SafeNet Authentication Client Compatibility Guide

Using SafeNet Authentication Client with Windows Defender Credential Guard



All information herein is either public information or is the property of and owned solely by Gemalto. and/or its subsidiaries who shall have and keep the sole right to file patent applications or any other kind of intellectual property protection in connection with such information.

Nothing herein shall be construed as implying or granting to you any rights, by license, grant or otherwise, under any intellectual and/or industrial property rights of or concerning any of Gemalto's information.

This document can be used for informational, non-commercial, internal and personal use only provided that:

- The copyright notice below, the confidentiality and proprietary legend and this full warning notice appear in all copies.
- This document shall not be posted on any network computer or broadcast in any media and no modification of any part of this document shall be made.

Use for any other purpose is expressly prohibited and may result in severe civil and criminal liabilities.

The information contained in this document is provided "AS IS" without any warranty of any kind. Unless otherwise expressly agreed in writing, Gemalto makes no warranty as to the value or accuracy of information contained herein.

The document could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Furthermore, Gemalto reserves the right to make any change or improvement in the specifications data, information, and the like described herein, at any time.

Gemalto hereby disclaims all warranties and conditions with regard to the information contained herein, including all implied warranties of merchantability, fitness for a particular purpose, title and non-infringement. In no event shall Gemalto be liable, whether in contract, tort or otherwise, for any indirect, special or consequential damages or any damages whatsoever including but not limited to damages resulting from loss of use, data, profits, revenues, or customers, arising out of or in connection with the use or performance of information contained in this document.

Gemalto does not and shall not warrant that this product will be resistant to all possible attacks and shall not incur, and disclaims, any liability in this respect. Even if each product is compliant with current security standards in force on the date of their design, security mechanisms' resistance necessarily evolves according to the state of the art in security and notably under the emergence of new attacks. Under no circumstances, shall Gemalto be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Gemalto products. Gemalto disclaims any liability with respect to security for direct, indirect, incidental or consequential damages that result from any use of its products. It is further stressed that independent testing and verification by the person using the product is particularly encouraged, especially in any application in which defective, incorrect or insecure functioning could result in damage to persons or property, denial of service or loss of privacy.

© 2010 - 2018 Gemalto. All rights reserved. Gemalto and the Gemalto logo are trademarks and service marks of Gemalto and/or its subsidiaries and are registered in certain countries. All other trademarks and service marks, whether registered or not in specific countries, are the property of their respective owners.

Doc Number: 007-014070-001, Revision A Release Date: April 2018

Contents

Description4
Applicability4
Validated Devices4
Environment4
Validated Use Cases with SAC4
MS Credential Guard and Code Integrity Configuration5
On the machine's Bios:5
Install Hyper-V feature6
Enable Device Guard7
Windows Defender Application Control Policy8
Deploy Windows Defender Application Control Policy9
Enforce Windows Defender Application Control Policy11
Support Contacts12
Customer Support Portal12
Telephone Support12

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:

Li atitude E654

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

General System Information Bott Sequence Mixmonsel Elegit Options Data/Time S System Configuration System Configuration Secure Boot Performance Performance POST Behavior System Logs Maintenance System Logs	ettings	Advanced Boot Options
Bott Sequence Morenaet Eqst Eqst Data Morenaet Eqst Eqst Data Morenaet Eqst Eqst Data Morenaet Eqst Eqst Data Morenaet Security Secure Boat Poor Enhance Poor Enhance System Logs	General System Information Battery Information	Enable Legacy Option ROMs
	Battery Information Boot Sequence Data Filme Data Filme Video Secury Secury Performance POST Behavior Virulaization Support Virulaization Support Virulaization Support Virulaization Support Virulaization Support Virulaization Support Virulaization Support	When in UEFI boot mode, the Enable Legacy Option ROMs option will allow legacy option ROMs to load. Without this option, only UEFI option ROMs will load. This option is required for Legacy boot mode. This option is not allowed if Secure Boot is enabled.

