Sophos
SafeGuard

Secured by RSA Implementation Guide for SecurID Authenticators

Last Modified: April 5, 2013

Partner Information

Product Information	
Partner Name	Sophos
Web Site	www.sophos.com
Product Name	SafeGuard Enterprise
Version & Platform	6.01
Product Description	SafeGuard Enterprise Device Encryption module provides sector based hard disk encryption combined with secure pre-boot authentication. The module provides transparent encryption to protect the confidentiality of data stored on hard disks and removable media.
Product Category	Disk/File Encryption

Solution Summary

SafeGuard Enterprise uses the RSA Security SID800 Token to perform a two-factor pre-boot authentication and to derive the disk (media) encryption key from data stored on the token.

For pre-boot authentication the token is accessed directly via low-level communication, without the use of any RSA middleware. Low-level communication is achieved by the implementation of the following two software components:

- Sophos built and supported 16bit real-mode CCID driver developed to support the “reader part” of the token.
- Sophos developed interface to the SID800 “smartcard” via APDU (Application Protocol Data Unit) commands to access the private container applet.

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

Product Configuration for Interoperability

Before You Begin

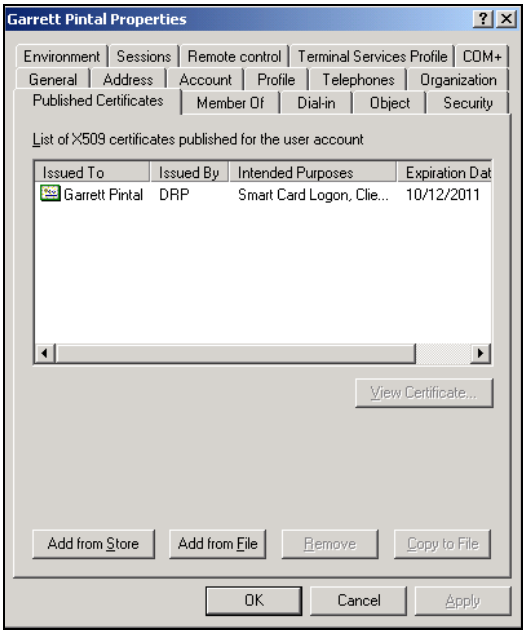
This section provides instructions for integrating RSA Authenticators with SafeGuard Enterprise. The document is not intended to suggest optimum installations or configurations.

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.

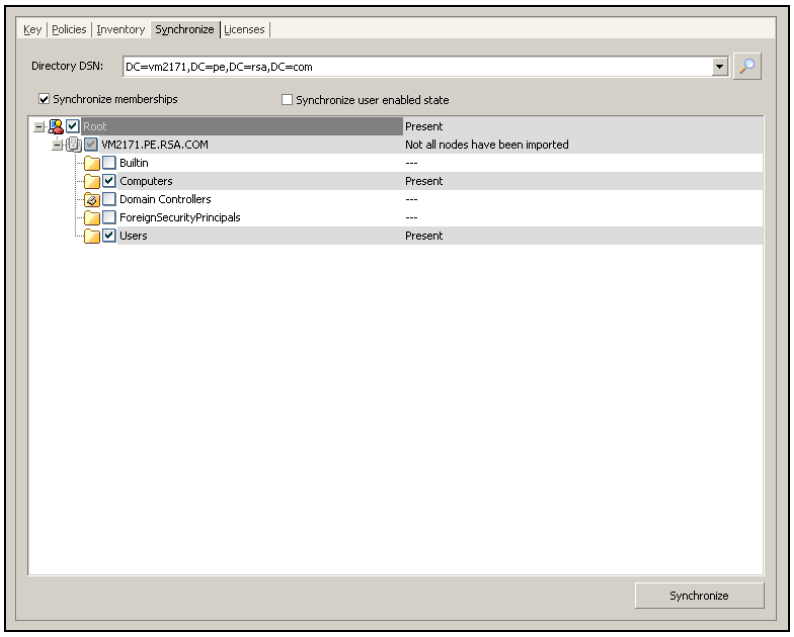
All vendor products/components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

