



Simplify Profiles Installation and Configuration Guide

Adam D. Oliver, Senior Sales Engineer
triCerat, Inc.

Table of Contents

- Prepping the Environment 3
 - Requirements 3
 - Architecture..... 3
 - Port requirements 3
 - Architecture diagram 3
 - Working with V1 and V2 Profiles..... 4
 - Setting up the Mandatory Profile..... 4
 - Simplify Profiles and Group Policy..... 5
 - Creating a Share for Folder Redirection 5
 - Third Party Profile Solutions 6
- Installation..... 6
 - Database Setup 6
 - Installing Simplify Profiles 7
- Configuration..... 7
 - Before Using the Simplify Console 7
 - Creating Profile Objects..... 8
 - Profile Segmentation..... 9
 - Locating Registry Data 9
 - Migrating Existing Roaming Profiles..... 9
- Troubleshooting 10
- Appendix 10
 - Using Process Monitor to Find Application Registry Locations 10

Prepping the Environment

Requirements

- Terminal or XenApp server running Windows 2003, 2008 or 2008 R2. Both 32-bit and 64-bit architectures are supported.
OR
- Workstation/Virtual Desktop running Windows XP, Windows Vista, or Windows 7. Both 32-bit and 64-bit architectures are supported.
- SQL Server 2000, 2005, 2008 or SQL MSDE/Express 2000, 2005, 2008 (small installations or PoCs only)
- Active Directory based network

Architecture

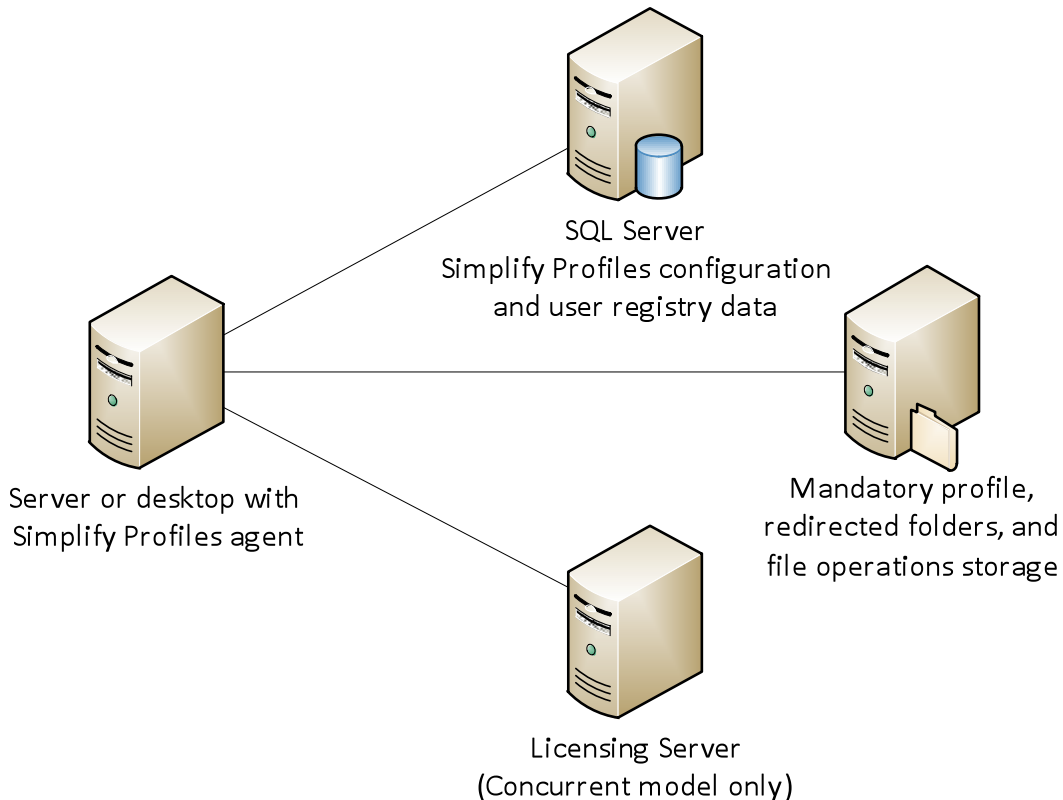
Simplify Profiles has very simple architecture requirements. There are no middle-man management servers. Servers and desktops with the Simplify Profiles agent connect directly to the database. In a concurrent licensing scenario servers and desktops with the Simplify Profiles agent will also contact a licensing server.

