SafeNet Authentication Client

Compatibility Guide

Using SafeNet Authentication Client with Windows Defender Credential Guard

gemalto
security to be free

Doc Number: 007-014070-001, Revision A

Release Date: April 2018

Contents

Description

Introduced in Windows 10 Enterprise and Windows Server 2016, Windows Defender Credential Guard uses virtualization-based security to isolate secrets so that only privileged system software can access them. Unauthorized access to these secrets can lead to credential theft attacks, such as Pass-the-Hash or Pass-The-Ticket. Windows Defender Credential Guard prevents these attacks by protecting NTLM password hashes, Kerberos Ticket Granting Tickets, and credentials stored by applications as domain credentials.

For more information please refer to:

https://docs.microsoft.com/en-us/windows/access-protection/credential-guard/credential-guard%0c

Applicability

The information in this document applies to:

- **SafeNet Authentication Client (SAC)** -SafeNet Authentication Client is a middleware client that manages Gemalto's extensive SafeNet portfolio of certificate-based authenticators, including eToken, IDPrime smart cards, iKey smart card, USB and software based devices.

Validated Devices

SAC 10.5 was validated with the following devices:

- SafeNet eToken 5110 GA
- SafeNet eToken 5110 FIPS
- SafeNet eToken 5110 CC
- Gemalto IDPrime MD 830 B
- Gemalto IDPrime MD 840 B

Environment

The integration environment that was used in this document is based on the following software versions:

- **SafeNet Authentication Client (SAC)** - 10.5
- **Microsoft Windows 10**
- **Dell Latitude e6540 - Laptop**

Validated Use Cases with SAC

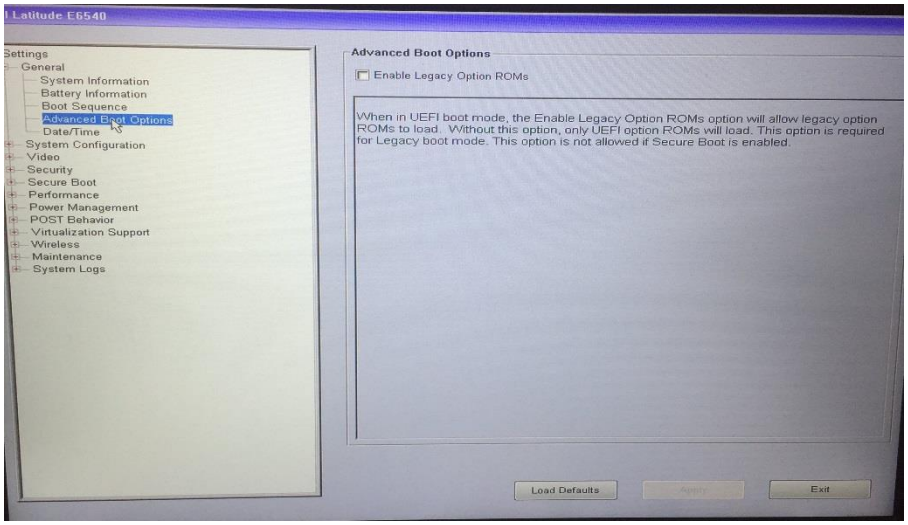
- Windows smart card Logon

MS Credential Guard and Code Integrity Configuration

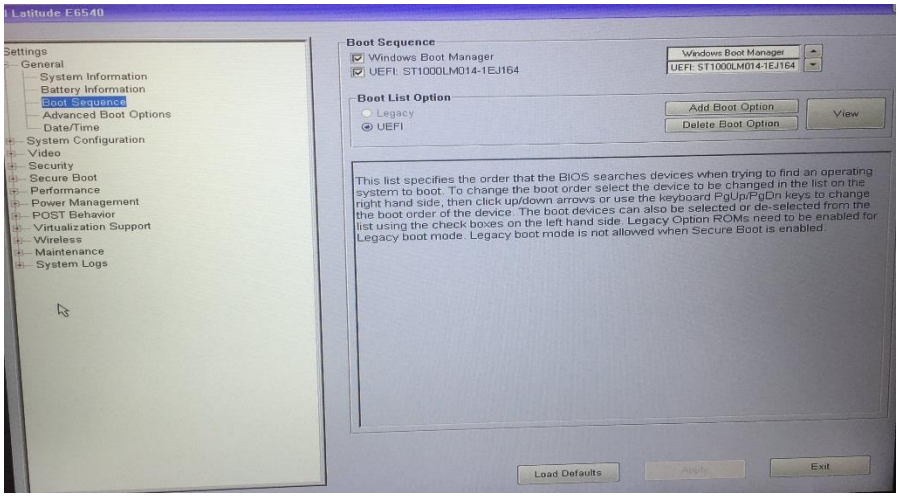
In order to test windows smart card authentication with credential guard and code integrity enabled, we use the following configuration:

