Becrypt
DISK Protect Enhanced

Secured by RSA Implementation Guide for SecurID Authenticators

Last Modified: December 3, 2013

Partner Information

Product Information	
Partner Name	Becrypt Ltd
Web Site	www.becrypt.com
Product Name	DISK Protect Enhanced
Version & Platform	4.1
Product Description	DISK Protect Enhanced is a software security solution for Laptop and Desktop computers running Windows Operating Systems.

#becrypt

Solution Summary

Becrypt DISK Protect Enhanced and the RSA Authenticators combine to provide end-users with a single form factor for enterprise-level two-factor authentication. Users can store the necessary keys to unlock the encrypted data on their hard drive on the same device used to provide RSA SecurID authentication throughout the organization.

Partner Integration Overview	
Interoperable through RSA Authentication Client	Yes
Pre-Boot Authentication	Yes
If Pre-Boot, which tokens are supported?	RSA SID800 Rev D4

Product Configuration for Interoperability

Interoperability between the RSA Authenticators and Becrypt DISK Protect Enhanced requires the installation of the RSA Authentication Client and Becrypt DISK Protect Enhanced.

Before You Begin

This section provides instructions for integrating RSA Authenticators with Becrypt DISK Protect Enhanced. The document is not intended to suggest optimum installations or configurations.

It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

All vendor products/components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

RSA Authenticator Configuration

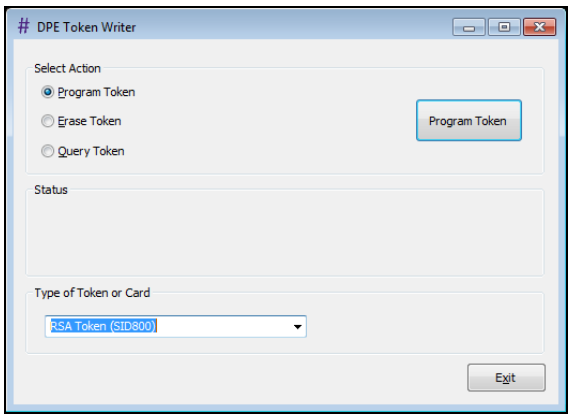
Before attempting Becrypt DISK Protect Enhanced installation, please ensure you have properly installed the correct RSA Authenticator drivers. Please consult the appropriate RSA documentation for driver installation details.

If RSA Security Middleware such as the RSA Authenticator Client is to be used, it can be installed independently of the Becrypt DISK Protect Enhanced product.

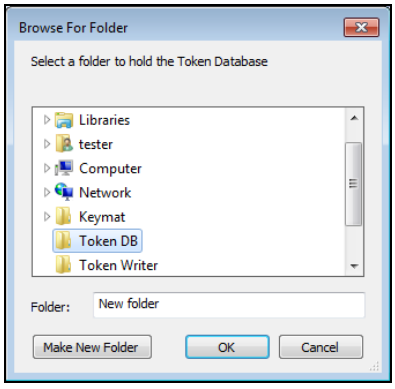
Becrypt DISK Protect Configuration

The following instructions outline the procedure for placing the keys on the smartcard and enabling the SecurID 800 at pre-boot. Instructions assume the workstation has RSA middleware installed. Refer to Becrypt documentation for specific instructions and deployment scenario.

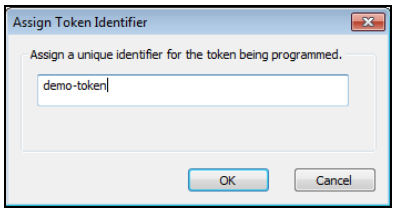
1. Run the token programming application, select **RSA Token (SID800)** and click **Program Token.**



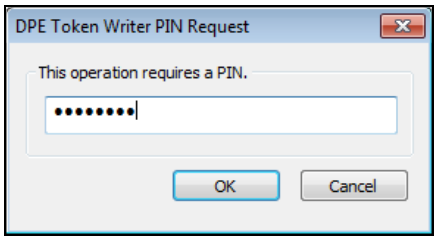
2. Select or create a new folder to save key log files and click **OK.**



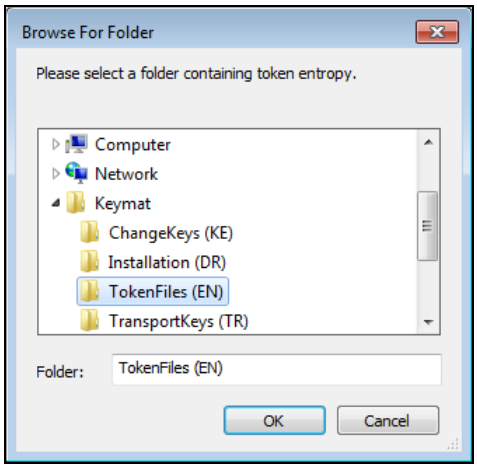
3. Enter a token label and click **OK.**



