Sophos
SafeGuard Enterprise

RSA Ready Implementation Guide for RSA SecurID

Last Modified: September 11, 2015

Partner Information

Product Information	
Partner Name	Sophos
Web Site	www.sophos.com
Product Name	SafeGuard Enterprise
Version & Platform	7.0
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.

Solution Summary

SafeGuard Enterprise uses the RSA Security SID800 Token to perform 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 Dx

Product Configuration for Interoperability

Interoperability between the RSA Authenticators and Sophos SafeGuard Enterprise requires the installation of the RSA Authentication Client and Sophos SafeGuard Enterprise.

Note: This integration is only supported with Windows 7. Sophos does not support the use of the RSA SID800 at pre-boot with Windows 8.x & 10 due to the use of BitLocker for disk encryption on these platforms.

Before You Begin

This section provides instructions for integrating RSA Authenticators with Sophos 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.

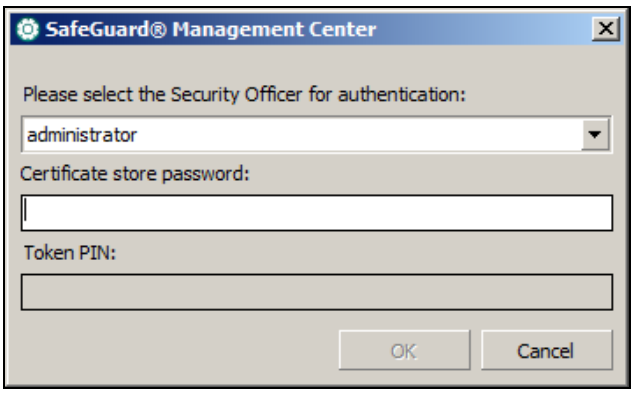
All vendor products/components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

Summary of steps

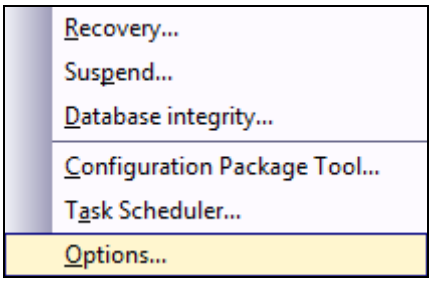
- Connect Sophos SafeGuard Enterprise to an LDAP.
- Assign user to a computer.
- Write the Sophos key or certificate to a token.
- Modify the Sophos Authentication Policy.

Connect Sophos to an LDAP

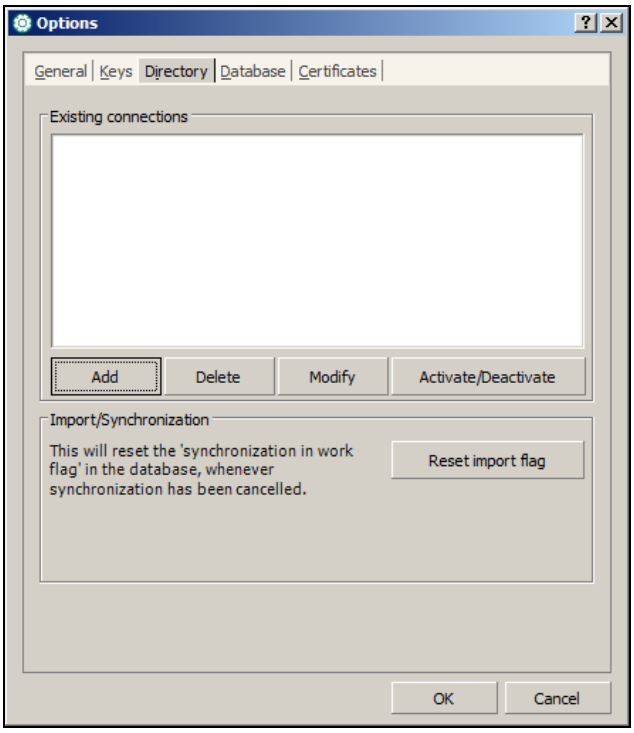
1. Login to the SafeGuard Management Center.



