, a folder added to **Default exclusion list –directories** or **Exclusion list –directories** cannot be synchronized even if you add it to **Folders to mirror**. Ensure that you remove the `appdata\local\packages` folder from the exclusion lists before you add it to **Folders to mirror**.

2. Enable the **Files to synchronize** policy and then add the following folder to the list of files to synchronize:
   - `Appdata\Local\Microsoft\Windows\UsrClass.dat*`

Outlook and Office 365

Microsoft recommends Cached Exchange Mode so that a consistent online and offline Microsoft Outlook experience is enabled. You can turn on the Cached Exchange Mode from the Microsoft Outlook client. For more information, see https://docs.microsoft.com/en-us/exchange/outlook/cached-exchange-mode.

When you use Cached Exchange Mode, there is always a copy of a user's Exchange mailbox in an offline folder file (*.ost). The file can grow large.

We recommend avoiding storing Microsoft Outlook data locally or on shared drives. Use the Enable native Outlook search experience feature instead. With this feature, the **Outlook offline** folder file (*.ost) and the Microsoft search database specific to the user roam along with the user profile. This feature improves the user experience when searching mail in Microsoft Outlook. For more information on using this feature, see Enable native Outlook search experience.

Configuring Profile Management from one location

There are three locations from which you can configure Profile Management. To configure Profile Management, use HDX policies in Citrix Studio, or a GPO in Active Directory. You can also configure Profile Management using Workspace Environment Management.

We recommend that you choose only one of the three locations to configure Profile Management.

Troubleshooting best practice

Always use the Profile Management configuration checker tool (UPMConfigCheck) to identify potential configuration errors.

When Profile Management does not work, first validate whether the User Store configured is accessible.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Cookie handling

Profile Management now supports deleting stale cookies for Internet Explorer 10 and Internet Explorer 11. You can use the "Process Internet cookie files on logoff" policy to delete stale cookies to avoid cookie folder bloat. In addition, add the following folders to the list of folders that you want to mirror:

- AppData\Local\Microsoft\Windows\INetCookies
- AppData\Local\Microsoft\Windows\WebCache
- AppData\Roaming\Microsoft\Windows\Cookies

Profile streaming with Microsoft Credentials Roaming enabled

By default, the following folders in the configuration file are excluded from profile streaming:

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

If you configure profile streaming exclusion manually, ensure to add the preceding folders to "Profile streaming exclusion list–directories."

Synchronizing profiles efficiently

Insufficiently synchronized user profiles can result in slow logons, losses of user settings, and profile corruption. It can also need excessive administrative efforts. To synchronize profiles efficiently, follow the recommendations described in this article.

Folder redirection

Folder redirection is a feature of Microsoft Windows that you can use with Profile Management. Folder redirection plays a key role in delivering a successful profile solution.

To use folder redirection, ensure that the relevant users are in the OU that Profile Management manages. We recommend that you configure folder redirection using a GPO in Active Directory.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

For example, you can redirect the following folders by enabling the corresponding policies under **User Configuration > Administrative Templates > Classic Administrative Templates (ADM) > Citrix > Profile Management > Folder Redirection**:

Documents, **Pictures**, **Music**, **Videos**, **Favorites**, **Contacts**, **Downloads**, **Links**, **Searches**, and **Saved Games**

> **Note:**
>
> - Folder redirection eliminates the need to copy the data in those folders each time users log on and thus accelerates user logons.
> - We strongly recommend not enabling **Folder Redirection** for **AppData (Roaming)** and **Start Menu** because it might cause issues in applications and the Start menu.
> - Do not redirect the **Desktop** folder if it is too large. Otherwise, a black screen might occur when a user logs on.

Include and exclude files and folders

Profile Management lets you specify files and folders that you do not want to synchronize by customizing inclusion and exclusion lists. To avoid profile bloat, exclude cache files for third party applications, for example, Chrome cache files located at Appdata\Local\Google\Chrome\UserData\Default\Cache. For more information, see Include and exclude items.

Profile streaming

Profile Management fetches files and folders in a profile from the user store to the local computer only when users access them after they log on. Doing so speeds up the logon process and reduces the profile size. For example, if a file is not actually used, it is never copied to the local profile folder. You can also use the Always cache policy to impose 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.

Active Write Back and Registry

This feature decreases logoff times compared to the Profile streaming feature, especially when there are many changed files. This feature synchronizes modified files and folders (but not registry entries) to the user store during the session, but before logoff.

Internet Explorer 10/11 cookie support

Profile Management 5.0 and later supports enhanced processing for cookies when using Internet Explorer 10 and Internet Explorer 11. To avoid cookie folder bloat, use the Process Internet cookie files

© 1997–2026 Citrix Systems, Inc. All rights reserved.

on logoff policy to delete stale cookies. You can add the following folders to the list of folders to mirror:

- AppData\Local\Microsoft\Windows\INetCookies
- AppData\Local\Microsoft\Windows\WebCache
- AppData\Roaming\Microsoft\Windows\Cookies

For more information, see Process Internet cookie files on logoff.