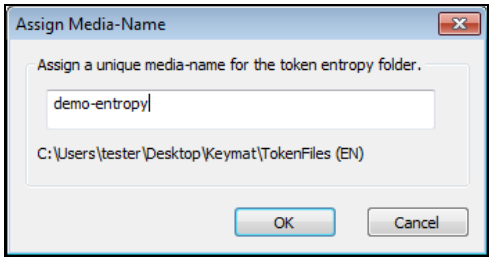
4. Confirm the token PIN and click **OK.**



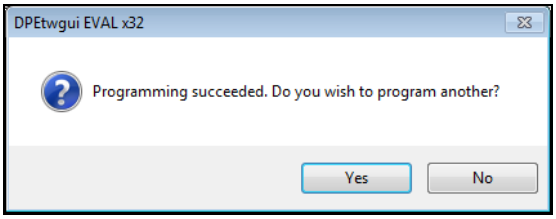
5. Locate the folder with the token Entropy and click **OK.**



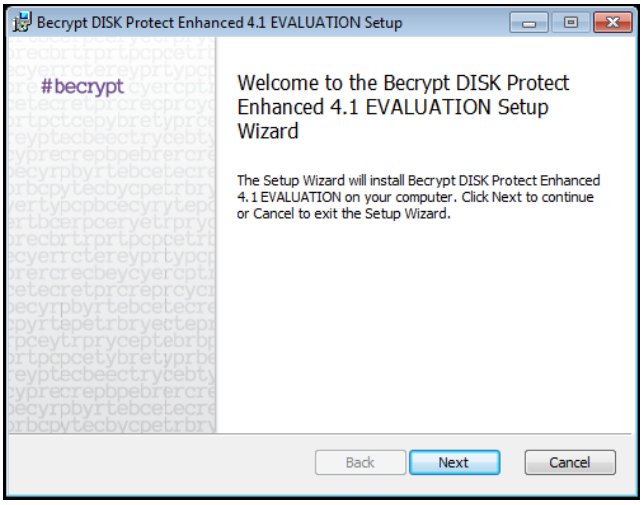
6. Enter a name to help identify the token and click **OK.**



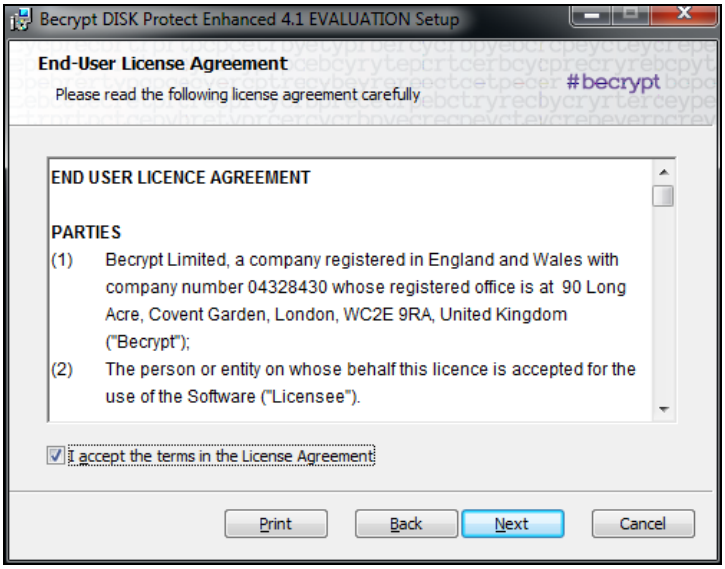
7. Select **No** to complete token programming.