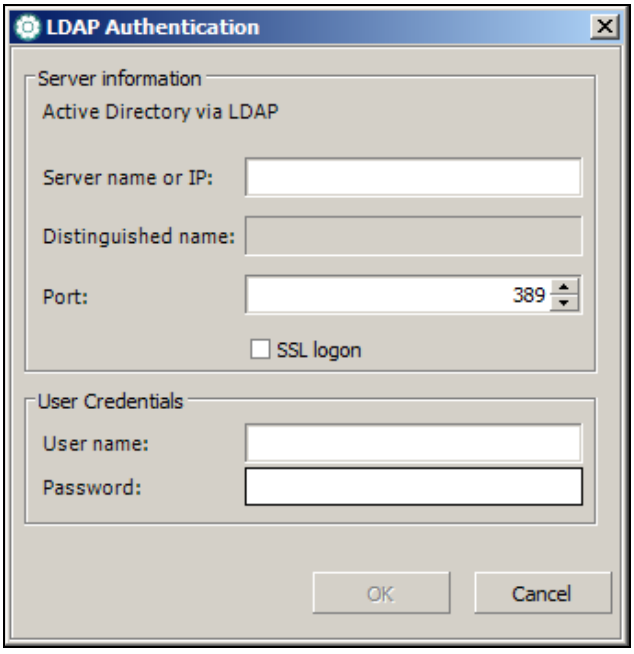
2. Select **Tools > Options.**



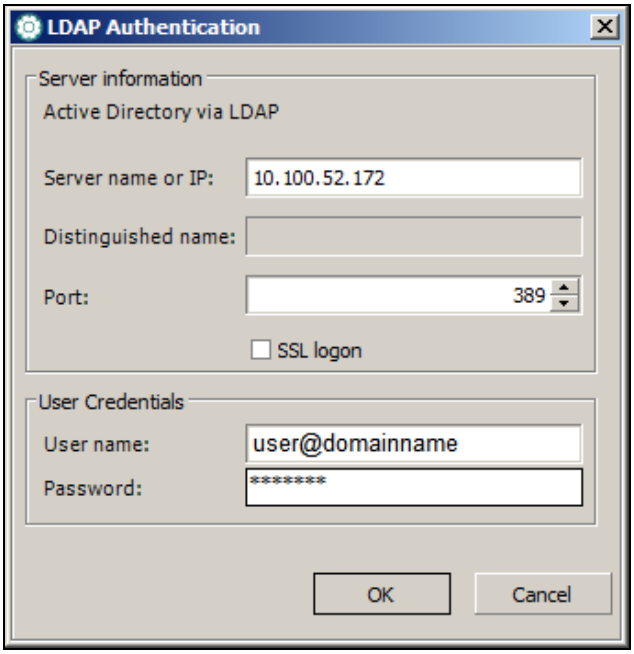
3. Select the **Directory** Tab.



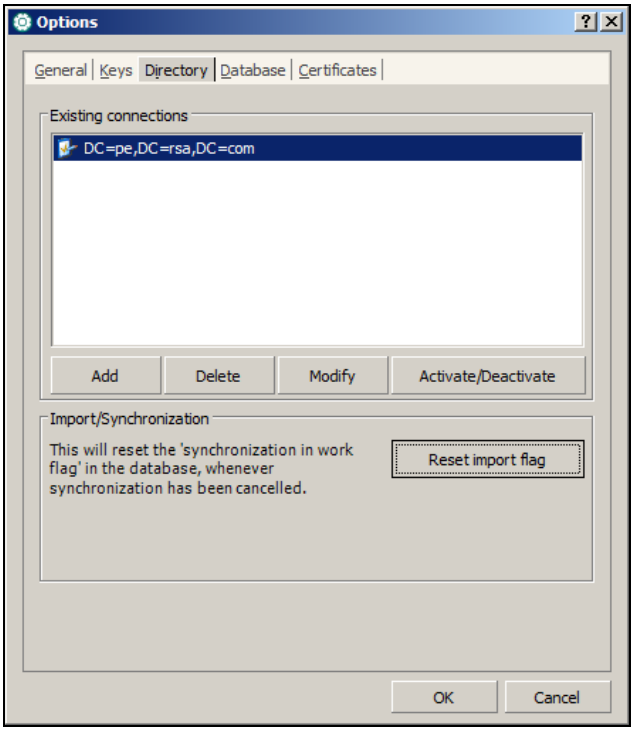
4. Select **Add** and enter the **Server name** or **IP address** and **User name** and **Password** of the LDAP.



