RSA SECURID® ACCESS
Authenticator Implementation Guide

Check Point SmartEndpoint Security

Daniel R. Pintal, RSA Partner Engineering
Last Modified: January 28, 2019

RSA READY

Solution Summary

RSA Security Authenticators and Check Point Full Disk Encryption integrate seamlessly by allowing users to strongly authenticate to encrypted information on their laptop or personal computer. Authentication is configured utilizing Check Point SmartEndpoint Security Management and by associating the user with a PKI certificate stored on the RSA SecurID 800 token.

Partner Integration Overview	
Check Point SmartEndpoint Security – Full Disk Encryption E80.90	
Interoperable through RSA Authentication Client	No
Pre-Boot Authentication	Yes
If Pre-Boot, which tokens are supported?	SID800 Rev Dx

Product Configuration for Interoperability

Interoperability between the RSA Authenticators and Check Point SmartEndpoint Security FDE requires the installation of the RSA Authentication Client.

Before You Begin

This section provides instructions for configuring the Check Point SmartEndpoint Security FDE with RSA SecurID Authentication. This 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 Check Point SmartEndpoint Security FDE components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

Configuration

There is one method of RSA SID800 integration available for use with Check Point SmartEndpoint Security FDE.

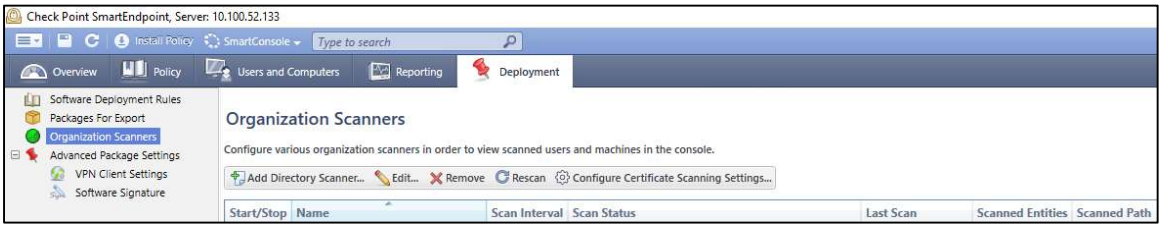
- **RSA PKI smart card** – PKI smart card authentication requires a Certificate Authority integrated with a Microsoft Windows Domain. The Certificate Authority issues the PKI certificate to a Windows Domain user. The private key is stored on the RSA SID800 smart card and associated with the Windows Domain user.

Overview

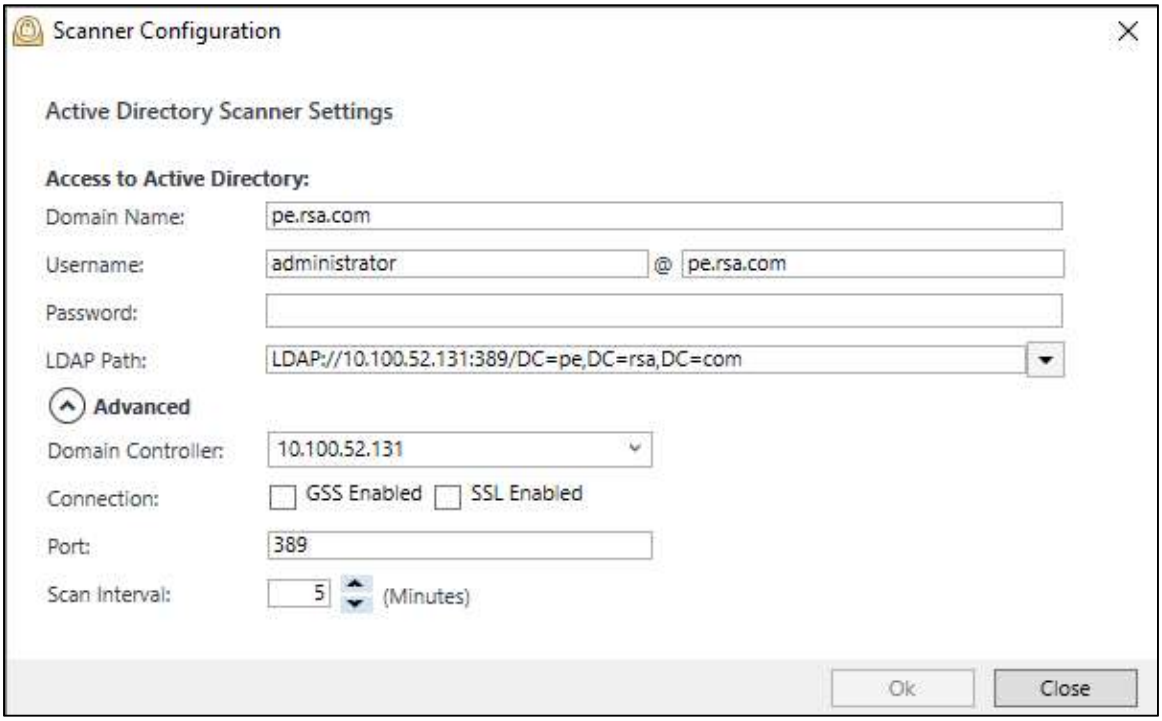
- Install Check Point SmartEndpoint Security Management Server.
- Issue a Smartcard User/Logon certificate for each user in Active Directory.
- Export the Public and Private key to a secure location.
- Use the RSA Authentication Client to write the key to the SID800.
- Use SmartEndpoint to configure a Directory Scanner to sync your Active Directory.
- Defining a policy for full disk encryption through SmartEndpoint.
- Creating a client installation package.
- Installing the client package on client PC.
- Encrypt the hard drive.