Port requirements

SQL ports – This is environment dependent. Please contact your database administrator to determine if a port needs to be specified.

License server ports – On the license server, port 3650 needs to be accessible. On the server or desktop with the agent, port 3651 needs to be accessible.

Architecture diagram



Working with V1 and V2 Profiles

Simplify Profiles does not separate registry data based on operating systems. Therefore, one database can provide registry settings for both version 1 and version 2 profiles. This can ease the transition from Windows XP and 2003 to Windows 7 and 2008 or allow a mixed environment. Both a V1 and V2 mandatory profile will be needed in this scenario.

Setting up the Mandatory Profile

Simplify Profiles uses a mandatory profile as a base for all users. To create the mandatory profile, do the following:

- 1) On a server with the required applications, log in a user in that has no existing roaming, mandatory, or local profile. This will create a brand new profile.
- 2) Make the necessary settings in the session that will apply to all users.
- 3) Log out of the session.
- 4) Log in as an administrator.
- 5) Run `sysdm.cpl` to launch System Properties.
- 6) Under the Advanced tab, click the Settings button for User Profiles.
- 7) Select the user with the brand new profile and click the Copy To button.

- 8) Enter the network path for the new mandatory profile. For Vista, Windows 7, 2008, and 2008 R2, make sure to include the .v2 extension to the folder.
- 9) Under "Permitted to use", click "Change" to specify who can use the profile.
- 10) Click "Object Types", select "Groups", and click "OK".
- 11) Under "Enter the object name to select", type in the names of the groups that will use the mandatory profile, e.g. Domain Users, and click "OK".
- 12) Click "OK" in the "Copy To" window to finish copying the profile.
- 13) Browse to the network location of the profile and rename ntuser.dat to ntuser.man.

Notes:

When sharing the mandatory profile, turn off caching. If the profile fails to load, make sure the owner of the mandatory profile folder is set to Administrators. In some scenarios leaving indexing on for the folder can also cause problems loading the profile.

Microsoft does not recommend mixing roaming or mandatory profiles amongst different operating systems. Use the target operating system to make your fresh profile, e.g. build the profile on 2003 x86 for 2003 x86 Terminal Servers and 2008 x64 for 2008 x64 Terminal Servers. When copying a profile for Windows 2008, Vista, or Windows 7 remember to add the .v2 extension to the folder.

For testing it is advisable to assign the mandatory profile to individual test users in Active Directory, or via a group policy only applied to the test servers. This will keep the mandatory profile from being used by a server in the production environment.

Simplify Profiles and Group Policy

Simplify Profiles can be used to replace many group policy settings and administrative templates. It can also be used in conjunction with existing group policies. However it is not recommended to create settings that conflict with existing group policies. When moving a setting from Group Policy to Simplify Profiles, please remove the link to the policy or clear the setting within.

Creating a Share for Folder Redirection

On the parent folder for redirected folders, make sure to set the following NTFS permissions:

- **CREATOR OWNER** - Full Control (Apply onto: Subfolders and Files Only)
- **System** - Full Control (Apply onto: This Folder, Subfolders and Files)
- **Domain Admins** - Full Control (Apply onto: This Folder, Subfolders and Files)
- **Everyone** - Create Folder/Append Data (Apply onto: This Folder Only)
- **Everyone** - List Folder/Read Data (Apply onto: This Folder Only)
- **Everyone** - Read Attributes (Apply onto: This Folder Only)
- **Everyone** - Traverse Folder/Execute File (Apply onto: This Folder Only)

For the share permissions, set “Everyone” to have Full Control. For a detailed explanation on how these permissions play out, see the Microsoft article [KB274443](#).

When implementing Simplify Profiles in an environment with bloated roaming profiles, it is best to start with a fresh set of Application Data folders.