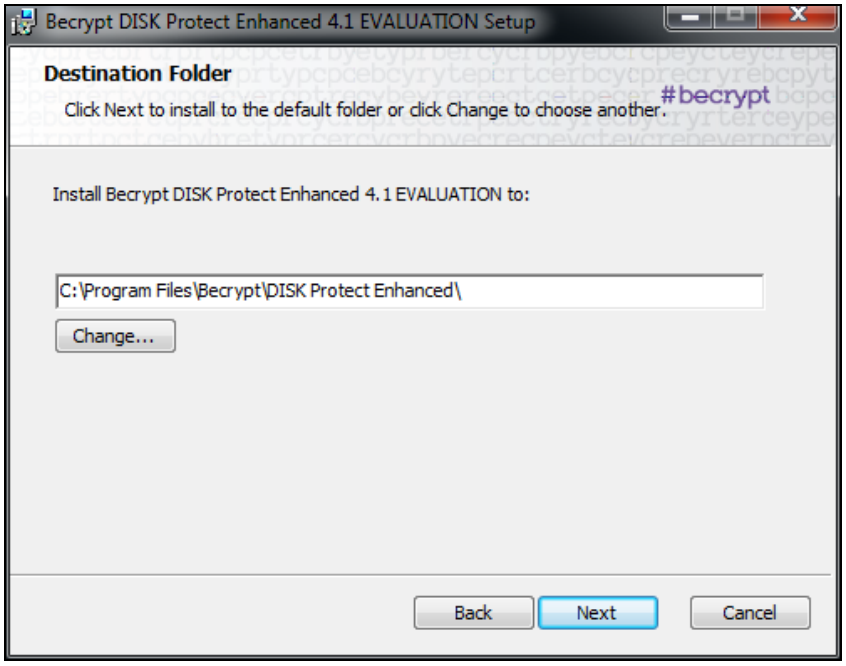
8. Launch the **Becrypt DISK Protect Enhanced msi** and select **Next** to begin installation.



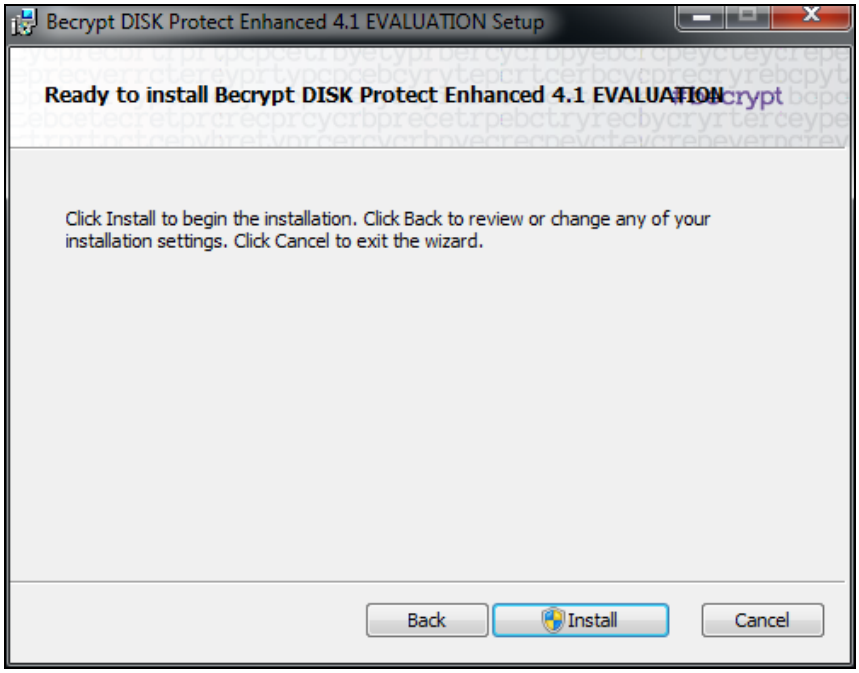
9. Accept the software license agreements terms and select **Next** to continue.



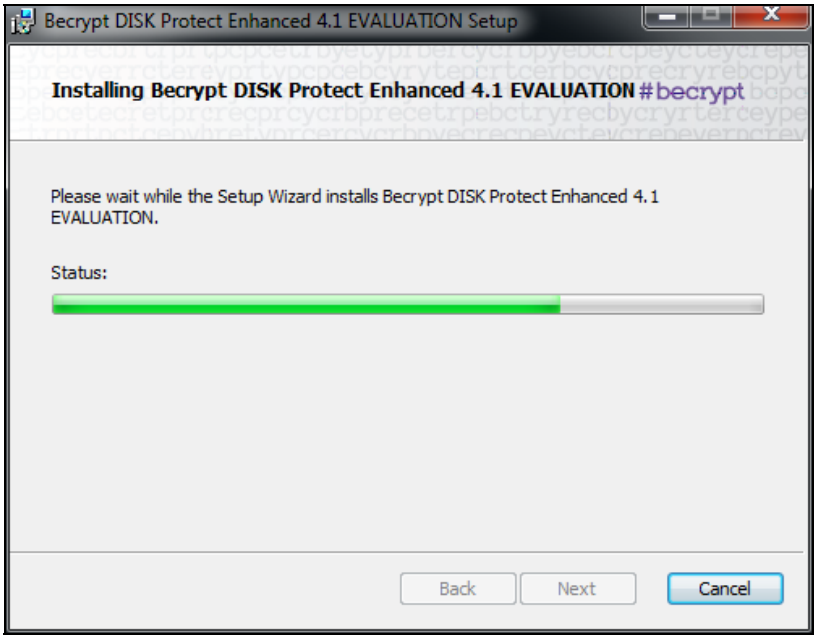
10. Confirm the installation location and select **Next** to continue.