Setting up a Directory Scanner

1. Launch SmartEndpoint.
2. Select the **Deployment** tab and go to **Organization Scanners** in the left pane.



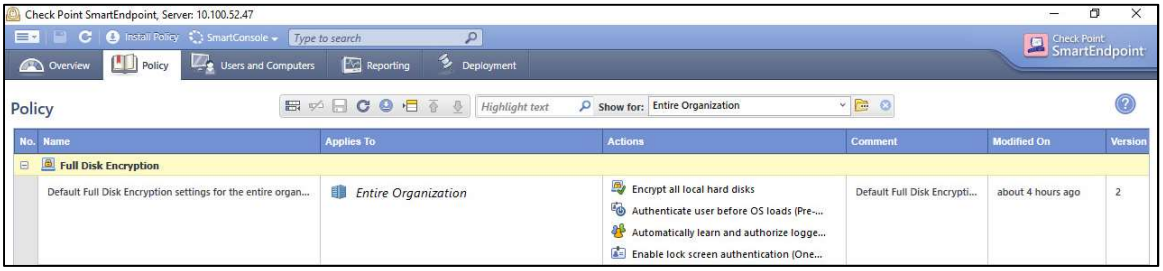
3. Click on **Add Directory Scanner**.
4. Enter the **Domain Name, Username and Password**. The LDAP Path and Domain Controller field should auto-populate.
5. Click **OK**.



6. Go to the **Users and Computers** tab to verify that scan was successful. You should now see your Active Directory structure.

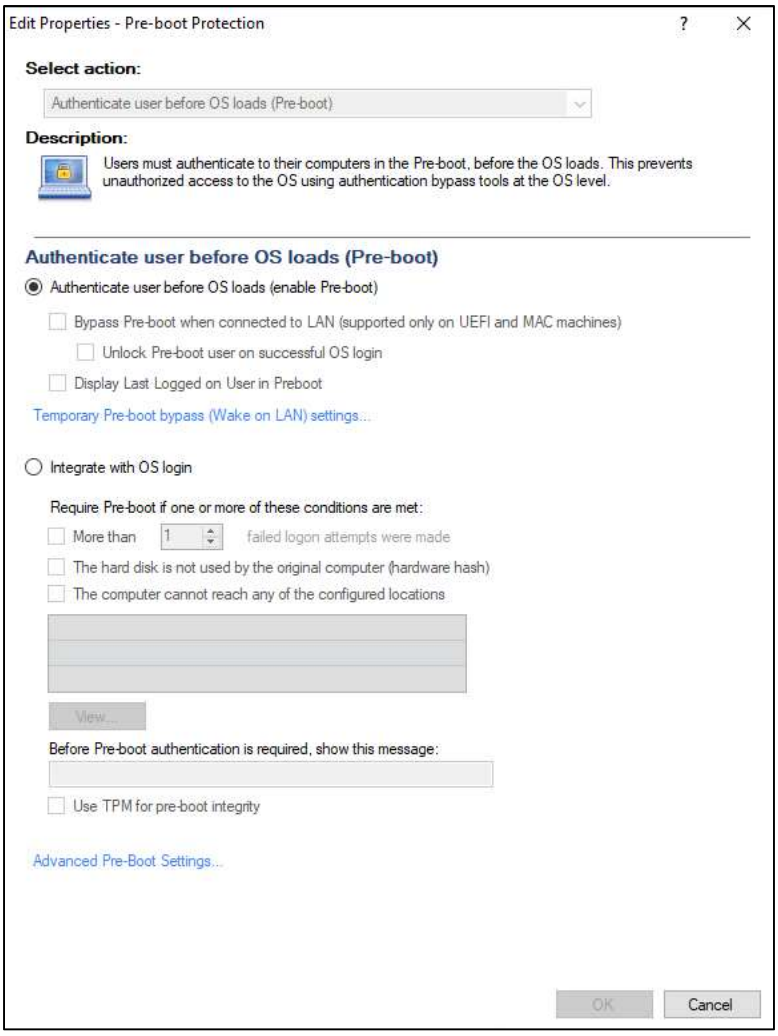
Defining a Policy for Full Disk Encryption

