



TECHNICAL OVERVIEW

Contents:

INTRODUCTION 3

MANDATORY AND ROAMING PROFILES 4

 ROAMING USER PROFILES 4

 MANDATORY USER PROFILES..... 4

PROBLEMS WITH EXISTING PROFILE SOLUTIONS 6

 MANDATORY PROFILES 6

 ROAMING PROFILES..... 6

 PROFILES AND CITRIX 6

 PROFILE CUSTOMIZATION 6

 PRINTER MANAGEMENT 6

 REGISTRY RULES 8

 FILES AND FOLDER RULES 8

 DRIVE MAPPING RULES 8

 SHORTCUTS RULES 8

 EXPLORER NAMESPACE EXTENSIONS (VIRTUAL FOLDERS) 8

 PRINTER RULES 9

 LOGGING..... 9

ADVANTAGES OF THE MANDATORY PROFILE SOLUTION 10

SUMMARY 10

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 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 – roaming profiles and mandatory profiles¹. As the ensuing sections show there are administration issues and disadvantages with both of these methods.

Another aspect of profile management that has proven to be problematic is that of printing. Specifically in assigning printers to users or users to printers and managing printer settings.

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. Managed Profile also addresses the issue of printer management.

¹ Local profiles are technically a third option but local profiles provide no manageability advantages and are not included as a potential option.
Managedprofilewp060103.doc

Mandatory and Roaming Profiles

The only two user profiles options that administrators currently have are 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.

Problems with existing profile solutions

Mandatory and roaming profile solutions each have their advantages. However, neither solution is a perfect fit in most environments.

Mandatory Profiles

Mandatory profiles have the advantage of being very stable. Because they are essentially read only profiles there is no risk of corruption when a profile is written back during the logoff process. They are easier to manage as settings can be managed centrally and there is no risk of the user profile growing to an unmanageable size. The downside is that users are unable to save profile settings between sessions and in many instances this is a major drawback.

Roaming Profiles

Roaming profiles are almost the exact opposite of mandatory profiles. They are more susceptible to corruption and can grow to unwieldy sizes but users can customize their settings and have the changes persist across sessions.

The above is valid in both desktop and terminal server / Citrix environments. However, there is an additional problem that is experienced with products such as Citrix.

Profiles and Citrix

In Citrix environments it is possible for a user to be simultaneously logged on to more than one server. In such instances two or more copies of the user profile are loaded at the same time. If changes are made to the profile in more than one session the only changes that will persist to the next session will be those made in the last session to close resulting in the loss of user profile settings. Neither mandatory nor roaming profiles can solve this problem.

Profile Customization

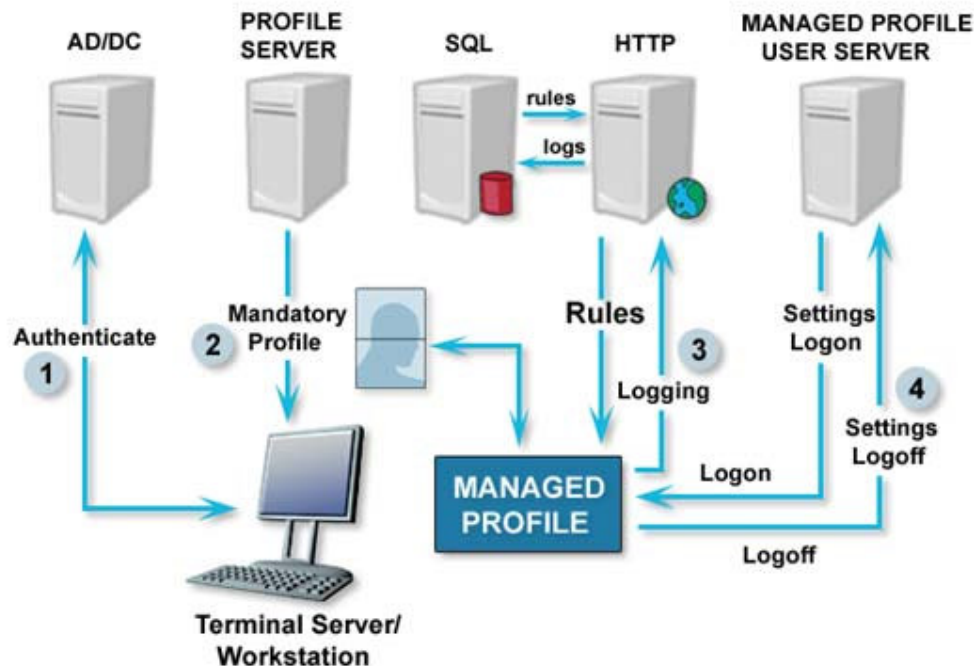
In a few situations one profile fits all users. In most situations this is not the case and different users or groups of users require different or common settings depending on the functions they perform. Group policy has to a certain extent provided a solution for administrators to customize user profiles but in many cases group policy is not the right tool for the job. This often leads to the creation of complex login scripts that perform further customization of user profiles after login. This is not always desirable as login scripts can be difficult to manage and are prone to developing spaghetti code and obsolete functionality that is never removed.