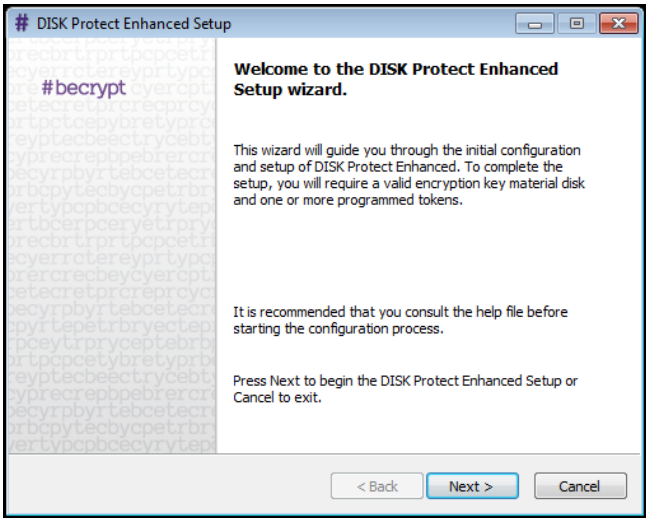
11. Select **Install** to begin.



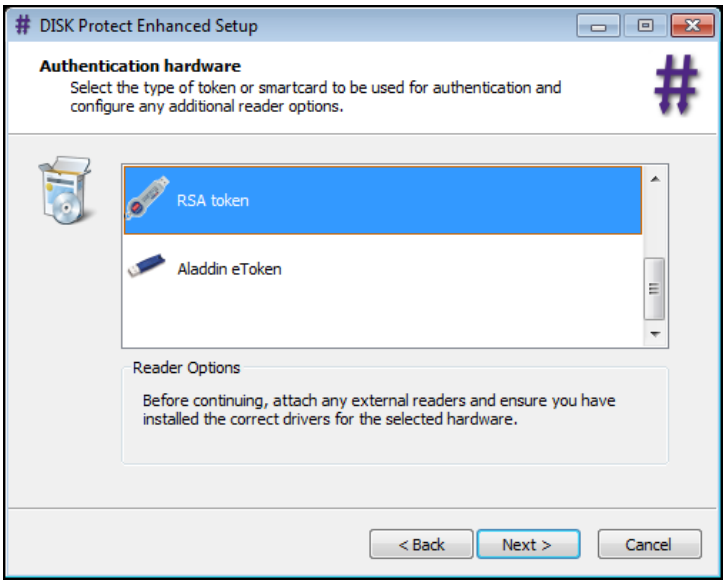
12. The application will begin the installation process.



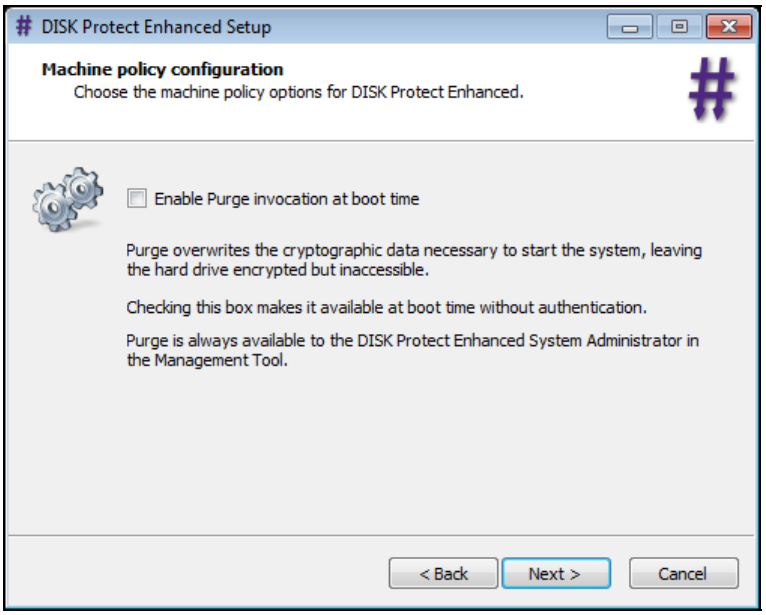
13. Select **Next** to configure Becrypt DISK Protect Enhanced.