5. Select **OK**.



6. Select **Ok** to complete the LDAP configuration.

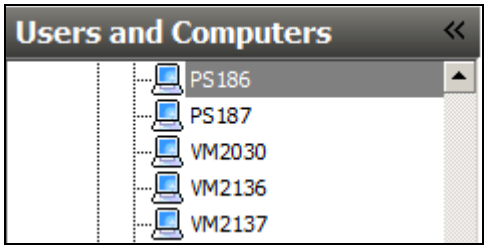


Assign a user to a computer

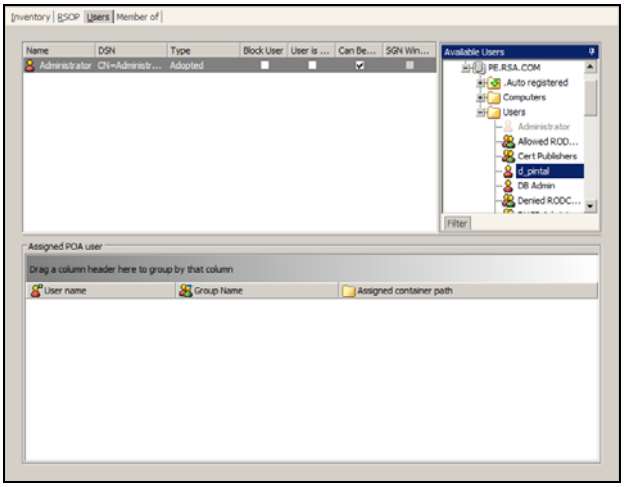
1. Select **Users and Computers**.

2. Locate the **newly registered LDAP/domain** within the list of Users and Computers.

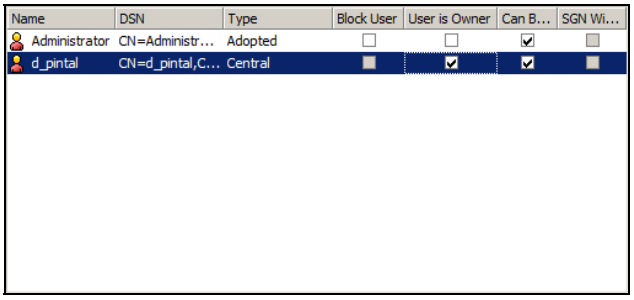
3. Within the LDAP/domain locate Computers and expand and locate the computer that you will assign a user to.



