

Managed Profile™

White Paper

April 2003

Julian Hansen
julian@marcorpsa.com

Contents:

INTRODUCTION.....	3
MANDATORY AND ROAMING PROFILES.....	4
ROAMING USER PROFILES.....	4
MANDATORY USER PROFILES.....	4
PROFILES IN A TERMINAL SERVICES ENVIRONMENT	5
PURE TERMINAL SERVICES ENVIRONMENT.....	5
TERMINAL SERVICES MANAGED BY CITRIX METAFRAME OR SIMILAR PRODUCT.....	5
PRINTING	5
ACCESSING NETWORK STORAGE.....	6
THE MANAGED PROFILE SOLUTION.....	7
THE REGISTRY	7
FILES AND FOLDERS	7
PRINTERS	8
USER MAPPED DRIVES AND FOLDERS.....	8
LOGGING	9
ADVANTAGES OF THE MANDATORY PROFILE SOLUTION.....	9
SUMMARY.....	11

Introduction

Administration of user profiles in a distributed network environment has always had its challenges. The advent of products such as Terminal Services and Citrix MetaFrame has further highlighted the necessity to implement sound user profile management solutions.

There are currently only two options available to administrators with respect to configuring user profiles in a Terminal Services / Citrix MetaFrame environment – roaming profiles and mandatory profiles¹. As the ensuing sections show there are administration issues and disadvantages with both of these methods.

The Managed Profile solution addresses these issues and provides a simple alternative to profile management that incorporates the best of both the mandatory and roaming profile solutions while at the same time simplifying the process of user profile management.

Another aspect of managing user profiles involves the setup and management of Printers. Not only do printer connections require management but printer properties also require management on a per user level. The Managed Profile also includes functionality for simplifying the task of managing user printer connections and settings.

¹ Local profiles are technically a third option but local profiles provide no manageability advantages and are not included as a potential option.

Mandatory and Roaming Profiles

The default installation of Windows based operating systems currently only provide administrators with two user profile options: mandatory and roaming profiles

Roaming User Profiles

The following description was taken from the Microsoft System Developer Network Library – January 2003 “*Setup and System Administration\Policies and Profiles\SDK Documentation\User Profiles>About User Profiles\Roaming User Profiles*”

If a computer is running Windows NT Server/Windows 2000 Server on a network, users can store their profiles on the server. These profiles are called *roaming user profiles*.

Roaming user profiles have the following advantages:

- **Automatic resource availability.** A user's unique profile is automatically available when he or she logs on to any computer on the network that is running Windows NT/Windows 2000/Windows XP. Users do not need to create a profile on each computer they use on a network.
- **Simplified computer replacement and backup.** When a user's computer must be replaced, it can be replaced easily because all of the user's profile information is maintained separately on the network, independent of an individual computer. When the user logs on to the new computer for the first time, the server copy of the user's profile is copied to the new computer.

Mandatory User Profiles

The following description was taken from the Microsoft System Developer Network Library – January 2003 “*Setup and System Administration\Policies and Profiles\SDK Documentation\User Profiles>About User Profiles\Mandatory User Profiles*”

A *mandatory user profile* is a special type of pre-configured roaming user profile that administrators can use to specify settings for users. With mandatory user profiles, a user can modify his or her desktop, but the changes are not saved when the user logs off. The next time the user logs on, the mandatory user profile created by the administrator is downloaded. There are two types of mandatory profiles: *normal mandatory* profiles and *super-mandatory* profiles.

User profiles become mandatory profiles when the administrator renames the NTuser.dat file (the registry hive) on the server to NTuser.man. The .man extension causes the user profile to be a read-only profile.

User profiles become super-mandatory when the folder name of the profile path ends in .man; for example, \\server\share\mandatoryprofile.man\.

Super-mandatory user profiles are similar to normal mandatory profiles, with the exception that users who have super-mandatory profiles cannot log on when the server that stores the mandatory profile is unavailable. Users with normal mandatory profiles can log on with the locally cached copy of the mandatory profile.

Only system administrators can make changes to mandatory user profiles.

Profiles in a Terminal Services Environment

There are two scenarios regarding profiles in a Terminal Services environment

Pure Terminal Services environment

A pure Terminal Services environment is where native Terminal Services on a Windows NT Server are accessed directly by users who are assigned to specific servers on which the applications required by those users have been pre-loaded.