On the machine's Bios:

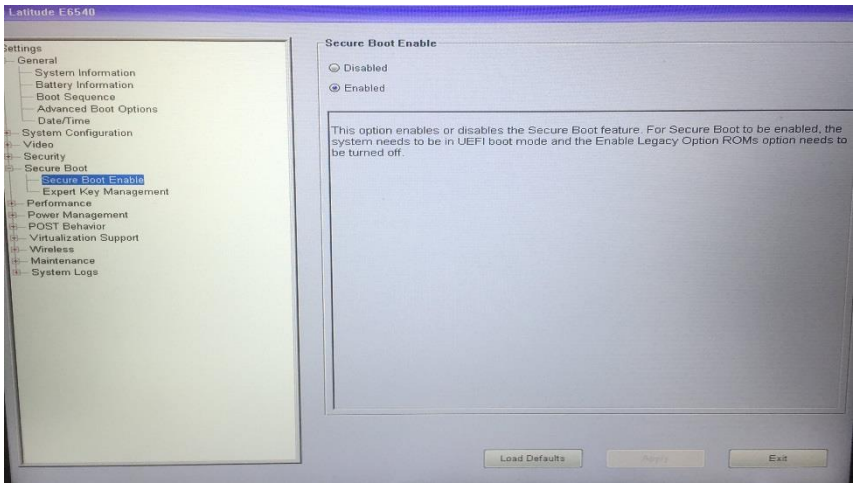
1. Under **Settings > General > Advanced Boot Options**, uncheck the **Enable Legacy Option ROMs**.