Printer Management

Printer management can be another cause for administrative headaches. Not only is there the process for connecting users to the correct printers but there is also a requirement for users to be able to set default settings for their mapped printers as well as to be able to manage print jobs.

Managed Profile

Managed Profile addresses all the problems described above as well as the issue of printer assignment and user 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 console, can configure exactly which settings a user is allowed to control



The Managed Profile agent accesses information in a database through a web server. When the user logs on and is authenticated by a domain controller, a mandatory profile is downloaded to the terminal server or workstation. A logon script launches the Managed Profile agent which in turn downloads setting and configuration rules from the Managed Profile database through a web service. The Managed Profile agent applies the rules to the mandatory profile by downloading previously saved settings from the Managed Profile Settings Server and restoring them to the relevant keys in the mandatory profile. During a logoff event the process is repeated with changed settings being written back to the Settings Server.

Rules are associated with the following objects

- Everyone
- User ID
- Group Name
- Machine Name

Managed Profile currently supports the following rules

Registry Rules

Registry rules are used to save and restore a particular registry key or sub-tree. The rule is created with the path to the key. When a user logs on to a device all registry rules are checked and if a previously saved setting is available for that rule in the users settings folder it is loaded into the user's registry. On logoff Managed Profile checks all registry rules to see which have changed during the session and writes only the changes to the user's settings folder. This ensures that no settings are overwritten across simultaneous sessions.

Files and Folder Rules

File and folder rules synchronize files and folders that have changed with those stored in the user settings folder. The process is similar to the normal roaming profile process but instead of all files and folders being synchronized only those associated with a rule in the Managed Profile database are synchronized giving administrators more control over which files are copied over the network during logon and logoff.

Drive Mapping Rules

Drive mapping rules do as the name suggests, map local drives to network resources. The process is similar to the normal process for mapping a drive where a drive letter and a destination is specified. The difference between mapping drives with Managed Profile is that drive mapping rules can be associated with a security object such as a user or a group which provides greater control over how drives are mapped.

Shortcuts Rules

Shortcut rules provide the functionality for creating shortcuts on the desktop, in the programs area and the quick launch toolbar. With this functionality it is possible to either add one or two program icons to a profile or configure a whole desktop based on user or group.

Explorer Namespace Extensions (Virtual Folders)

Virtual folders are an alternative to mapped drives. They use explorer namespace extensions to add folders on a remote server or workstation to the explorer namespace, thereby giving access to files and folders on a file server without having to map a drive. An example of where this can be advantageous is as follows. If a file server has multiple folders that exist under a single shared folder where each user or group of users potentially has access to a different subset of folders a drive mapping can be confusing. By mapping a drive at the highest common level users have to know which folders they have access to and which not. The virtual folder solution provides the functionality for remote folders to be added directly to the users explorer namespace without the need for the folder to be shared or a drive to be mapped.

Printer Rules

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. Administrators determine which printers users are allowed to access – this is done using user and group rules. The PrintGUI uses this information to display a list of printers that a user may choose to include in his profile. The PrintGUI can also be used to specify a default printer as well as user specific printer settings such as orientation, paper size etc. The Managed Profile agent uses this information to setup and configure printers in the profile during logon. Users can also use the PrintGUI in place of the normal printer control panel applet to manage and monitor print jobs

Administrators can now also configure printer mappings based on the IP Address of the client. This means that when users move around they can get the closest printer rather than a default printer that might be situated in a remote location.

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.

All errors are logged to the Managed Profile database where they can be viewed using the Administration Console.

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 Managed Profile Solution

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
- Web Server Configuration

Once the above items have been configured the administrator can start creating rules.

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.

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.