Glossary

September 7, 2025

This article contains terms and definitions used in the Profile Management software and documentation. Profile-related terms used in other Citrix® software are also included. To understand other concepts relating to Windows user profiles, visit the Microsoft website.

Term	Definition
Base platform	See cross-platform settings store.
Base profile	The base profile is defined by a UNC path to a profile in the user store. If the cross-platform settings feature is used, registry settings and files that can be shared across platforms form a subset of the base profile. This subset is copied to the cross-platform settings store, and, from there, they are added to the profile used as the target for migration or roaming. Although the cross-platform settings store contains a subset of the base profile, this (and the target profile) is always stored as complete profiles. And it can, if necessary, be used as standard Windows roaming or local profiles. Note however that if the streamed user profiles feature is used, the base profile might temporarily be incomplete. Some files might exist in the pending area until the user logs off. See roam for considerations when defining base profiles in roaming scenarios.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Term	Definition
Cache	The terms cache and synchronize refer to the act of downloading files from the user store, or uploading to it. The term fetch is more specific and refers to how the streamed user profiles feature downloads, anytime after logon when the user needs them, a subset of files from the user store.
Citrix mandatory profile, Citrix roaming profile, Citrix user profile	Citrix user profile is the general term for the profile that a user receives when Profile Management is installed and enabled. There are two types of Citrix user profiles: Citrix roaming profiles and Citrix mandatory profiles. A Citrix roaming profile is the standard collection of files, folders, and registry settings that users customize in their day-to-day work, that are saved in the user store at logoff, and that are treated by Profile Management policies. A Citrix mandatory profile is similar to a Citrix roaming profile in how Profile Management treats them. But no changes are saved in the user store at logoff. At logons, a fresh copy of the mandatory profile is loaded. Citrix user profiles are different from Microsoft local, Microsoft roaming, or Microsoft mandatory profiles.
Computer	As used in these Profile Management topics, the general term computer can refer to any machine on which the Citrix Profile Management Service is installed. This can be a user device, virtual desktop (possibly provisioned from a Citrix Virtual Desktops™ virtual machine), or a Citrix Virtual Apps server that hosts published applications.
Cross-platform definition file	This file is an .xml file supplied with Profile Management that contains the information needed to make the cross-platform settings feature work. There is one file per supported application.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Term	Definition
Cross-platform settings store	This location, which is separate from the user store, holds the settings for supported applications once the cross-platform settings feature is configured. Choose which platform's profile data is used to seed the cross-platform settings store. It is the base platform.
Fetch	See cache.
Legacy application	A legacy application is a badly behaved one because it stores settings in a non-standard location. It includes systems that store temporary application data in user profiles and, by doing so, create profile bloat.
Migrate	Migration is the planned, one-way movement of profiles from one platform to another (for example, from Windows XP to Windows 7).
Profile bloat	Windows user profiles can increase in size when temporary files are not deleted. This causes slow logons and is referred to as profile bloat.
Roam	Roaming is the use of different base profiles from multiple computers or sessions (for example, one base profile for a computer running Windows 2008 R2 and a second one for Windows 7). Users roam when they connect back and forth between computers or sessions that have different base profiles. Depending on how you configure your Organizational Units (OUs), a base profile can be shared across platforms. For example, Windows 2008 R2 and Windows 7 OUs can use the same profile. In this case, users do not roam because the same base profile is shared. Base profiles can only be shared by operating systems with the same profile version (Version 1 or Version 2 profiles). Users always roam when both Version 1 and Version 2 profiles are active.
Synchronize	See cache.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Term	Definition
User store	The user store is the central, network location for storing Citrix user profiles. See also cross-platform settings store.
vDisk, Personal vDisk	A vDisk is a virtual disk created from a master image by Citrix Provisioning™ Services. A Personal vDisk is a disk used by Citrix Virtual Desktops to store profiles, user-installed and departmental applications, and user data. Personal vDisks are separate from the disks used for the operating system, registry, and base applications.
Version 1 profile, Version 2 profile	Profiles in Microsoft Windows XP and Windows Server 2003 are known as Version 1 profiles. Those profiles in Windows Vista, Windows 7, Windows Server 2008, and Windows Server 2008 R2 are known as Version 2 profiles. Version 1 and Version 2 profiles have different namespaces, which affects some aspects of their configuration.

© 2025 Cloud Software Group, Inc. All rights reserved. This document is subject to U.S. and international copyright laws and treaties. No part of this document may be reproduced in any form without the written authorization of Cloud Software Group, Inc. This and other products of Cloud Software Group may be covered by registered patents. For details, please refer to the Virtual Patent Marking document located at https://www.cloud.com/legal. Citrix, the Citrix logo, NetScaler, and the NetScaler logo and other marks appearing herein are either registered trademarks or trademarks of Cloud Software Group, Inc. and/or its subsidiaries in the United States and/or other countries. Other marks are the property of their respective owner(s) and are mentioned for identification purposes only. Please refer to Cloud SG's Trademark Guidelines and Third Party Trademark Notices (https://www.cloud.com/legal) for more information.