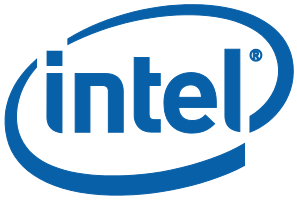


Intel® vPro™ Technology Use Case Reference Design

Enhanced Remote Repair - Registry Edits

Revision 1.1

June, 2010

Document ID: 1071

Revision History

Revision	Revision History	Date
1.0	Initial Release	February 2010
1.1	Changed name per Marketing	June 2010

Contents

1 Preface

Intel® vPro™ technology provides the ability for the help desk to perform all kinds of remote diagnostics and repair that otherwise would have taken a desk side visit. This Use Case Reference Design (UCRD) will outline how to view or edit a remote Intel vPro technology based system's registry.

1.1 Document Scope

This document describes a theory and process for viewing or editing a remote system's registry. We recommend that you follow the included procedures in your test lab and then adjust the process based on the specific needs of your production environment. Note that the process described in this document assumes you have gained access to the remote system's hard drive using the Remote Drive Share software and procedures (see 1.3, Related Documentation below). Other remote access methods may work with these steps as well, but they have not been tested as part of this document's development.

NOTE

This document assumes that readers are experienced with editing a system's registry (see Section 1.2, Intended Audience).

1.2 Intended Audience

This document is intended for Information Technology (IT) professionals who work on, manage, or develop processes for a help desk. Readers should be experienced with editing a system's registry.

Furthermore, readers should be familiar with Remote Drive Sharing (RDS), as described in the document(s) listed in 1.3, Related Documentation below.

1.3 Related Documentation

The following documents and software are required in order to perform the procedures contained in this Use Case Reference Design.

- UCRD 1040, *Use Remote Drive Sharing to Remotely Access and Repair a PC with Intel® vPro™ Technology*, available at
  http://communities.intel.com/docs/DOC-4785

2 Introduction

2.1 Example Illustrated in This Document

The steps in this document outline a lab experiment to prove the concept of editing an offline remote registry database (referred to as a “hive”). Steps include setting up the lab environment and then editing the registry hive to fix a problem. The lab example involves two computers:

Role	Requirement
Help Desk Console	• Any computer running Windows software. Remote access to the hard drive of Managed Client using Remote Drive Sharing.
Managed Client with Intel vPro Technology	• Any PC with Intel vPro Technology.

2.2 Process Overview

Once you have gained remote access to the client hard drive many tasks become possible to execute remotely. Viewing or editing an offline remote registry hive is one such task. Using Remote Drive Sharing, the remote drive is mapped to a drive letter on the Help Desk Console (see 1.3, Related Documentation on page 5). Once remote access is established, you can use the registry editor resident on the Help Desk Console to load an offline registry hive from the mapped drive.

CAUTION

Incorrectly editing the registry could damage the Management Console system or the remote Managed Client system. Before making any changes to the registry, you should back up any valued data on the Management Console and the remote Managed Client.

Phase description	The IT professional performs tasks to prepare the Help Desk Console and the Target Client for the lab experiment.
Phase prerequisites	• You have read, understood, and performed the procedures in UCRD 1040, *Use Remote Drive Sharing to Remotely Access and Repair a PC with Intel® vPro™ Technology* (see see 1.3, Related Documentation on page 5) • Remote Drive Sharing is working in the lab between the Help Desk Console and the Target Client
Phase flow	1. Using Remote Drive Share, map a drive on the management console to the hard drive of the remote client. 2. Back up the remote client’s registry on the management console. 3. Back up the local management console registry.

	4. Open regedit on the management console. 5. Load an offline hive from the mapped drive (client's hard drive). 6. Access/edit the newly loaded offline hive. 7. Unload the offline hive to save it back to the remote client.
Phase outcome	Any needed actions on the Managed Client's registry have been performed remotely from the Management Console.

3 Detailed Steps

Follow the steps in this section to load and edit offline registry databases on the mapped hard drive of the remote Managed Client. Once the Managed Client's registry databases are loaded in the Management Console's registry editor, you can perform such actions as removing items from the "Run line" among others.