2. Under **Setting > General > Boot Sequence**, set the **Boot List Option** to **UEFI**.

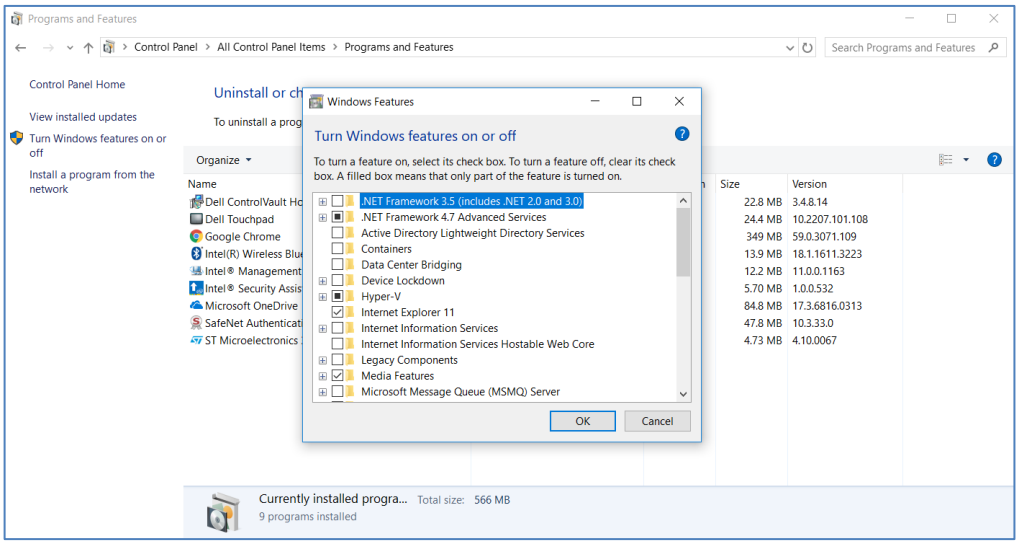


3. Under **Settings > Secure Boot > Secure Boot Enable**, enable the **Secure Boot Enable** option.



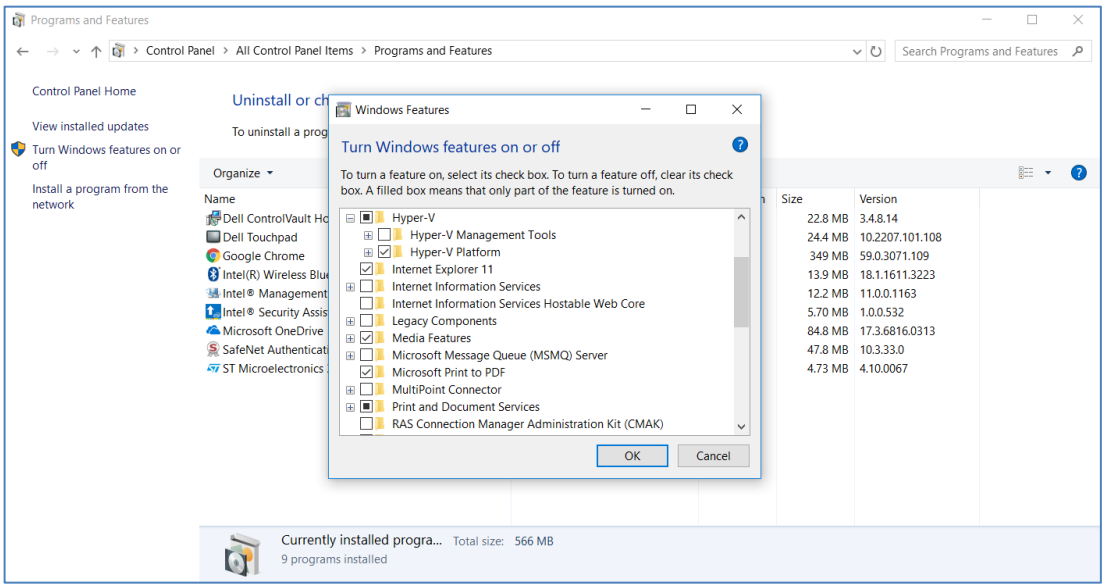
Install Hyper-V feature

1. Login to the Windows machine and open the **Control Panel**
2. Select **Programs > Programs and Features** > **Turn Windows features on or off**



(The screen image above is from Microsoft®. Trademarks are the property of their respective owners).

3. Expand the **Hyper-V** feature and enable **Hyper-V Platform.**



(The screen image above is from Microsoft®. Trademarks are the property of their respective owners).

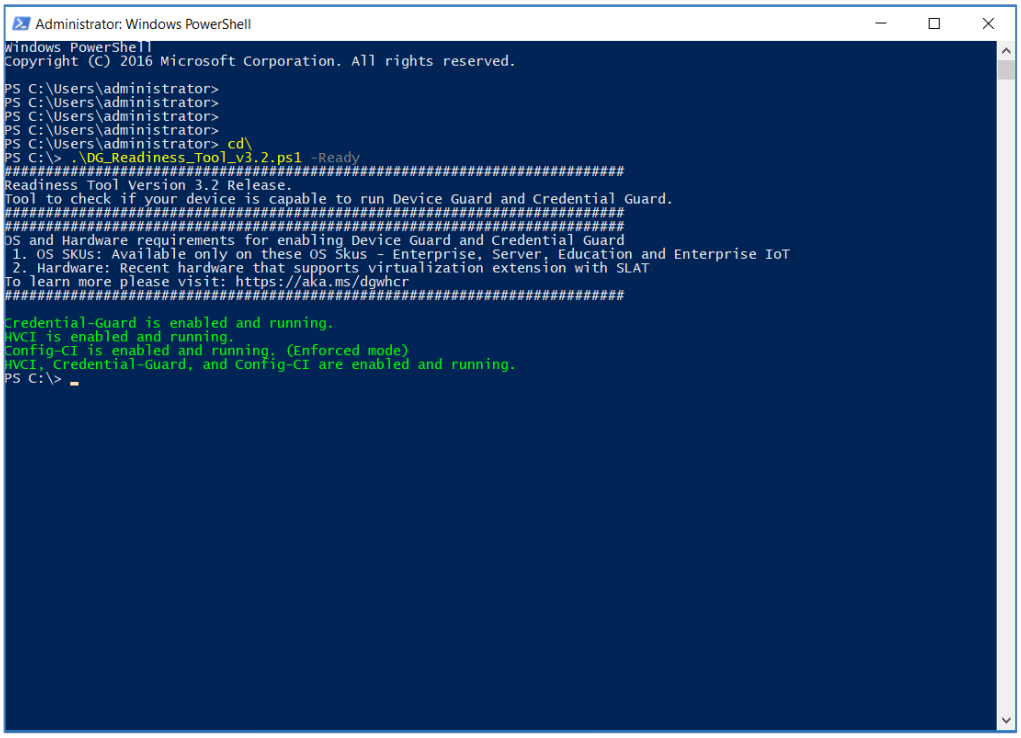
4. Click **OK**.