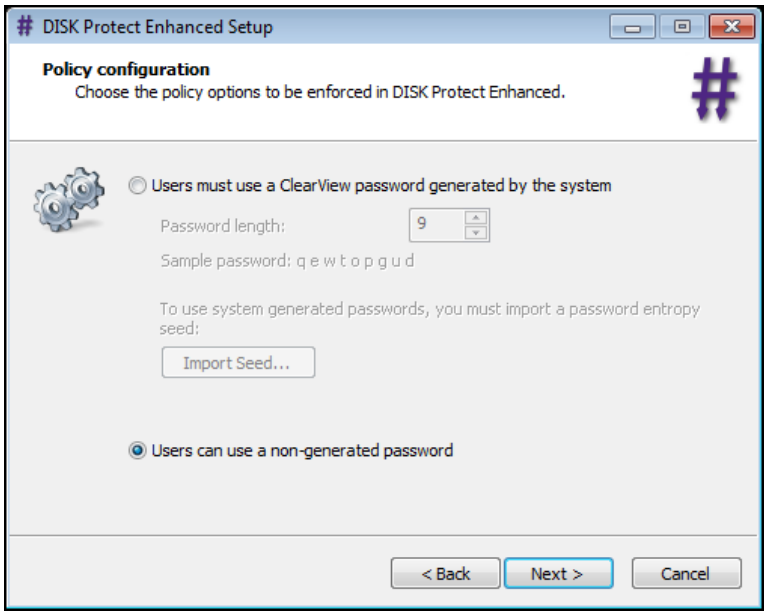
14. Highlight **RSA Token** and select **Next** to continue the setup.



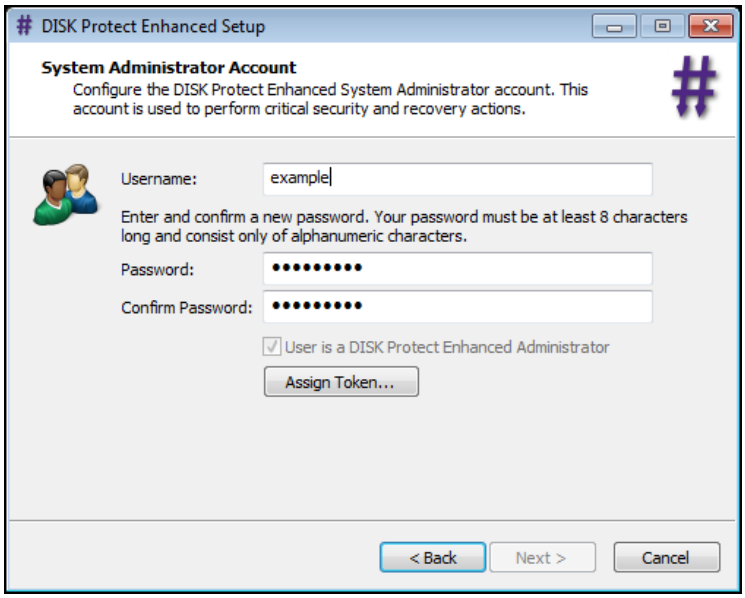
15. Select **Next** to continue.



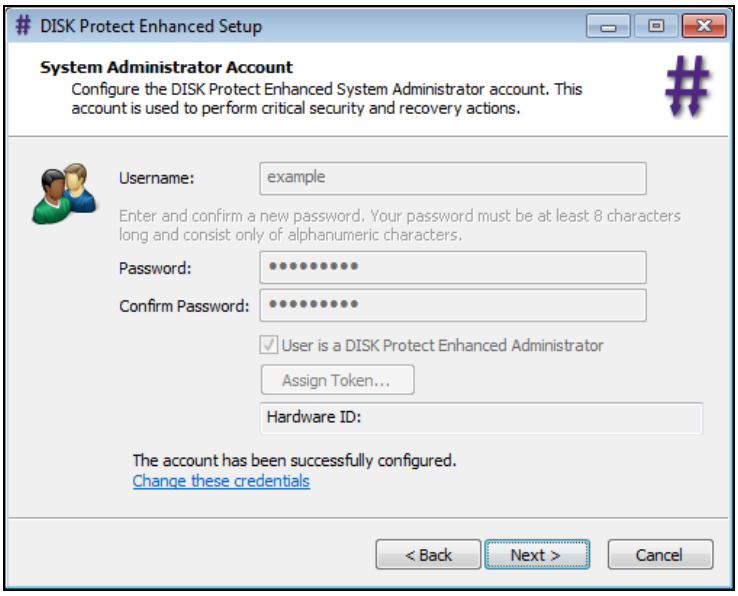
16. Change the password settings if required. Select **Next** to continue.