1. Go to the **Policy** tab.

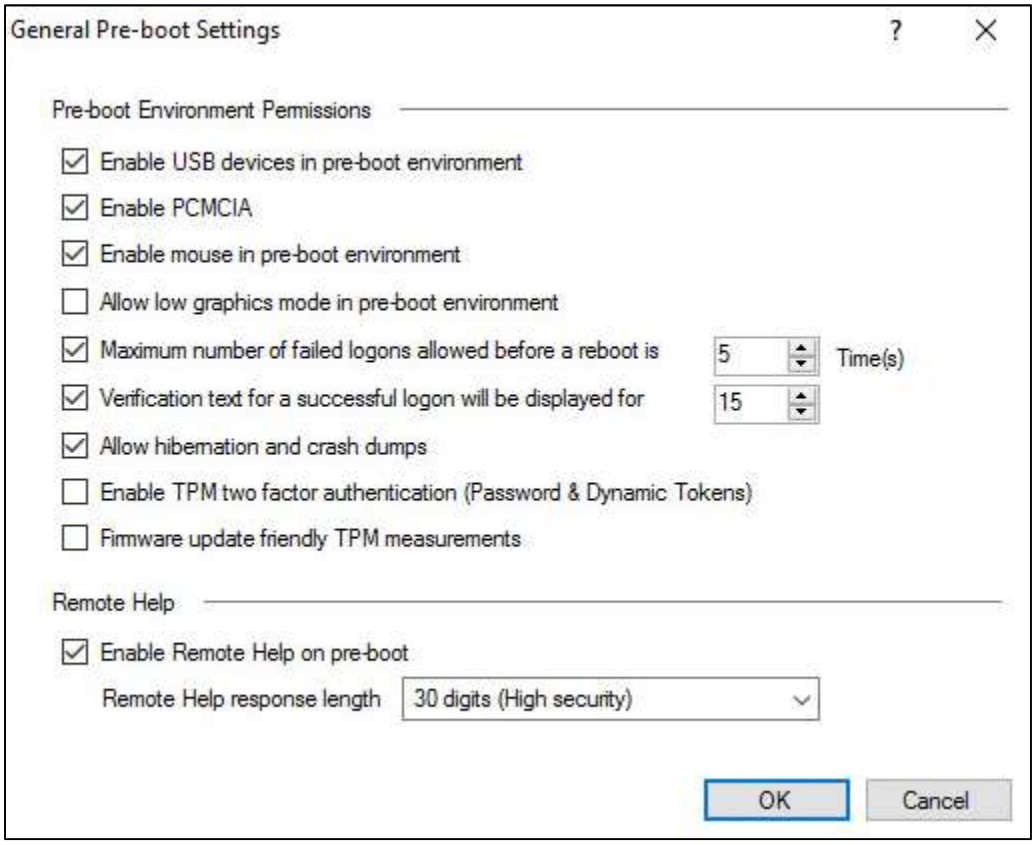


2. By default the Full Disk Encryption Policy is enabled to Encrypt all hard disks. This can be disabled if needed to get pre-boot authentication working as needed. A Policy modification can be made to encrypt the drives once pre-boot is working. Disabling encryption through the policy is not required.

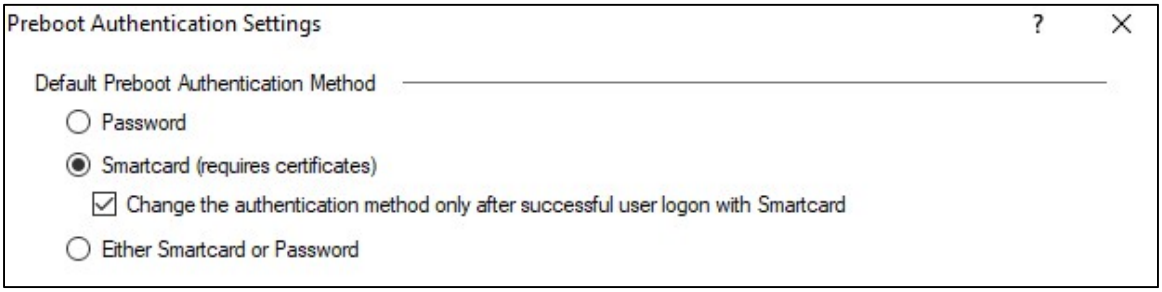
3. In Full Disk Encryption Policy rule, open the **Authenticate user before OS loads** action.
4. At the bottom of the page, click on **Advanced Pre-boot Settings**.