This is not a recommended practice for most Terminal Services installations for the following reasons

- Fail Over – should a server become unavailable all users assigned to that server will be unable to work.
- Efficiency – this model does not provide for proper load balancing.
- Stability – there are inherent stability risks associated with installing and running multiple applications on a single machine. There is increased potential of one application adversely affecting other applications.

The primary issues relating to profiles in a pure Terminal Services environment would be that of size. A roaming profile can (and often does) grow to an unmanageable size which can have an impact on perceived performance. A large profile will result in delays in logon and logoff which could be erroneously interpreted as a performance problem. Roaming profiles are also prone to corruption which in turn affects application stability.

Terminal Services managed by Citrix MetaFrame or similar product.

In a managed Terminal Services environment applications are loaded on and published from specific servers which are managed and load balanced by management software such as Citrix MetaFrame. In such an environment each request for an application could potentially result in a new logon event if the application requested is published from a different group of servers from the group where currently open applications are published from. This scenario creates a new problem as far as user profiles are concerned. If user profile changes are made in more than one simultaneous session, the last session to close will determine the profile settings that are retained. For example, assume a situation where application X and application Y are published from different servers. A user starts 1 instance of X and 1 instance of Y. In application X the user makes a colour change and then exits the application. The user then makes a menu bar change in application Y and exits the application. In this example, any changes made to the user's profile from application X will be overwritten by the profile changes from application Y.

In both the scenarios described above a mandatory profile would solve some of the issues. In the case of a pure Terminal Services environment profile size and corruption issues would go away and in a Citrix MetaFrame environment profile overwrites would be eliminated. However, this would be at the cost of usability as in many cases dynamic profile modifications are a necessary user function for example loading and unloading mail folders in Microsoft Outlook.

Printing

Printer connections and printer settings can create certain problems for administrators in a Citrix environment or any other environment that makes applications available through a portal (such as Citrix's NFuse). In such situations users do not have the normal desktop. This means they do not have access to the standard management tools available with Windows based products such as the Printers control panel applet. Because of this, users cannot make permanent setting changes for printers – settings can be changed in the print dialog that is displayed when a print job is being created but these do not persist and have to be set for each new job.

Accessing Network Storage

A common configuration issue is providing users with access to the correct locations where data is stored and retrieved. A simple example would be the user's home drive but can also include drive mappings to other locations as well. In many cases there is the problem that, due to administration overhead, access is given at too high a level i.e. users are given access to view or even browse folders and files they should not be able to see. A major obstacle for administrators is the lack of functionality available in logon scripts. ADSI has to a certain extent breached the functionality gap but the issue of management remains. Unless a generic solution with accompanying management system is developed the scripts would most likely have to included hard coded settings that require an involved process for updating.

The ideal solution would be to have a single central management system for all functionality and settings relating to user configuration (logon scripts, profile, printers etc).

The Managed Profile Solution

The Managed Profile solution addresses all the problems described above as well as the issue of printer assignment and printer settings management. This solution works on the principle of “that which is not expressly permitted is denied” in other words the user profile is assumed to be mandatory and the administrator, by means of the Managed Profile administration utility, can configure which registry keys and which folders and files a user is allowed to make persistent changes to.

The Managed Profile agent accesses information in a database through a web server. Currently supported databases include Microsoft Access and Microsoft SQL Server. Future releases will support other databases and formats (Oracle, MySQL and XML files). The agent uses the information in the database to either restore or save settings that have changed during a session. Settings can be configured to activate based on the following specific entity settings

- Everyone
- User ID
- Group Name
- Machine Name

The Managed Profile solution currently supports 3 configuration management functions: registry, files and folders and printers.

The Managed Profile agent distinguishes between a logoff and a logon event and either saves or restores settings accordingly – giving the impression that a roaming profile is being used when in fact a managed mandatory profile is being used.

Although it is not necessary for the Managed Profile to be used in conjunction with Mandatory User Profiles it is highly recommended that users are configured to use Mandatory Profiles in order for the solution to function correctly. The Managed Profile agent merges saved user settings with the mandatory profile during logon and saves any profile changes the user makes when a logoff occurs. Only changes relating to objects defined in the database will be saved and restored.

The Registry

An administrator determines which keys in the registry a user should be allowed to make persistent changes to. These are loaded into the administration system by means of the administration console. Entries in the database for Registry keys synchronization are assigned the following values

- An object – the path to a registry key in the HKEY_CURRENT_USER hive
- A name – a unique identifier for these settings.
- An entity – is one of the four entity values listed above.

Only registry settings that have changed are saved during a logoff event. During a logon event all saved registry keys are merged with the user’s profile.