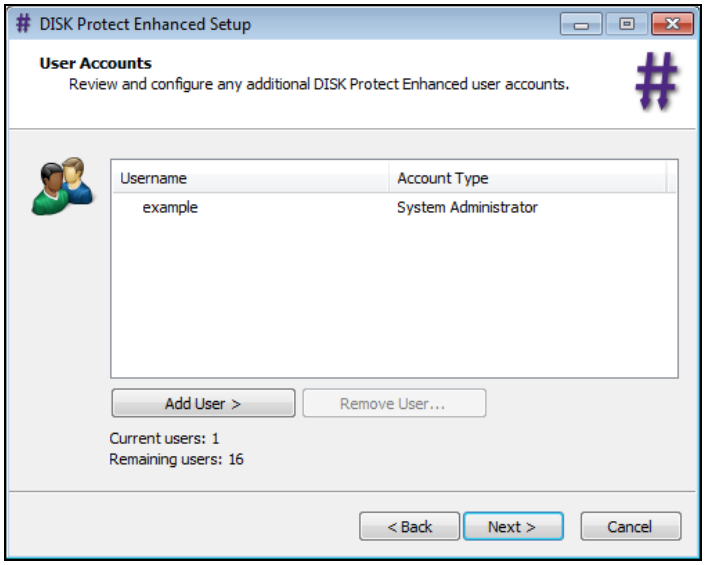
17. Enter the token username set during token programming and enter a password. Select **Assign Token…** then select **Next** to continue.



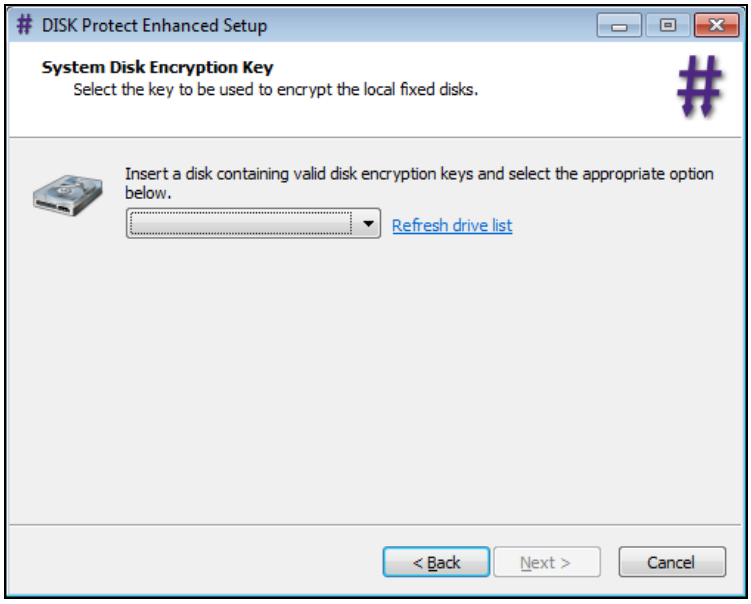
18. Select **Next** to continue.



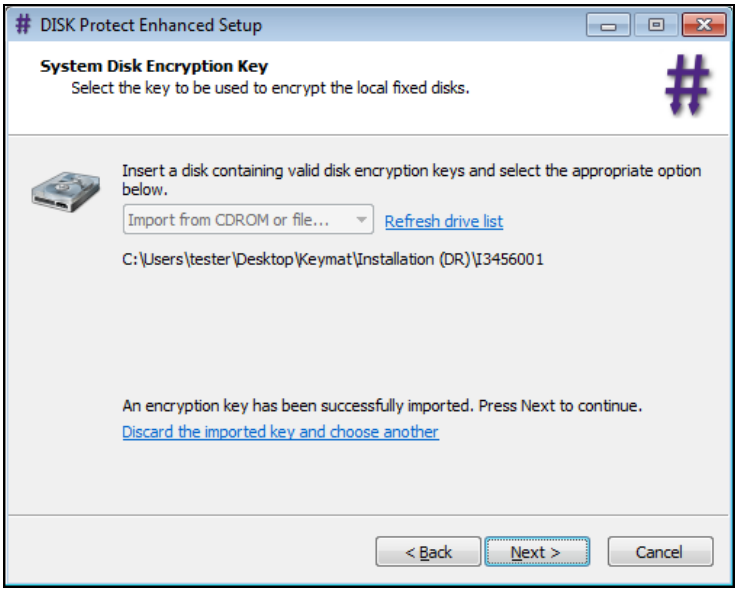
19. Add additional accounts if needed, and select **Next** to continue.