Third Party Profile Solutions

If your servers currently have another profile solution installed please make sure to fully remove the product before installing of Simplify Profiles. In testing it is preferable to create a fresh server matching production on which to install Simplify Profiles instead of reusing a server used to test another profile solution.

Installation

Database Setup

Supported Databases

- SQL Server 2000, 2005, 2008
- SQL Express 2005, 2008 (PoCs and 1-2 server installs only with TCP/IP and Named Pipes enabled)
- SQL Clusters (for HA)

Database Authentication

Both SQL and Windows Authentication are supported. When using Windows Authentication the database will need to be pre-created with certain permissions. No extra steps are required to install using SQL authentication.

Installing the Simplify Suite Using SQL Windows Authentication

- 1) Contact triCerat support to obtain the proper SQL script.
- 2) Create an AD group for all the triCerat servers and workstations, you may alternatively use the Domain Computers group. Once a server is added to the group, it must be rebooted to renew its security principle.
- 3) Add an SQL login for the new AD group using Windows Authentication.
- 4) Add an SQL login for the user account performing the Simplify Suite if it does not already exist.
- 5) Create a database for Simplify Profiles. For installations prior to 5.3.0, the database must be named “Simplify”.
- 6) Give both the new AD group login and the user login the dbowner role on the Simplify database.

- 7) Install the Simplify Suite on all the servers and workstations.

Post-installation Permissions

- 1) Run the appropriate script from triCerat for your SQL version.
- 2) The new roles can be added to the appropriate logins. You may use the Domain Users group or create a new group for all users Simplify Profiles will affect.
 - db_datareader – needed by all logins
 - ExecuteSP – needed to run the Simplify Console
 - SaveRestore – needed on Windows 2003/ XP Suite installations to save registry data
 - LicenseUpdate – needed by all logins

Installing Simplify Profiles

- 1) Run the Simplify Suite installer for your architecture.
- 2) At the **Welcome** screen click **Next**.
- 3) Accept the license agreement and click **Next**.
- 4) At the **Upgrading** window, please read the warning if you are doing an upgrade. If ready to proceed, click **Next**.
- 5) Select the desired destination folder and click **Next**.
- 6) On the **Custom Setup** screen remove any unneeded components. The Database component is always required to setup the connection to the Simplify Database. Click **Next**.
- 7) At the **Database Installation Help** screen, click **Next**.
- 8) Enter the database server name. Custom ports should be added after the database name, separated by a comma. Select the authentication type, if using Windows Authentication please review the Windows Authentication portion of this guide. For 5.3.0 installs and higher the database name may be changed. Click **Next** to proceed.
- 9) At the **Ready to Install** windows, click **Install**.
- 10) Once the install is complete, click **Finish** to exit the installer.

Configuration

Before Using the Simplify Console

Before implementing the first Simplify Profiles objects, make sure to have a list of your company policies for users. Take note of any restrictions already in effect that might come down from group policy, e.g. forcing a Windows theme, hiding drives, or other machine restrictions. If the Simplify Profiles servers are isolated from group policy this step will give you a guideline to follow for creating objects in the Simplify Console.

Simplify Profiles can make assignments on a wide variety of objects in Active Directory. Creation of an organizational unit structure to support your assignments design is unnecessary. Continue the Microsoft best practice of creating your OU structure based on your organizational design. Use standard Active Directory security groups to assign objects to users spread out across multiple OUs. New users added to Active Directory groups with Simplify Profiles assignments will automatically inherit those assignments.

About Profile Objects

Within a registry object, a key can be created, deleted, or marked as Save/Restore. When marked Save/Restore a key, and all subkeys if specified, will be saved in the SQL database when users with that assignment logout. At login the saved data will be restored to those user profiles. Higher level keys marked Save/Restore, may contain lower level keys that should not be retained. After creating a Save/Restore, lower level keys may be right-clicked and marked as an exception. If marking HKCU\Software as a key to Save/Restore, at least the following keys below it should be marked as an exception.