4. Locate the Available Users within the far right window frame and drag and drop a user to the Users Tab.



5. Select the **User is Owner** checkbox next to the new user account assigned to the computer.

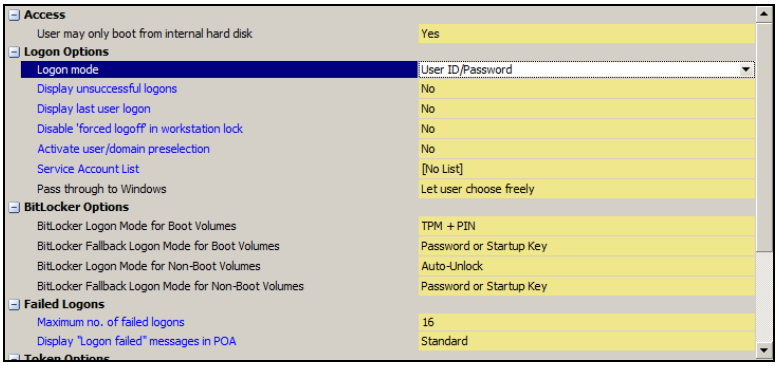


6. Select the **save** option from the SafeGuard Management Center toolbar.

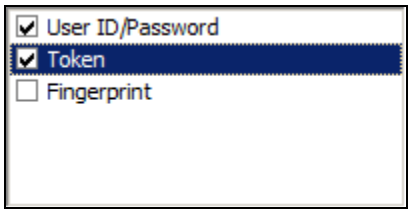
Modify default policies

1. Select **Policies** from the sidebar menu.

2. Within the Default Authentication frame, locate the **Authentication tab** and the **Logon Option**.



3. Select the drop down list for Logon mode and add **Token**.

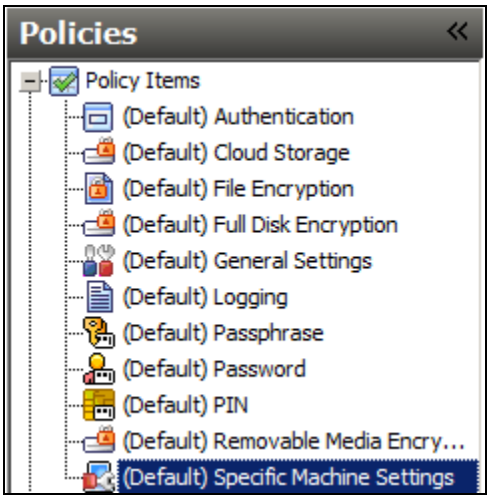


4. Select the **save** option from the SafeGuard Management Center toolbar.

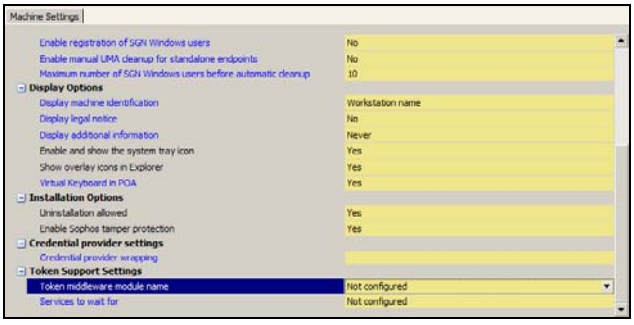
Enable RSA Smart Card Support

1. Select **Policies** from the sidebar menu.

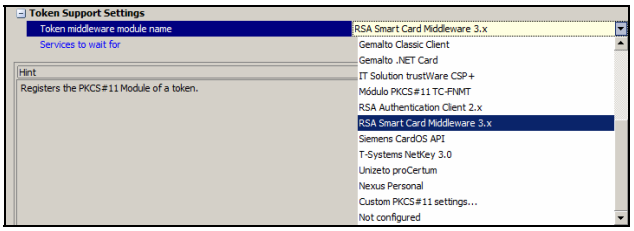
2. Select **Policy Items and (Default) Specific Machine Settings**.



3. Scroll down to the Token Support Settings within the Machine Settings Window and select **Token middleware module name**.



4. Select the dropdown for the Token middleware module name and select **RSA Smart Card middleware 3.x**.

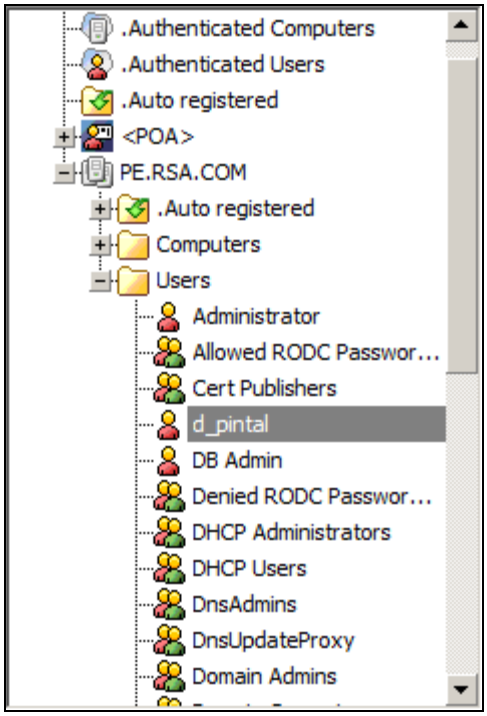


5. Select the **save** option from the SafeGuard Management Center toolbar.

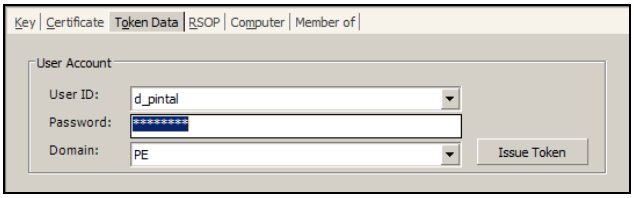
Write the Sophos key to a token

1. Insert the RSA SID800 Smart Card into the computer running the SafeGuard Management Center.
2. Select **Users and Computers** from the sidebar menu.

3. From the Users group select the user you will be assigning to the RSA SID800 smart card.



4. Select **Issue Token**.



5. Remove the token from the USB slot on the Management Center system and perform an authentication test with the user's workstation.

Note: If configuring SafeGuard Enterprise for use with certificates please contact Sophos Customer support for assistance.

Certification Checklist for 3rd Party Applications

Date Tested: September 11, 2015

Product	Tested Version	Operating System
RSA Authentication Client	3.6	Windows 2008 R2 x64 SP1
Sophos SafeGuard Enterprise	7.0	Windows 2008 R2 x64 SP1
Sophos SafeGuard Ent. Client	7.0	Windows 7 SP1
RSA SecurID 800	3.6	Windows 7 SP1

Test Cases	Symmetric Keys	Asymmetric Keys
RSA SecurID 800		
Preboot Authentication	✓	**N/A**
Disk/File Encryption	**N/A**	**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