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

	Boot Sequence	
Settings	Windows Boot Manager Windows Boot Manager	
Seneral Sustan Information	UEFI: ST1000LM014-1EJ164	
Battery Information		
Battery momation	Boot List Option	
Advanced Boot Ontions	Add Boot Option	liew
Date/Time	© LIFFI Delete Boot Option	
System Configuration		
Video		
Security		
- Secure Boot	This list specifies the order that the BIOS searches devices when trying to find an ope	rating
- Performance	system to boot. To change the boot order select the device to be changed in the list of	hange
Power Management	right hand side, then click up/down arrows or use the keyboard right provide selected from	m the
POST Behavior	the boot order of the device. The boot devices can also be selected on the boot of the boot of the device of the boot devices can also be selected on the boot of	bled for
- Virtualization Support	list using the check boxes on the left hand side toget, open source Boot is enabled.	
- Wireless	Legacy boot mode. Legacy boot mode is not allotted	
Maintenance		
B System Logs		
Da la		
	Lood Defaults Apply Exit	
	Load Dolading	

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

ettings	Secure Boot Enable
- General	O Disabled
- System Information	Cisable
Battery Information	Enabled
Advanced Boot Options	
Date/Time	
 System Configuration 	This option enables or disables the Secure Boot feature. For Secure Boot to be enabled the
+) Video	system needs to be in OEPI boot mode and the Enable Legacy Option ROWs option needs of
Secure Boot	
Secure Boot Enable	
Expert Key Management	
Performance	
Power Management POST Behavior	
- Virtualization Support	
+) Wireless	
Maintenance	
a System Logs	
	Load Defaults April Exit

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.

🛐 Programs and Features					- 🗆 ×
$\leftarrow \rightarrow \checkmark \uparrow \overline{\mathfrak{A}} \rightarrow Control F$	Panel > All Control Panel Ite	ems > Programs and Features	```	・ ひ Search Program	ns and Features 👂
Control Panel Home View installed updates Turr Windows features on or	Uninstall or ch	Windows Features – – × Turn Windows features on or off			
off Install a program from the network	Organize ~ Name Dell ControlVault Hc Dell Touchpad Google Chrome Intel® Management Intel® Security Asis Microsoft OneDrive SafeNet Authenticat To ST Microelectronics	To turn a feature on, select its check box. To turn a feature off, clear its check box. A filled box means that only part of the feature is turned on.	Size 22.8 MB 24.4 MB 349 MB 13.9 MB 12.2 MB 5.70 MB 84.8 MB 4.73 MB 4.73 MB	Version 3.4.8.14 10.2207.10.108 59.0.3071.109 18.1.1611.3223 11.0.0.1163 10.0.532 17.3.6816.0313 10.3.33.0 4.10.0067	

(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"
- 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.

Local Group Policy Editor	-	ЭX
File Action View Help		
(= -> 📅 🔛 🕒 🖬 🖬		
Vertical Sector 1 and 1	Name Compute Configuration descriptions User Configuration	
	Constrainty Constrainty	

(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.

Printers	Deploy Code Integrity Policy	— 🗆 🗙	
Server Start Menu and Taskbar System	Deploy Code Integrity Policy	Previous Setting Next Setting	
Access-Denied Assistance App-V Audit Process Creation Credentials Delegation	Not Configured Comment: Enabled Disabled	~ ~	
Device Guard Device Installation Device Redirection Dok NV Cache	Supported on: At least	Windows Server 2016, Windows 10	
Disk Quotas	Options:	Help:	
> Distributed COM	Code Integrity Policy file path:	Deploy Code Integrity Policy	
Driver Installation	cl/Cl_Pol.bin	This policy setting lets you deploy a Code Integrity Policy to a	
Sound Window INP Sever Induced Sever		mediante to control what is allowed to non en that machine. If your obligave, Cacho heatingh heating, Carlowan will involve that an one in table homel models and on the Windows Decisiop based on the policy's consubs this palling heating heating heating involved to the table of the table of the table of the table reasonal. The file gash must be online a Killer gash tips exemption. Shows haven thanknown (Shorige yr), for an isolarly used gash tips reasonape. (CARS SSTIM) must have access permission to the policy Hea- H using a capacity and particulate good the datability give policy useting doars' remove the feature from the computer. Instead, you must either:	
PIN Complexity Power Management Prover Management		OK Cancel Access	

(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

SafeNet Authentication Client: Compatibility Guide

Using SafeNet Authentication Client with Windows Defender Credential Guard Document PN: 007-014070-001, Rev. A.

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