- \Policies
- \Microsoft\Windows
- \Microsoft\Windows NT

Both HKCU\Software\Policies and HKCU\Software\Microsoft\Windows\CurrentVersion\Policies and the Group Policies caches. They should never be marked Save/Restore. Windows and Windows NT should not be marked as a Save/Restore in their entirety.

Individual values in the registry can be created, deleted, or marked Save/Restore. In addition, an individual value can be set to a default value. In this scenario, any change to that value will be reset at next login to the value specified by the administrator.

A file operation can copy, move, rename, or delete a file or folder. Operations are performed at logon and logout. Folder operations can easily include or exclude all subfolders. For environments where application data redirection performs poorly, file and folder operations allow an administrator to copy data out of the profile before a user logs out. At login those files and folders can be copied back into the profile, allowing application data to change as needed from session to session.

Windows policies objects provide an easy-to-use interface to apply options commonly done within group policy. The objects available are drive mappings, drive restrictions, explorer restrictions, and folder redirection. The flexibility of making assignments in the Simplify Console makes it better suited to making these types of assignments. When using Simplify Profiles to make these objects, remove any group policies that do the same, eliminating any conflicts that might occur during the group policy refresh cycle.

Creating Profile Objects

<add step by step>

Profile Segmentation

Simplify Profiles is a form of profile segmentation. Each application's registry and data can be isolated. This allows the removal of specific corrupt data instead of the entire profile. Typically corrupt registry data is removed by deleting ntuser.dat. A user will now have to rebuild all application settings. Simplify Profiles allows the removal of registry data by object in the Console. In an environment with Adobe Reader, Microsoft Office, and Internet Explorer, each application can have a related object within Simplify Profiles. Registry corruption for a single object, e.g. Adobe Reader, can be removed using the triReg utility. This allows the other applications to retain their settings, minimizing the impact of the corruption.

It is possible to create a "catch-all" type object and slowly move towards a segmented design. Start with marking all of "Software" as Save/Restore. Make the necessary exceptions mentioned in the "Creating Profiles Objects" section to avoid saving the Group Policy cache the Windows keys in their entirety. As applications are segmented and get their own profile object, their keys can be excepted from this "catch-all" object. This method can shorten the initial setup time for Simplify Profiles, but reduces the benefit of the software when just the "catch-all" object is in use.

Locating Registry Data

The Simplify Suite provides a utility called RegDiff to located registry values altered by an application. From the "Tools" menu, go to "External->RegDiff". Start a new compare and snapshot either HKEY_Current_User or HKEY_Local_Machine. Run the application in question and make configuration changes. After closing the application, take another snapshot and RegDiff will show you what has changed in the registry. Any level of the registry in the results can be marked for a Save/Restore or other registry operation. Once the necessary operations are marked, go to File->Create Registry Object to create a new object in the Simplify Suite. For more in-depth registry monitoring, please view the Process Monitor section of the Appendix.

Migrating Existing Roaming Profiles

Simplify Profiles should be run alongside existing roaming profiles once objects have been created and assigned. This will allow user settings to be migrated to the database at the end of the user's next

session. Leaving both in place for a week or two should catch almost all users within an organization. After the migration period, users can be switched to a mandatory profile. Group Policy can be leveraged to point to a mandatory profile located on the local machine using the %COMPUTERNAME% variable.

Troubleshooting

I'm getting database errors on install and the SQL logs show denied logins for Anonymous Logon.

Make sure you specify the SQL server by computer name or FQDN, not the IP address. When doing a PoC, make sure the machines involved are domain members.

Save/Restore operations are not pulling registry information into the database when using Windows Authentication.

This is indicative of a permissions issue in SQL or Licensing problem. Check the event viewer for license related messages. Review the Windows Authentication installation procedures to find any missing permissions within SQL.

A newly added server is being denied access to the database during install.

If not using Domain Computers, make sure the computer was rebooted after being added to the triCerat AD group. This will make sure that group membership is part of its security principle.