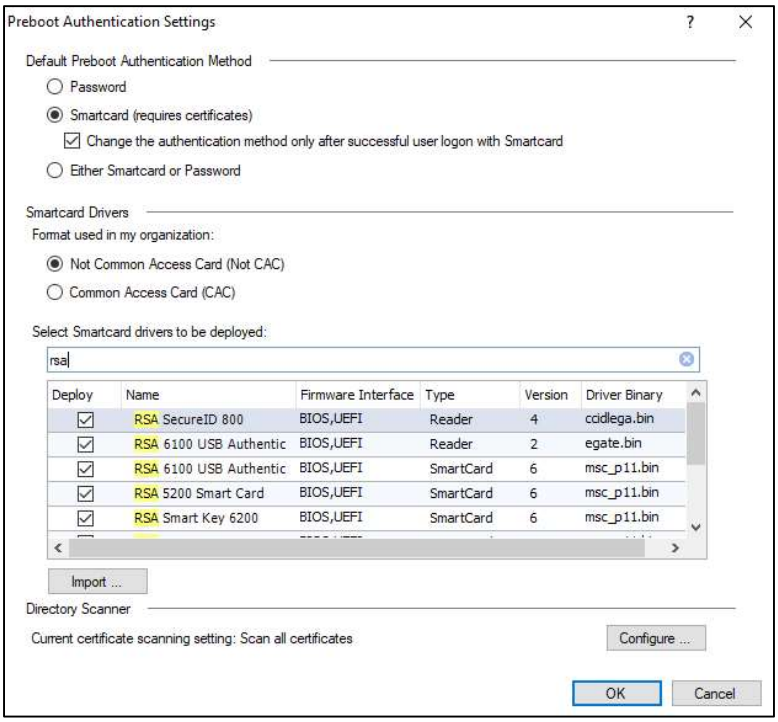
5. Select **Enable USB devices in pre-boot environment**.



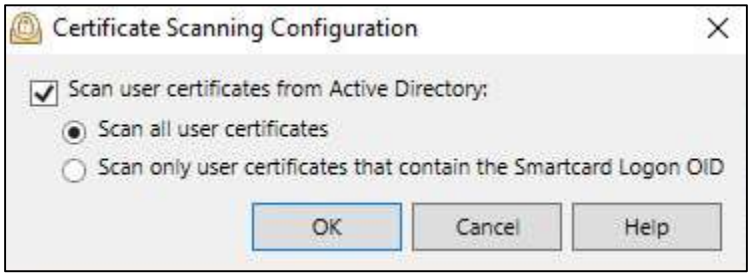
6. Click **OK** and return to the Policy tab.
7. In a **User Authentication (OneCheck)** rule, right-click the **Authenticate users** action and select **Edit**.



8. Select **Smartcard (requires certificates)**.
9. Select **Change authentication method only after user successfully authenticates with a Smart Card**.
10. Under Smartcard Drivers, search for and select the RSA drivers required for your Smartcard.
11. In the **Directory Scanner** area, click **Configure**.



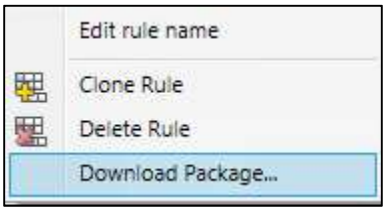
12. Select **Scan user certificates from Active Directory** and select **OK**.