The steps in this section assume that you have already mapped a drive on the Management Console to the shared hard drive on the remote Managed Client using the procedures in UCRD 1040 *Use Remote Drive Sharing to Remotely Access and Repair a PC with Intel® vPro™ Technology* (see Section 1.3, Related Documentation on page 5). Furthermore, the steps assume that drive letter Q: has been mapped to the remote Managed Client's hard drive and that the drive partition labeled "sda2" contains the client's operating system files.

NOTES

- *To perform this procedure, you must be a member of the Administrators group on the local Management Console computer, or you must have been delegated the appropriate authority. If the computer is joined to a domain, members of the Domain Admins group might be able to perform this procedure. As a security best practice, consider using* ***Run as*** *to perform this procedure. If your computer is connected to a network, network policy settings might also prevent you from completing this procedure.*
- *The* ***Load Hive*** *and* ***Unload Hive*** *commands (described below) affect only the HKEY_USERS and HKEY_LOCAL_MACHINE keys and are active only when these predefined keys are selected. When you load a hive into the registry, the hive becomes a subkey of one of these keys.*

3.1 Back Up the Remote Managed Client's Registry

In this section you will create a backup copy of the remote Managed Client's registry on the Management Console system. This is done so that you can restore the remote Managed Client's registry if you accidentally corrupt it while editing it.

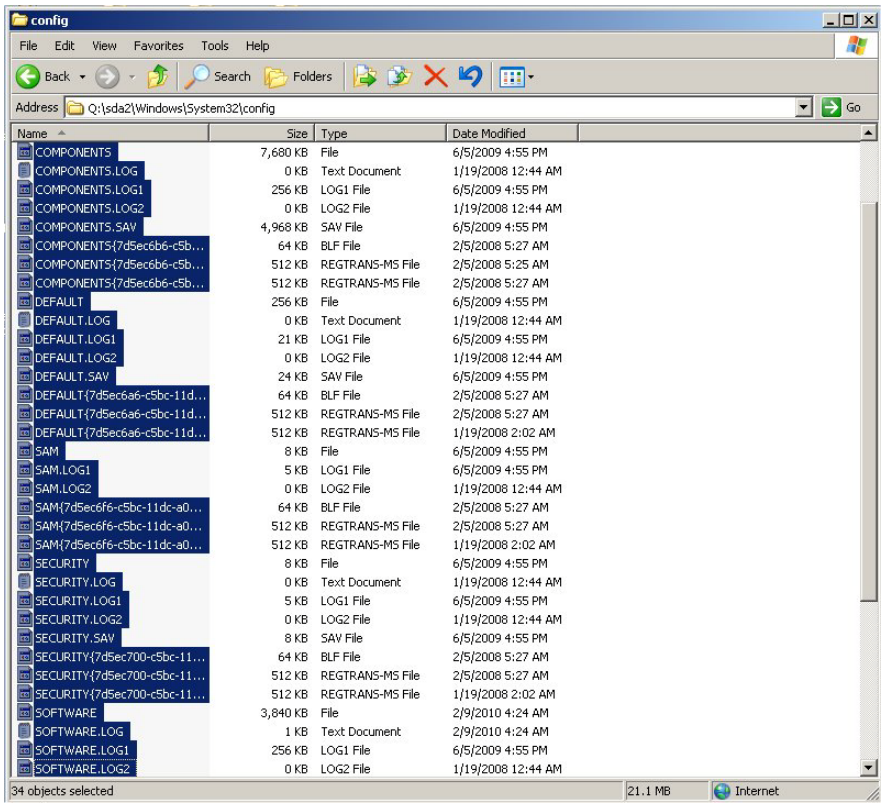
CAUTION

It is extremely important that you back up the remote Managed Client's registry as described in this section before you do anything else. If you do not do this, you may not be able to restore the remote Managed Client's registry if you corrupt it.

1. On the Management Console system, open Windows Explorer and create a new folder called C:\Remote_RegBack.j
2. In Windows Explorer, open the mapped drive to the Managed Client's hard drive (Q: in the document example) and navigate to Q:\sda2\Windows\System32\config.

This step assumes that your remote Managed Client's hard drive is mapped to drive Q: and that its operating system is installed on the partition labeled sda2.