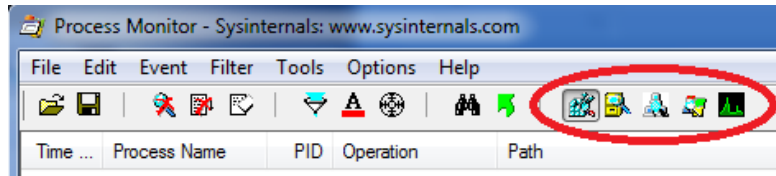
Appendix

Using Process Monitor to Find Application Registry Locations

Process Monitor is a utility from Microsoft that can be used to find portions of the registry accessed by an application. Once the locations are known, an object can be created in Simplify Profiles to Save/Restore that area. The suite of utilities containing Process Monitor can be downloaded from <http://www.sysinternals.com>.

Process Monitor captures a large amount of events happening in Windows. By default the filter captures a lot of events. The filter will need to be modified to slim down the events to just the pertinent registry information. Launch Process Monitor by executing the procmon.exe executable. From here on Process Monitor will be referred to as Procmon.

Event capture happens automatically once the filter window is closed. To stop capture until ready, hit CTRL-E or go to "File->Capture Events". At the far right of the toolbar there are five icons that will turn on or off specific types of events. Make sure only the far left icon, Show Registry Activity, is selected.



Certain registry operations can be ignored while monitoring. This includes HKEY_Classes_Root and HKEY_Local_Machine. To filter these out press CTRL-L or go to "Filter->Filter". Create the following two filters:

Path	begins with	HKLM	Exclude
Path	begins with	HKCR	Exclude

If you are on a Terminal Server and want to monitor user registry access as opposed to your own, filter out HKEY_Current_User with the following:

Path	begins with	HKCU	Exclude
------	-------------	------	---------

You will now only see events inside the HKEY_Users hive. Be careful about filtering all registry entries but RegSetValue. You may miss keys and values needed by the program that were not set during normal operation. Focus both on set operations and query operations.

Once a registry key or value is located, follow the path back to determine the highest level at which you can create your object. For instance, setting Adobe Reader to display the splash screen creates the following value:

```
HKCU\Software\Adobe\Acrobat Reader\9.0\Originals\bDisplayAboutDialog
```

Following the path back, it can be determined that a Save/Restore operation on HKCU\Software\Adobe\Acrobat Reader will most likely catch all of Adobe Reader's settings for a user. When capturing events on a terminal or Citrix server the path will show HKU\<sid>, however the operation in the Simplify Console will be for HKCU.

If it is determined that a specific process, operation, or path can be ignored, you can easily right-click on it and exclude the item. To exclude a registry path and all sub-paths, after excluding the path edit the filter and change "is" to "begins with". Be careful with excluding svchost.exe. It will need to be determined what processes that instance (PID) is running and if they are related to the program being monitored. See the appendix for breaking down svchost.exe.


```
C:\>tasklist /svc /FI "ImageName eq svchost.exe"
```

Image Name	PID	Services
svchost.exe	668	DcomLaunch, PlugPlay, Power
svchost.exe	788	RpcEptMapper, RpcSs
svchost.exe	868	AudioSrv, Dhcp, eventlog, HomeGroupProvider, lmhosts, wscsvc
svchost.exe	916	AudioEndpointBuilder, CscService, Netman, PcaSvc, SysMain, TrkWks, UxSms, Wlansvc, wudfsvc
svchost.exe	948	AeLookupSvc, Appinfo, AppMgmt, BITS, Browser, CertPropSvc, EapHost, gpsvc, iphlpsvc, LanmanServer, ProfSvc, RasMan, Schedule, seclogon, SENS, ShellHWDetection, Themes, Winmgmt, wuusersv
svchost.exe	684	EventSystem, fdPHost, netprofm, nsi, SstpSvc, WdiServiceHost, WebClient
svchost.exe	1200	CryptSvc, Dnscache, LanmanWorkstation, NlaSvc, TapiSrv
svchost.exe	1572	FDResPub, SCardSvr, SSDPSRV, upnphost, wcnscvc
svchost.exe	1604	BFE, DPS, MpsSvc
svchost.exe	1708	stisvc
svchost.exe	3116	bthserv
svchost.exe	3168	PolicyAgent
svchost.exe	4152	WinDefend
svchost.exe	3340	p2pimsvc, p2psvc, PNRPsvc