Enable Device Guard

In order to enable Device Guard please follow these steps:

1. Download the readiness tool from:
   https://www.microsoft.com/en-us/download/details.aspx?id=53337
2. Extract the downloaded zip file, where you will find the DG readiness tool (DG_Readiness.ps1)
3. Open Windows power shell and run these commands:
   a. Set-ExecutionPolicy RemoteSigned
   b. DG_Readiness.ps1 –Enable
   c. Restart the machine

4. After restarting, in order to check that the Device Guard is active, run the following command: **DG_Readiness.ps1 –Ready**. You should see this status screen:



Windows Defender Application Control Policy

To create the application control policy, follow these steps:

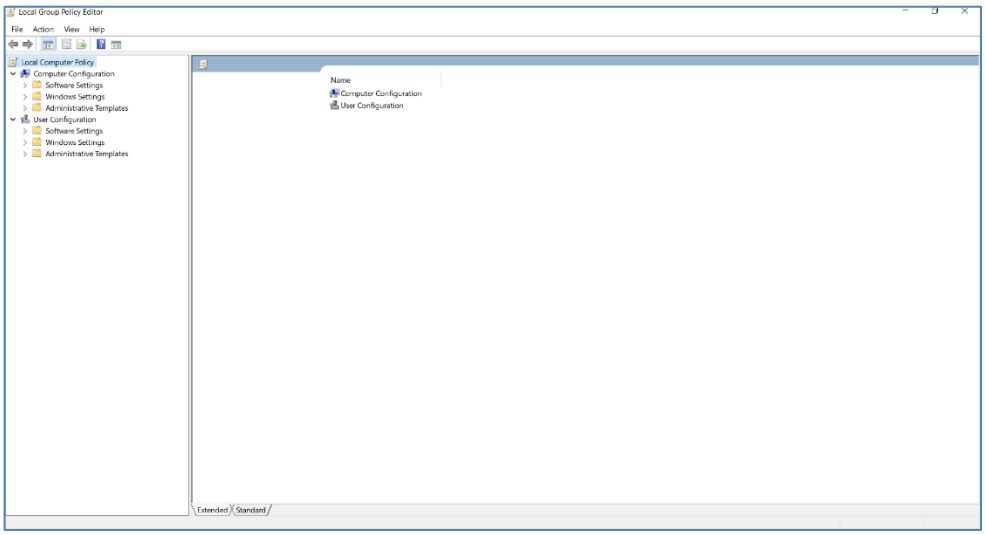
1. Initialize variables that you will use:
   a. `$CIPolicyPath=$env:userprofile+"\Desktop\"`
   b. `$InitialCIPolicy=$CIPolicyPath+"InitialScan.xml"`
   c. `$CIPolicyBin=$CIPolicyPath+"DeviceGuardPolicy.bin"`
2. Create a new WDAC policy by scanning the system:
   New-CIPolicy -Level PcaCertificate -FilePath $InitialCIPolicy –UserPEs 3> CIPolicyLog.txt
3. Convert the policy to binary format:
   ConvertFrom-CIPolicy $InitialCIPolicy $CIPolicyBin

Deploy Windows Defender Application Control Policy

In this section, we will deploy and enable the application control policy in audit mode.