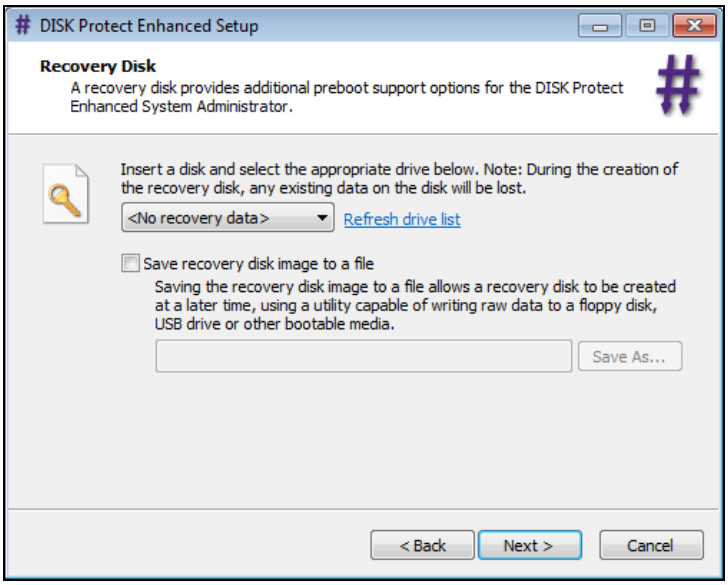
20. Select the location of your encryption key file and browse to the file.



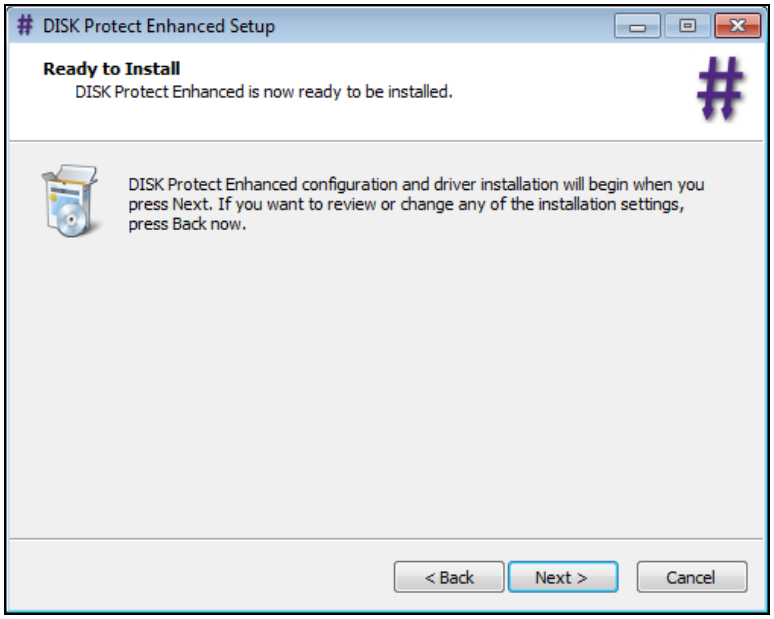
21. Select **Next** to continue.