The Managed Profile solution allows changes to be made to the user registry only i.e. no changes to the machine registry are permitted as in a shared environment this could have disastrous effects. Should changes to the machine registry be required it is recommended that policies be used to achieve this.

Files and Folders

As with the registry entries an administrator can specify certain files and folders that need to be synchronized during logon and logoff. The Managed Profile uses an intelligent process of synchronisation for files and folders that have changed, to minimize network traffic at logon and logoff times. Configuration for files and folders is a similar process to Registry entries. An administrator specifies the following values for each folder synchronization entry

- A file or folder path
- An entity

Printers

Printer connections are managed during a logon process. A user's printer connections are automatically created and the user printer settings for each printer are loaded into the user's profile. Users can configure which printers they want to have access to by means of the Managed Profile PrintGUI. The PrintGUI uses information read from a database about which printers a user has access to. A user is given access to a printer using Active Directory groups – a user can only see those printers his/her group membership allows him/her to see. Using the PrintGUI users can add or remove printers from their profiles. The PrintGUI also allows users to specify the default printer and set the printer properties for each printer loaded into the profile. These properties will persist across user sessions.

Tools for importing printer information from print servers and automatic group assignment based on printer names etc are also provided.

User Mapped Drives and Folders

The Managed Profile solution provides two mechanisms for managing user access to network storage.

- Group mapped drives
- Group mapped folders

Group mapped drives

This functionality allows administrators to use user names and groups to control drive mappings.

An administrator specifies a drive letter, a location and a security object. The Managed Profile determines if any of the user's credentials match the security object specified (ALL, USER, GROUP and MACHINE). If a match is made the Managed Profile attempts to map the specified drive to the specified location reporting any errors to the log if it fails.

Group mapped folders

The group mapped folder functionality is similar to the group mapped drives described above but allows administrators to specify virtual folders instead of drive mappings. Using the built-in virtual folder functionality of the Windows Explorer Shell the Managed Profile adds folder definitions which can be configured to appear in either the user's "Desktop" or "My Computer" namespaces based on settings configured by the administrator. Once a folder has been added to the user's profile the user can access that folder in the same way as any other folder on a local or mapped network drive.

After a folder has been added it becomes part of the local file system and can be accessed in exactly the same way as any other folder in the system.

The advantage of the mapped folders is that administrators can provide much better control over which users have access to which data without having to exhaust the limited supply of drive letters for mapped drives.

Logging

The Managed Profile solution provides a comprehensive logging mechanism. The agent has execution trace functionality that can be switched on or off by command line switch. The trace functionality is useful for identifying system errors and malfunctions relating to the Managed Profile agent.

In addition to this a multi-level system error logging facility allows an administrator to specify a logging level (from *none* to *verbose*). Any errors picked up by the agent during execution are logged to a central log database where they can be centrally monitored.

Logging of user logon and logoff events is also available. Administrators can configure the system to record every logon and logoff event or to record only the most recent logon and logoff event per user.

Advantages of the Mandatory Profile Solution

In addition to solving the problem of overwritten profile settings in a published application environment, an important advantage of the Mandatory Profile solution is management. It provides administrators with a simple and central point of control all configuration issues relating to user profiles providing advanced functionality without the need to have to write complex and difficult to support logon scripts and processes.