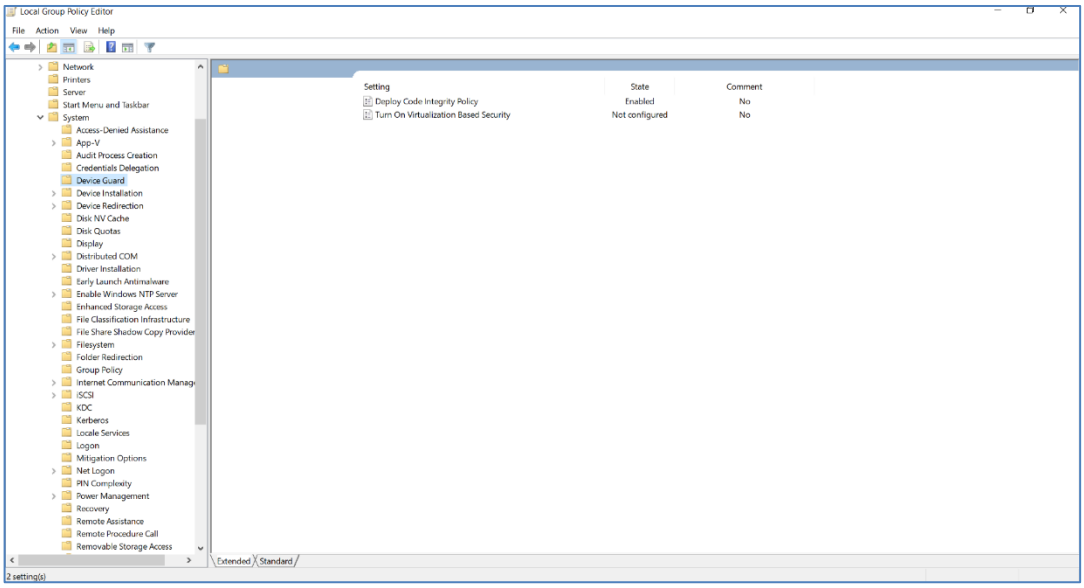
To deploy the policy, find the *.bin file you created.

1. Run **GPEdit.msc** on the machine you want to configure with the application control policy.



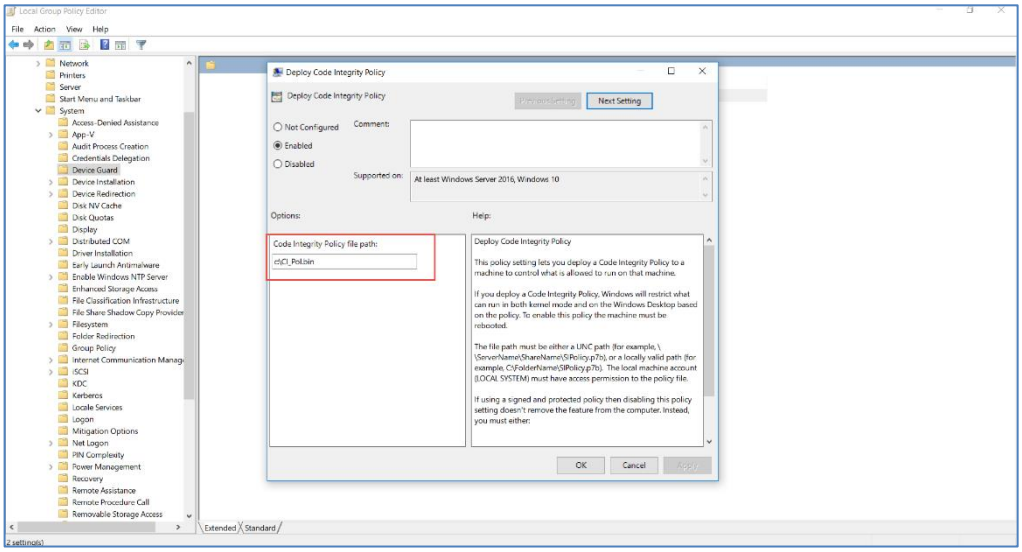
(The screen image above is from Microsoft®. Trademarks are the property of their respective owners).

2. Navigate to **Computer Configuration > Administrative Templates > System > Device Guard**



(The screen image above is from Microsoft®. Trademarks are the property of their respective owners).

3. Double click on **Deploy Code Integrity policy**. The Deploy Code Integrity Policy is open. Enter the bin file path in the file path text box.



(The screen image above is from Microsoft®. Trademarks are the property of their respective owners).