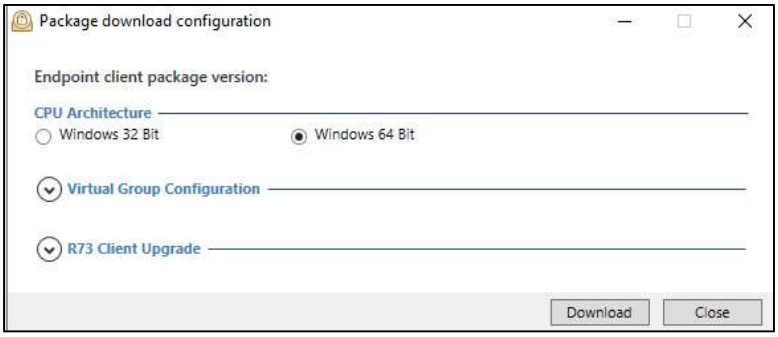
Creating a Client Installation Package

1. On the **Deployment** tab, select **Software Deployment Rules** located in the left menu.

2. Right-click the **Default Software Deployment settings** rule in the right menu and select **Download Package**.



3. Click **Download**.

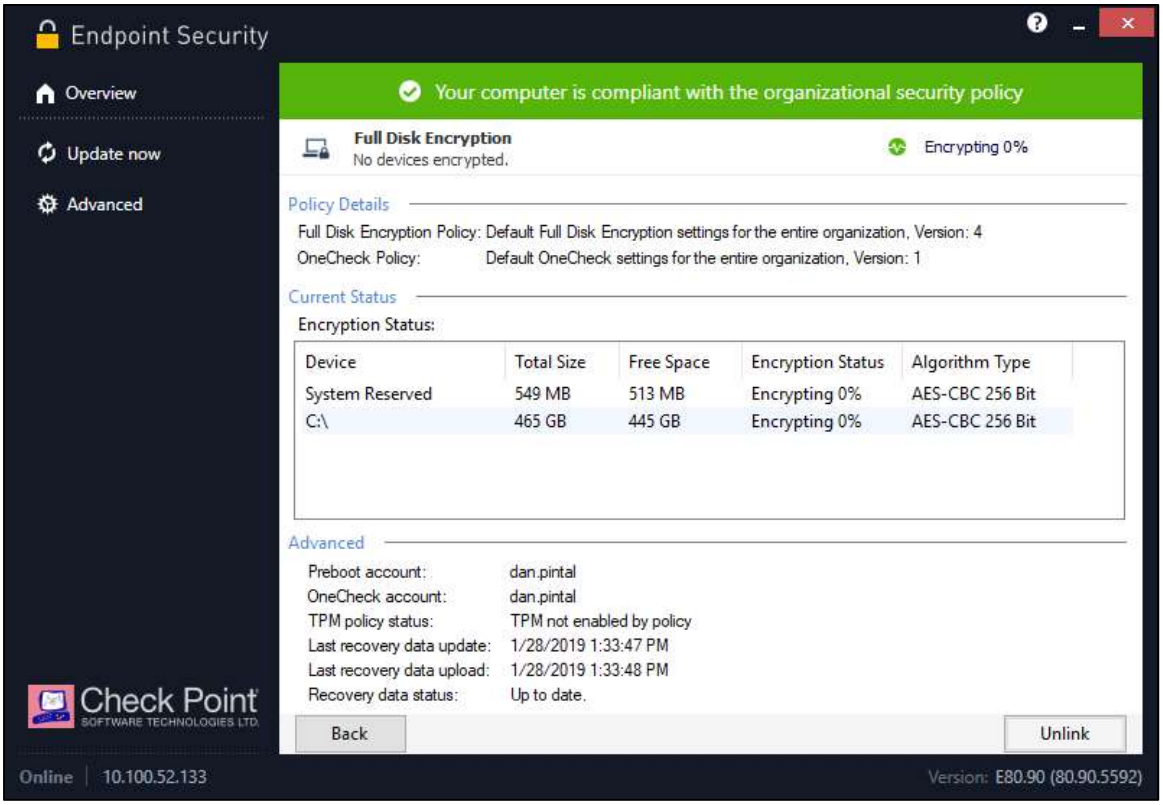


4. From the Clients workstation install the downloaded Check Point Endpoint Security software.

Installing the Client Package

1. When the client install is complete, and users are able to login at pre-boot enable encryption by right clicking the encryption policy within the Check Point SmartEndpoint Manager and selecting **Encrypt all local hard disks**.

2. Once the policy has been pushed to the clients the encryption of the hard disk will begin.



Certification Checklist for 3rd Party Applications

Date Tested: January 28, 2019

Product	Tested Version	Operating System
Check Point Security Management	Gaia R80.20	E80.20
Check Point SmartEndpoint Client	Window 10 x64	8.8.255
RSA Authentication Client	3.6	Windows 10 x64
RSA SecurID 800	Firmware 3.7	Revision Dx

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

Known Issues

Check Point has reported an issue when deploying Check Point SmartEndpoint on Windows 10. The issue is related to a Microsoft KB3213986. More information on this can be found on the Check Point support website at the following url.

https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk115485