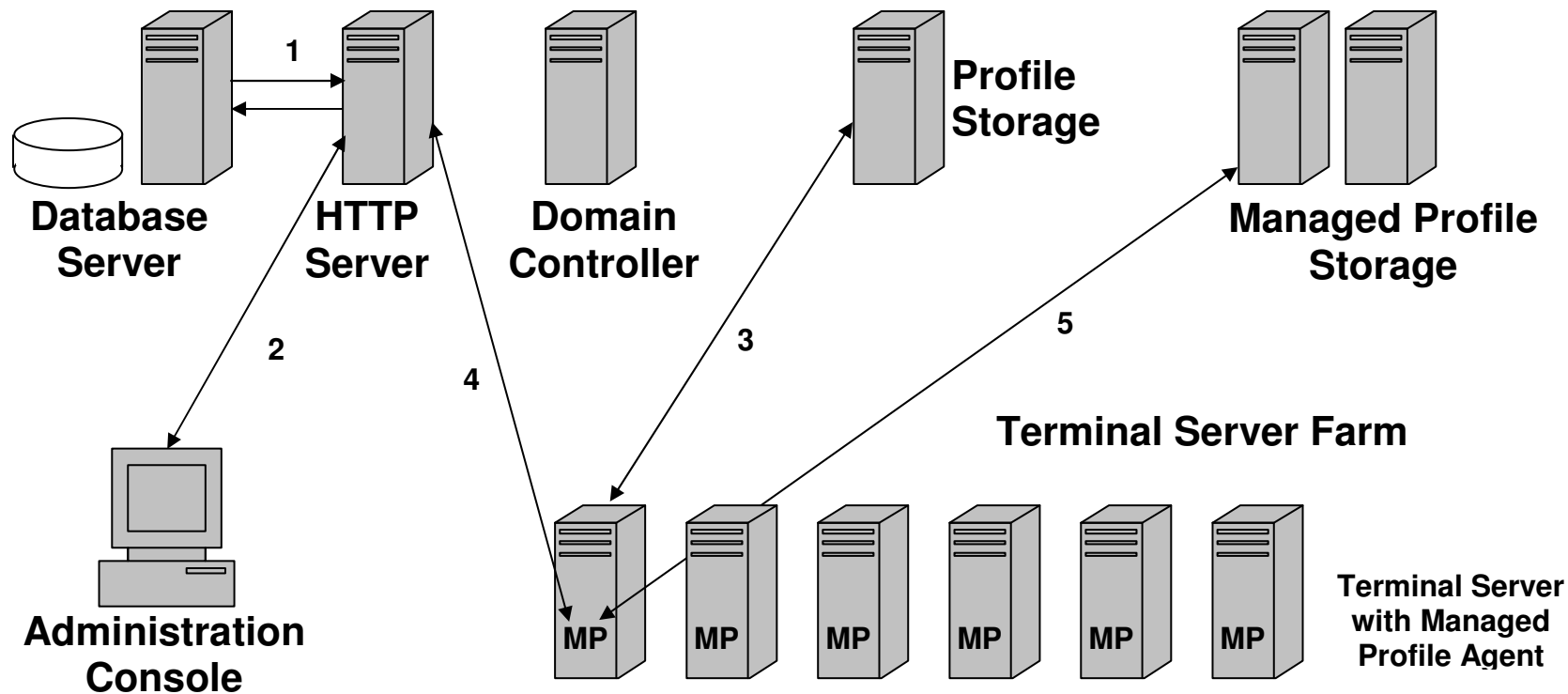
The Mandatory Profile Solution has been designed to be simple but effective. Installation of the agent is a simple process of distributing a single file (<100K) to each Terminal Server or device on which a user can logon and adding a single line to the Active Directory logon and logoff scripts.

The administration console requires two processes to be completed

- Database creation – this is done by means of a script or template database (in the case of Microsoft Access)
- Web Server Configuration – this is done by copying the server scripts to the web server.

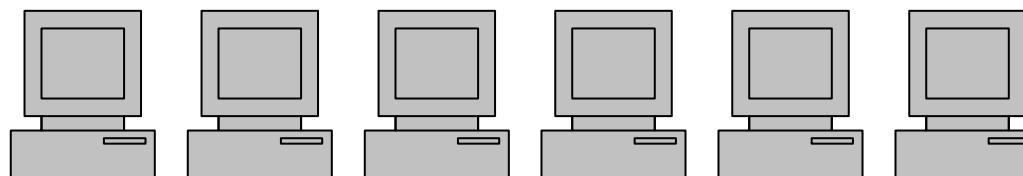
Once the system has been installed the administrator can setup objects and entities required for synchronization and profile management using the administration console.

Agents can also be configured to have multiple data sources for fail over and load balancing allowing administrators to implement load balancing while maintaining central control of configuration settings.



1. All data transactions carried out by HTTP server.
2. Management provided by admin console on HTTP Server.
4. Profile downloaded from profile storage as part of normal logon.
3. Managed Profile uses HTTP Server to set and retrieve data.
5. User profile settings retrieved and stored by MP from MP storage.

CITRIX (optional)



Terminal Server Clients

Summary

The Managed Profile Solution is a simple but effective means of centrally managing user profiles. It has been designed to be easy to install, easy to use and easy to maintain which translates into lower costs for the client and increased return on investment. The product is continually being improved and developed to provide more tools and functionality for administrators in an attempt to further simplify the task of user profile management.

Managed *Profile* White Paper

Managed Profile and its logo are trademarks of Marketing & Research Corporation cc

Citrix MetaFrame is a registered Trademark of Citrix Systems Inc.

Microsoft and Windows are registered Trademarks of the Microsoft Corporation.

Oracle is a registered trademark of the Oracle Corporation.