Implementing the Solution

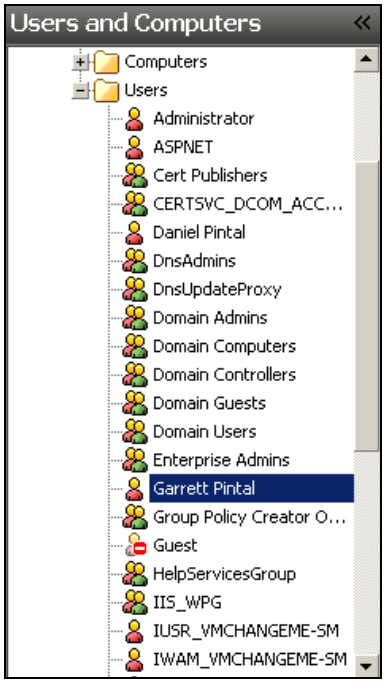
1. Interoperability between the RSA Authenticators and SafeGuard Enterprise requires the installation of the RSA Authentication Client and SafeGuard Enterprise.
2. To begin the user will need to provision the RSA SecurID 800 token with a certificate from the Windows Domain CA. Once the token is provisioned the certificate will be associated with the Users Profile within Active Directory.



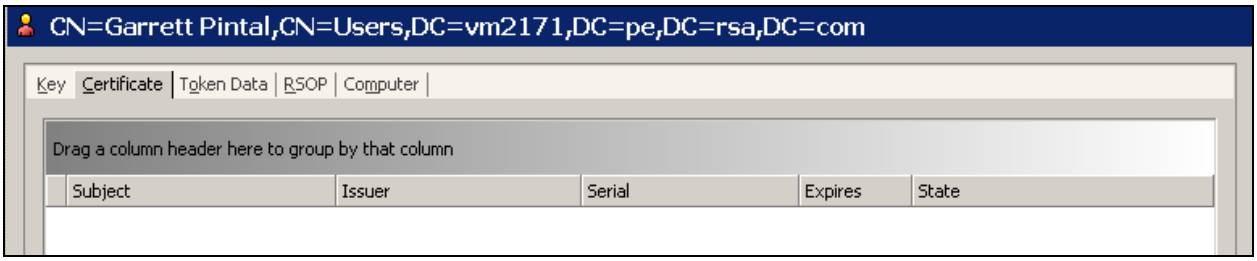
3. Perform a SafeGuard Directory Synchronization to insure that SafeGuard Enterprise has the most current information related to the Microsoft Active Directory.



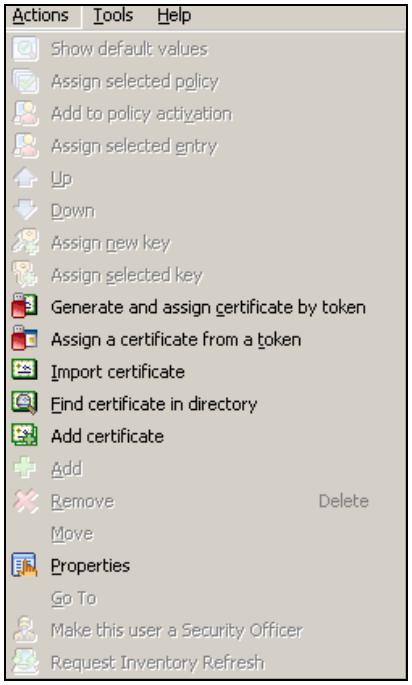
4. From the **User and Computers** drop down list select the user account to be associated with Sophos Enterprise.