3. Copy the following files from Q:\sda2\Windows\System32\config to your new remote registry backup folder, C:\Remote_RegBack:
   - COMPONENTS.*
   - DEFAULT.*
   - SAM.*
   - SECURITY.*
   - SOFTWARE.*
   - SYSTEM.*



The remote Managed Client's registry is now backed up on your Management Console system and can be restored if necessary.

To restore a corrupted registry on the remote Managed Client, copy the entire set of backup registry files from C:\Remote_RegBack to Q:\sda2\Windows\System32\config, thus overwriting the entire corrupted remote registry with the clean backup. Do not copy individual registry files.

3.2 Back Up the Local Management Console's Registry

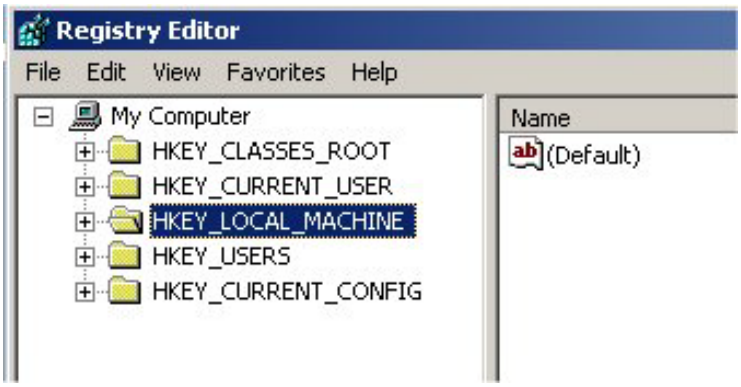
In addition to backing up the remote Managed Client's registry as described above, you should also back up your local registry for the Management Console, since you will be opening the Registry Editor on the Management Console in the next section. See the procedures outlined in the following Microsoft technical article, under the subheading "Back up the registry":

http://support.microsoft.com/kb/256986

3.3 Load a Remote Registry Database File from the Managed Client

In this section you will open the Registry Editor on the Management Console and load a registry database file (referred to as a "hive") from the remote Managed Client's registry, using the mapped drive to the client's hard drive.

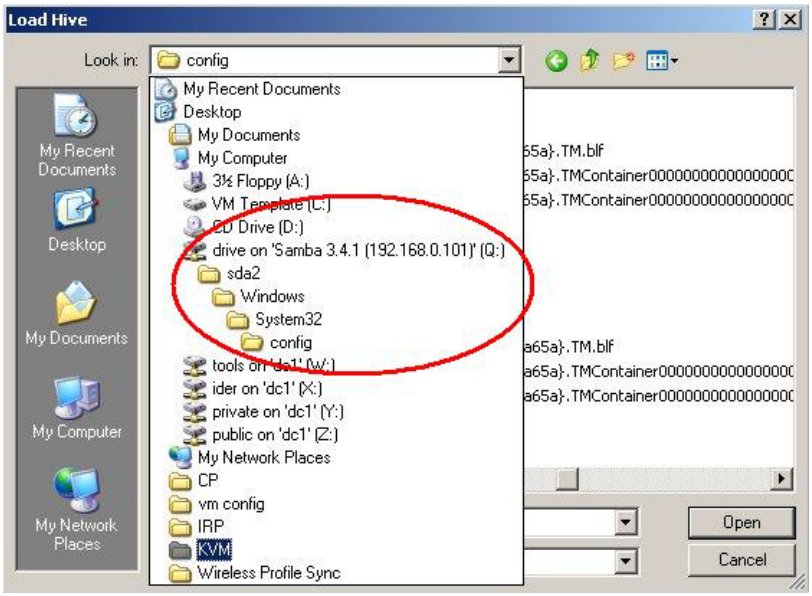
1. On the Management Console, open the Registry Editor as follows: click **Start** > **Run**, then type **regedit** and click **OK**.
2. In the registry tree (in the left-hand pane), select either HKEY_USERS or HKEY_LOCAL_MACHINE. In the document example we select HKEY_LOCAL_MACHINE.

