

# WinMagic Encryption Software Installation and Configuration

Don Mendonsa, Faranak Nekoogar, Harry Martz  
Lawrence Livermore National Laboratory  
Livermore, CA 94551

Work performed on the  
Science & Technology Directorate of the  
Department of Homeland Security  
Statement of Work  
PR RSEN-08-00066

September 29, 2009  
LLNL-TR-419263



 Lawrence Livermore  
National Laboratory



This document was prepared as an account of work sponsored by an agency of the United States government. Neither the United States government nor Lawrence Livermore National Security, LLC, nor any of their employees makes any warranty, expressed or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States government or Lawrence Livermore National Security, LLC. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States government or Lawrence Livermore National Security, LLC, and shall not be used for advertising or product endorsement purposes.

This work performed under the auspices of the U.S. Department of Energy by Lawrence Livermore National Laboratory under Contract DE-AC52-07NA27344.

# Table of Contents

Introduction	4
Installation steps	4
Post boot and configuration wizard	4
Encrypting data	6
Fixed Disk Encryption	6

## Introduction

This document describes the steps needed to install and configure the WinMagic Encryption software. This software should be installed on 'the' server that data will be copied to and from for the use of transporting data between sites. File included with these instructions are:

SecureDoc(#%#\$)Setup.exe  
Profiletest.spf  
Auto-settings.ini

These files should be copied to a folder for later use.  
The actual setup file is very long and begins and ends with naming convention indicated here.

## Installation steps

double click the **setup (long file name)**  
click **next**  
click accept and **next**  
click accept and **next**  
user name click **next**  
location press **next**  
click **install**  
click **finish**  
click **yes** to reboot

## Post boot and configuration wizard

The configuration wizard will start automatically, prior to letting you login to windows.

click **next**  
make sure it's no and **next**  
key file name 'what ever' and click **next** to create (you can take the default)  
click **yes** to create new key file  
create user ID: shared user ID – This will be a shared user. Make it generic and document the user ID and password to make available to anyone who uses the system  
    create user ID for everyone to use  
    create password  
    confirm password  
    click **next**

Confirm password again and click **next**  
key file success full click **ok**  
create key, add name in key name and click **generate**  
AES (key name) click **next**  
click **next** to skip  
emergency disk , click no and **next**  
click **next**  
click **finished**  
click **ok**  
click **ok**  
click **ok** to reboot  
click **ok** again

### **System Restarted**

upon boot  
input the user ID you created: '**user name**'  
input password created for user id  
logon to windows  
click **ok** on disk not encrypted  
put password in to login to the control center  
click on '**customize**' tab  
click on the '**import**' button – browse to the profile file and click open  
upon 'profile imported successfully' click **ok**  
**exit** control center  
copy the 'auto-settings.ini' to "**C:\Program Files\WinMagic\SecureDoc-NT\**"  
click **start, run** and input cmd  
go to c:\program files\winmagic\secoredoc-nt  
type 'sdbat.exe auto-settings.ini' and press enter (do not include the quotes)  
**exit** command window  
Reboot server

### **System Restarted**

input the user ID you created: '**user name**'  
input password created for user id  
logon to windows  
reboot one more time

### **System Restarted**

windows login should appear  
system ready to use

## Encrypting data

NOTE: If you have a USB attached disk that windows sees as another hard drive and not removable media follow the steps labeled fixed disk encryption

To encrypt data on 'removable' drives USB / CD /DVD etc. start windows explorer and navigate to drive.

**Right click** on drive and select '**encrypt media**'

Check 'Encrypted media can be accessed with a password' and click **ok**

Confirm encryption, click **yes**

Input password and confirm then click **ok**

NOTE: This process could take a while, larger disks will take significantly longer.

## Fixed Disk Encryption

**Right click** on the system tray icon for secure doc and select 'SecureDoc Control Center'

Click **ok** for disk not encrypted

Input password to login to the control center

Select the 'boot control' tab

Click 'install / uninstall boot logon'

Click 'install boot logon'

Make sure disk 2 is checked and click **ok**

**Exit** control center and disk should be available for encrypting

NOTE: make sure at least 5 megabytes of sequential disk space is available prior to this step