4. Click **OK**.

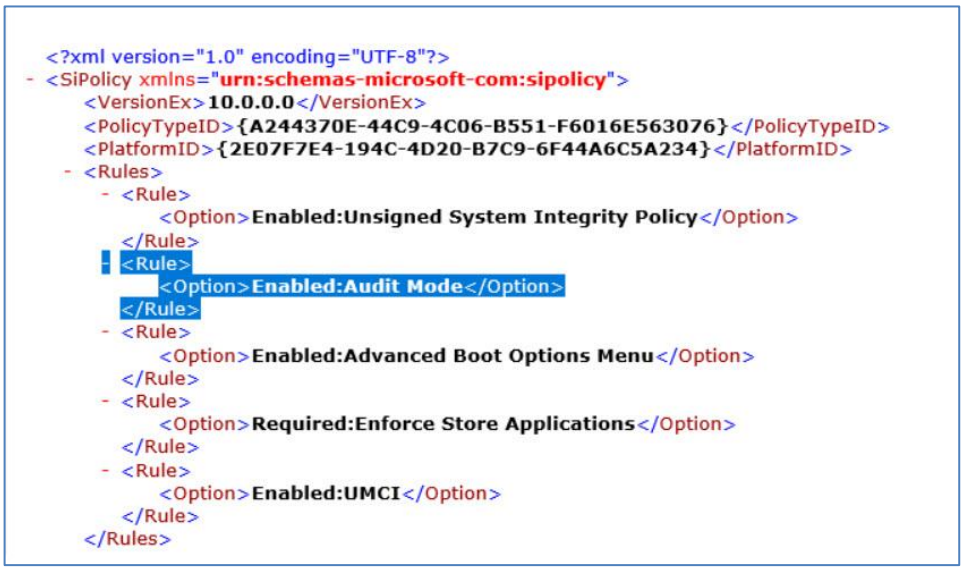
More information can be found here:

https://docs.microsoft.com/en-us/windows/device-security/device-guard/steps-to-deploy-windows-defender-application-control

Enforce Windows Defender Application Control Policy

In this section we will disable the audit mode and configure the application control policy to work in restricted mode:

1. Edit the xml file you created in the **Windows Defender Application Control Policy** section



2. Look for the **Enabled:Audit Mode** section and delete the rule
3. Convert the xml file (see **Windows Defender Application Control Policy**, step 3)
4. Configure the bin file (see **Deploy Windows Defender Application Control Policy** section)

More information can be found here:

https://blogs.technet.microsoft.com/ukplatforms/2017/04/04/getting-started-with-windows-10-device-guard-part-1-of-2/#enforce-ci

Support Contacts

If you encounter a problem while installing, registering, or operating this product, refer to the documentation. If you cannot resolve the issue, contact your supplier or Gemalto Customer Support.

Gemalto Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between Gemalto and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Customer Support Portal

The Customer Support Portal, at https://supportportal.gemalto.com, is a where you can find solutions for most common problems. The Customer Support Portal is a comprehensive, fully searchable database of support resources, including software and firmware downloads, release notes listing known problems and workarounds, a knowledge base, FAQs, product documentation, technical notes, and more. You can also use the portal to create and manage support cases.

NOTE: You require an account to access the Customer Support Portal. To create a new account, go to the portal and click on the **REGISTER** link.

Telephone Support

If you have an urgent problem, or cannot access the Customer Support Portal, you can contact Customer Support by telephone. Calls to Customer Support are handled on a priority basis.

Region	**Telephone number** (Subject to change. An up-to-date list is maintained on the Customer Support Portal)
Global	+1-410-931-7520
Australia	1800.020.183
China	North: 10800-713-1971 South: 10800-1301-932
France	0800-912-857
Germany	0800-181-6374
India	000.800.100.4290
Israel	180-931-5798
Italy	800-786-421

Region	Telephone number (Subject to change. An up-to-date list is maintained on the Customer Support Portal)
Japan	0066 3382 1699
Korea	+82 2 3429 1055
Netherlands	0800.022.2996
New Zealand	0800.440.359
Portugal	800.863.499
Singapore	800.1302.029
Spain	900.938.717
Sweden	020.791.028
Switzerland	0800.564.849
United Kingdom	0800.056.3158
United States	(800) 545-6608