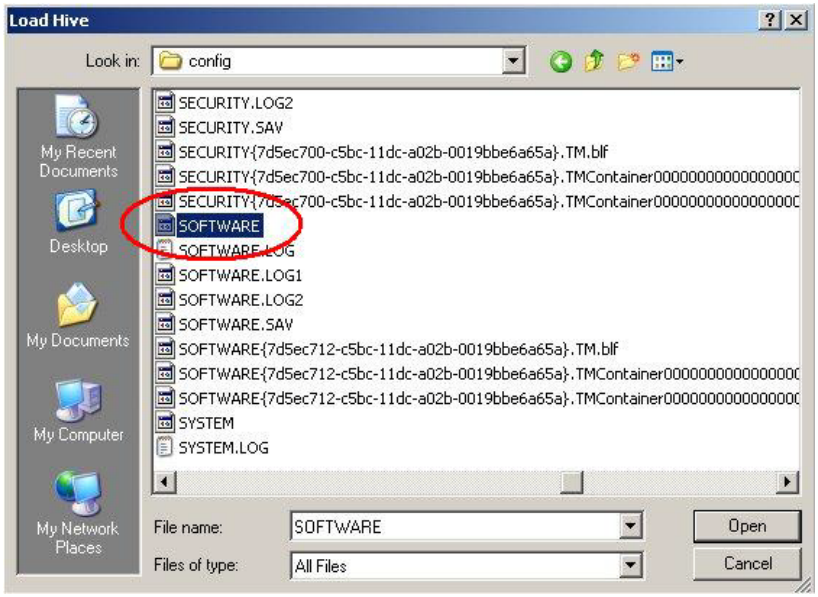


3. On the menu bar, click **File** > **Load Hive**.

4. In the **Look in** field of the Load Hive dialog, select the drive, folder, or network computer and folder combination that contains the hive you want to load.

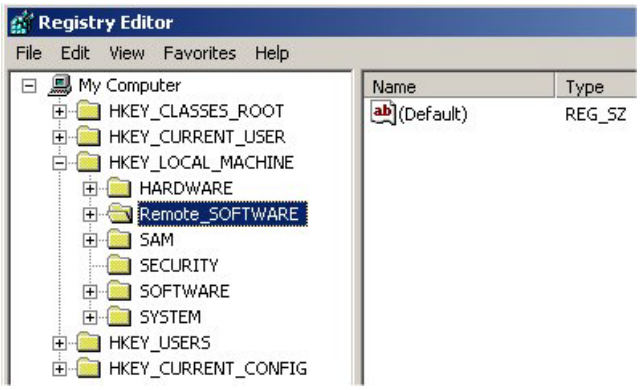
   In the document example, we want to load [HKEY_LOCAL_MACHINE \SOFTWARE] (%windir%/system32/config/SOFTWARE) from the remote Managed Client machine. This hive is located in Q:\sda2\Windows\System32\Config\SOFTWARE (no file extension), assuming that the Managed Client's hard drive is mapped to drive letter Q: and that the drive partition sda2 contains the Managed Client's operating system files.





Other hives you may want to load from the Managed Client are:
[HKEY_LOCAL_MACHINE \SYSTEM] (%windir%/system32/config/SYSTEM)
[HKEY_USERS \.Default] (%windir%/system32/config/DEFAULT)

5. In the Load Hive dialog, click **Open**.
6. In the **Key Name** dialog, enter the name that you want to assign to the newly loaded remote hive, and then click **OK**. Be sure to give the newly loaded remote hive a unique name such as "Remote_SOFTWARE" so that you will not confuse it with the local SOFTWARE registry key. The newly loaded remote hive is displayed in the left-hand pane of the Registry Editor, as shown below.



7. At this point you have the ability to perform remote registry edits using the newly loaded remote hive. Make changes as needed to fix the Managed Client's registry.
8. To save your changes, unload the remote hive as follows: in the left-hand pane of the Registry Editor, select the Hive Key Name (Remote SOFTWARE, in this example), then click **File > Unload Hive** on the menu bar. The changes you made to the remote hive are set in the Managed Client's local registry.
9. Exit the Registry Editor on the Management Console.
10. Disconnect the mapped drive to the Managed Client's hard drive.
11. Reboot the Managed Client to ensure that it stops sharing its hard drive.