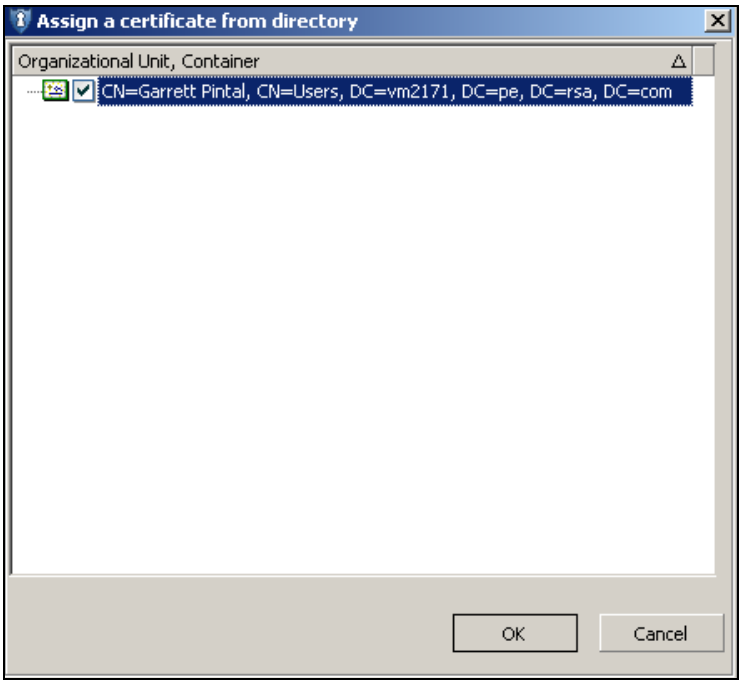
5. Select the **Certificate** tab within the Sophos Enterprise Management Center.



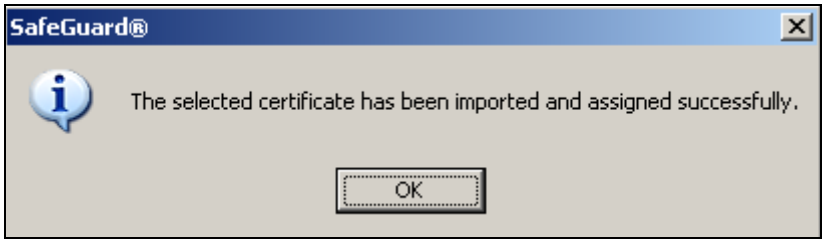
6. Assign the new certificate to the user, from the SafeGuard Enterprise menu select **Actions** > **Find certificate in directory**.



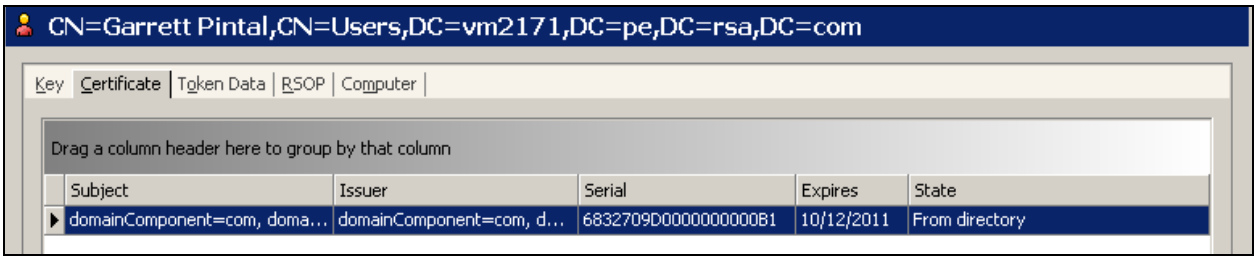
7. Select the **certificate** imported from Microsoft Active Directory and **OK** to continue.



8. Select **OK** to acknowledge the import and assignment of the certificate to the Sophos user.



9. Synchronize the client with Sophos Enterprise and reboot the client to test Pre-boot authentication.



10. With the RSA SecurID 800 token inserted during pre-boot the client will be prompted for their token PIN. When the token PIN is entered the operating system will boot as normal.

Certification Checklist for 3rd Party Applications

Date Tested: April 5, 2013

Product	Operating System	Tested Version
RSA Authentication Client	Microsoft Windows 7	3.5.7
SafeGuard Enterprise	Windows 2003 SP2	6.01
SafeGuard Client	Microsoft Windows 7	6.01
RSA SecurID 800	NA	Rev D (Sahara)

Test Cases	Symmetric Keys	Asymmetric Keys
RSA SecurID 800		
Preboot Authentication	N/A	✓
Disk/File Encryption	N/A	✓
1024 Certificate	N/A	✓
2048 Certificate	N/A	✓
Write Key/Certificate	N/A	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