



## SecureDisc for Rimage Technical Bulletin

2008 Jan. 21

*RE: Testing SecureDisc for Rimage in a Forced-Encryption Environment*

This document details a testing procedure for verifying the functionality of SecureDisc for Rimage in a forced-encryption environment.

A forced-encryption environment is typically configured when it is undesirable or impossible for a third party application to enable the “Recording Modifications” (sometimes referred to as “User Type”) flag in the rimage order submission API.

Forced-encryption is implemented when the Rimage Production Server is placed into a special mode, invoked through a registry switch that is changeable via registry modification (Discrete provides registry modification short-cuts for this purpose). When Production Server is in forced-encryption mode, all orders for disc production are sent through the SecureDisc for Rimage plug-in (called “ModifyDisc.dll”) for processing. Because of this forced behavior, all orders sent for production are expected to be targeted for encryption, and must comply with the requirements for encrypting an order.

The procedure below details how to test SecureDisc for Rimage in this forced-encryption environment. Discrete support provides the following file for testing:

[http://mail.discretetech.com/downloads/scd\\_test\\_prism.zip](http://mail.discretetech.com/downloads/scd_test_prism.zip)  
(15kb ZIP)

**Note:** the included label file is meant to use with a Prism printer. If you are using an Everest printer or 2000i system, please use a label template that functions properly and make a copy of it for use in this procedure.

Using the file linked above, use the procedure below to enable the forced-encryption environment and create an encrypted disc using the Rimage QuickDisc interface.

1. Download the ZIP file linked above.
2. Copy the file to the Rimage Control Center (desktop is fine).
3. Unzip (extract) the downloaded file to the desktop. It will contain four files:
  - scd\_label\_prism.btw
  - scd\_merge.txt
  - eps\_normal\_mode.reg
  - eps\_encrypted\_mode.reg
4. Open the SecureDisc for Rimage console application (Start -> Programs -> SecureDisc for Rimage -> SecureDisc Console)

5. Select the “Merge field” password option.
6. Set the merge field number to 6.
7. De-select the “Skip Header” option.
8. Click OK to exit the console.
9. From the extracted ZIP files, double-click on “eps\_encrypted\_mode.reg”.
10. Answer Yes to the “are you sure?” question.
11. Click OK to continue.
12. Open Rimage System Manager.
13. Click OK to connect to the Messaging Server. This could take up to 30 seconds for a response.
14. In the left navigation bar, select Production Server
15. Press the Stop button.
16. Answer Yes to the “Terminate recordings?” question.
17. Wait for Production Server to shut down.
18. Start Production Server by clicking on the Play button.
19. A Production Server Configuration window will be displayed during start-up. The last line of this window will say “ModifyDisc DLL is always used if present” – this indicates the forced-encryption environment is enabled.
20. Open QuickDisc (double-click on the desktop shortcut).
21. Click “New”.
22. Select the “CD” tab.
23. Click on “Data CD”.
24. Drop in any data files to test with. These files should be located on the local computer, and should fit onto a single disc.
25. Click Next.
26. From the Desktop, drag the label file (“scd\_label\_prism.btw” from the downloaded ZIP file) to the “Add the label to this area” portion of the QuickDisc window.
27. Select the merge file (“scd\_merge.txt” from the downloaded ZIP file) on the right side of the window. The file may be automatically selected for you.
28. Click Next.
29. Enter a disc title in the “Disc Title” field.
30. Click on More Settings.
31. Select “Recording” from the navigation on the left side of the window.
32. De-select “Enable recording modifications”.
33. Select “Disc” from the navigation on the left side of the window.
34. De-select “Use PowerImage”.
35. Click OK at the bottom of the window.
36. Set “Copies” to 1.
37. Click Record.

38. Open the merge file (“scd\_merge.txt” from the downloaded ZIP file) in Notepad and compare the fields to what was printed on the disc. Note that merge field number 6 was not printed because it was used as the encryption password, and was blanked during processing.
39. Place the disc into a standard PC and check for readability. If the SecureDisc client IS installed, you will be prompted for a password (field 6 from the merge file). If the SecureDisc client is NOT installed, the disc should be unreadable by the computer.
40. Assuming this test is successful as described in steps 38 and 39, attempt to process another test using your own merge file, changing the field values.

To return the unit to normal operating mode from the forced-encryption environment, double click on “eps\_normal\_mode.reg” and re-start Production Server.