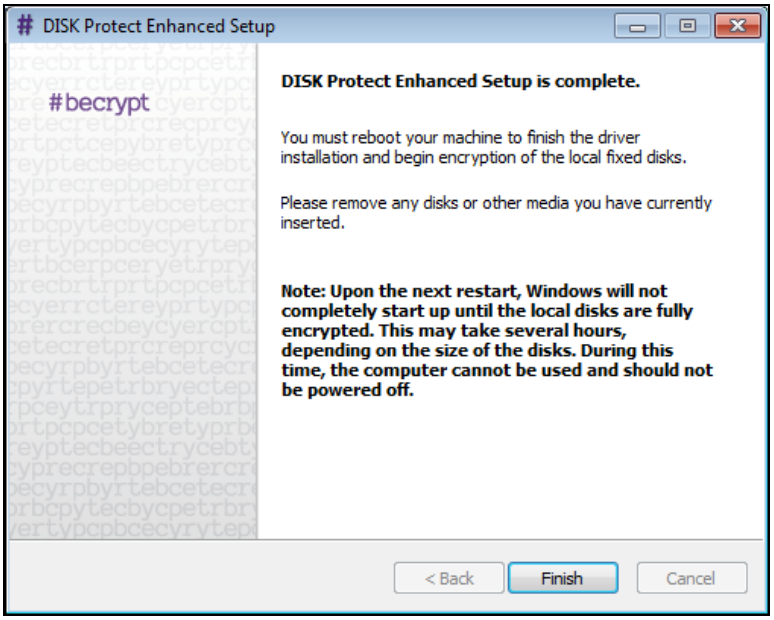
22. Select **Next** to continue.



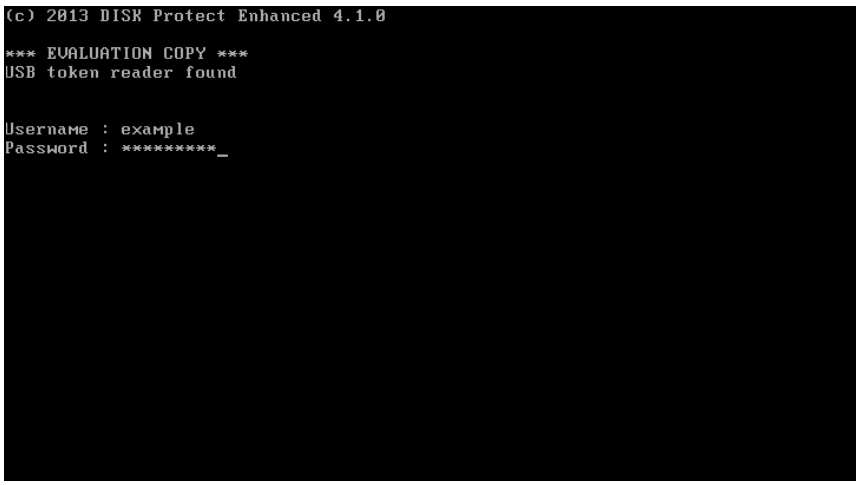
23. Select **Next** to continue.



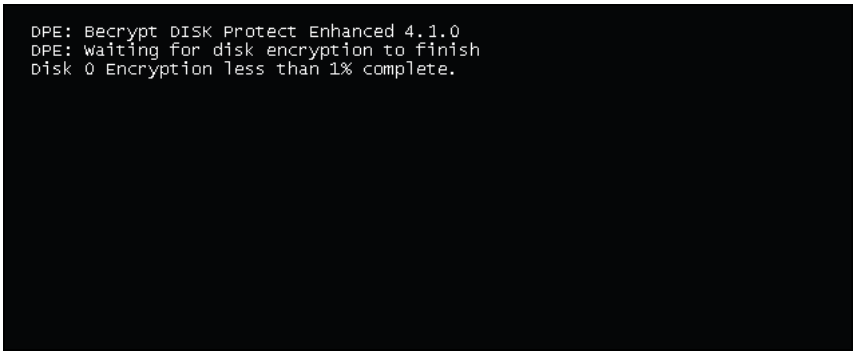
24. Select **Finish,** to reboot the system and complete the installation. The initial reboot will install DISK Protect, and all subsequent boots will require the RSA SID800 smart card, Username and Password to access the disk.



25. With the token attached, enter the username and password to load the OS.



26. The OS will load once all internal disks have completed encryption.



Certification Checklist for 3rd Party Applications

Date Tested: December 3, 2013

Product	Tested Version	Operating System
RSA Authentication Client	3.6	Windows 7
Becrypt DISK Protect Enhanced	4.1	Windows 7
RSA SecurID 800	D4	Proprietary

Test Cases	Symmetric Keys	Asymmetric Keys
RSA SecurID 800		
Preboot Authentication	✓	N/A
Disk/File Encryption	✓	N/A
1024 Certificate	N/A	N/A
2048 Certificate	N/A	N/A
Write Key/Certificate	✓	N/A
Delete Key/Certificate	N/A	N/A
Token Management		
RAC API		
Modify Token PIN	N/A	N/A
Verify Token PIN	N/A	N/A
Initialize Token	N/A	N/A

DRP/PAR

✓ = Pass ✗ = Fail N/A = Non-Available Function