# Aloaha Smartlogin

Aloaha Smartlogin allows you to logon to your windows machine with a Smart Card, PKCS #11 Token, USB Memory Stick or just a plain Memory Card such as I2c or Mifare.

Authentication is not limited to the workstation logon but it supports also Remote Desktop, Shares, Hyper-V Sessions, etc.

# Contents

Features
Requirements
Installation
Logon Types4
Smart Card with any certificate loaded5
Automatic updating of Softtoken7
Sharing of Softtoken via Network Share7
Sharing of Softtoken via Active Directory8
PKCS #11 Token10
Plain USB Memory Stick
UserPass.ini Settings
Hide Username Field12
Aloaha Credential Provider Filter12
Albana Credential Fronder Filter
Card Removal Action
Card Removal Action13
Card Removal Action
Card Removal Action
Card Removal Action
Card Removal Action13ForceCRLChecks13Emergency Logon13Registry Settings13Checking of Certificate Revocation Lists13
Card Removal Action13ForceCRLChecks13Emergency Logon13Registry Settings13Checking of Certificate Revocation Lists13Enable/Disable CRL checking14
Card Removal Action13ForceCRLChecks13Emergency Logon13Registry Settings13Checking of Certificate Revocation Lists13Enable/Disable CRL checking14CRL checking parameter14
Card Removal Action13ForceCRLChecks13Emergency Logon13Registry Settings13Checking of Certificate Revocation Lists13Enable/Disable CRL checking14CRL checking parameter14Windows XP/2003 and GINA14
Card Removal Action13ForceCRLChecks13Emergency Logon13Registry Settings13Checking of Certificate Revocation Lists13Enable/Disable CRL checking14CRL checking parameter14Windows XP/2003 and GINA14SSO for legacy applications15
Card Removal Action13ForceCRLChecks13Emergency Logon13Registry Settings13Checking of Certificate Revocation Lists13Enable/Disable CRL checking14CRL checking parameter14Windows XP/2003 and GINA14SSO for legacy applications15Single Sign-On for Web Applications15

http://www.aloaha.com/download/AloahaCertificateCreator.zip	16
Aloaha Crypt Disk	16

This document is included in the setup package. An updated version is always available at: <a href="http://www.aloaha.com/handbuecher/AloahaSmartlogin\_en.docx">http://www.aloaha.com/handbuecher/AloahaSmartlogin\_en.docx</a>
http://www.aloaha.com/handbuecher/AloahaSmartlogin\_en.pdf

The German version can be found at:

http://www.aloaha.com/handbuecher/AloahaSmartlogin\_de.docx http://www.aloaha.com/handbuecher/AloahaSmartlogin\_de.pdf

Aloaha Smartlogin Blog:

http://blog.aloaha.com/category/aloaha-smartcard-software-en/aloaha-smart-login/

# **Features**

- Supports full Kerberos authentication (Active Directory required)
- Smart Card Logon even WITHOUT Active Directory possible.
- No special requirements for the Logon Certificate.
- Besides Smart Cards, Aloaha also supports other login tokens such as USB Memory Sticks, Memory Cards and PKCS #11<sup>1</sup> Tokens.
- Logon to network shares, remote desktop sessions, Hyper-V Consoles, etc. are also supported.
- Network Level Authentication (NLA) and Credential Security Support Provider (CredSSP) supported.
- Smart Card Logon also for legacy applications (SSO)
- MSI based installer available.

## **Requirements**

- Windows XP (Logon via GINA)
- Any other Windows from Vista onwards and incl. Windows 8/8.1. Both 32 and 64 Bit.
- .NET 3.5 Framework installed
- Active Directory supported but **NOT REQUIRED**
- Installed Middleware<sup>2</sup> for Smart Card(s).

## Installation

To install Aloaha you need to download the setup package from <a href="http://www.aloaha.com/download/smartlogin.zip">http://www.aloaha.com/download/smartlogin.zip</a>.

The MSI setup is wrapped into an executable. In case you require the plain MSI for your software management you can extract it from the exe OR request it from <u>info@aloaha.com</u>.

Please call the setup **smartlogin.exe** with administrator rights. Ideally you launch the setup with a right mouse click -> "Run as Administrator".

In case you do not own a valid license key please request an evaluation key from info@aloaha.com.

You need to make sure that the driver/middleware for your smart card is installed. If you do not have any driver/middleware for your smart card OR you are using the Aloaha Card, you can use the Aloaha Cardconnector as your middleware. It currently supports more than 45 different smart cards. Aloaha Cardconnector can be installed from:

http://www.aloaha.com/download/cardconnector.zip

<sup>1</sup> Please make sure you install the PKCS #11 Library of your token.

<sup>2</sup> The Aloaha Cardconnector Middleware supports more than 45 different Smart Cards. In case you do not have a middleware for your smart card or you are using the Aloaha Card please install the Aloaha Cardconnector from <u>http://www.aloaha.com/download/cardconnector.zip</u>

# **Logon Types**

The following logon tokens are supported:

- Smart Card with any certificate loaded.
   This is the most common used configuration since it does NOT require the certificate issued by a Domain Certification Authority. Active Directory is supported but not required.
   <u>http://blog.aloaha.com/2012/07/28/windows-logon-via-any-smartcard/</u>
- 2. PKCS #11 Token <u>http://blog.aloaha.com/2012/07/26/windows-logon-via-credentials-saved-encrypted-on-pkcs-11-token/</u>
- 3. Plain USB Memory Stick http://blog.aloaha.com/2012/07/25/windows-logon-with-plain-usb-memory-stick/
- 4. Kerberos http://blog.aloaha.com/2012/07/29/windows-logon-via-any-smartcard-and-kerberos/

# Smart Card with any certificate loaded

If you use a smart card, you need to link the Chipcard Certificate with the credentials. To do so please call "Encrypt Credentials" from the Windows Start Menu OR "Card Credentials" from the Aloaha System Tray Menu. The following dialog will open:

🕵 Aloaha Smart I	ogin Set Credentials	_ 🗆 🗙
Tools		
Usemame:	stefan	
Domain:	WROCKLAGE	
Password:		
Repeat Password:		
0) John Doe,1	9/03/2024 13:08:31,019	D,55ABA8295B4575 Set Credentials

You need to type in your windows password, choose the smart card to be used and click "Set Credentials".

A Softtoken will be created and saved to <Installdir>\CredentialStore. That Token contains some settings, the public part of the card certificate and a smart card encrypted secret.

ONLY the private key of the chip card is able to decrypt this secret!

Now you are already able to logon with your card to your windows system.

In some cases it might be required that you need to assign a smart card to a different user than suggested. In that case please start **SmartLogin\_SetCredentials.exe** with the parameter **/e** from the Aloaha installation folder. The tool will allow you then to edit all fields as shown below:

🕵 Aloaha Smart L	ogin Set Credentials	
Tools		
Usemame:		
Domain:	WROCKLAGE	
Password:		
Repeat Password:		
0) John Doe,19	9/03/2024 13:08:31,019	D,55ABA8295B4575
		Set Credentials

Alternatively, you can use the tool **SetCredentials.exe** from the installation folder. That tool also allows you to verify the smart card assignment(s):

et Card Credentials	5.0.300			
Refresh	🗖 Show All	🔽 Only Hardware Token		Import License
John Doe, 019D, 55A	BA8295B45753	910FE64951C7D3567F6AFA	Settings	
			Card Removal Action:	Lock Screen 💌
			Issuer Filter:	
			EKU Filter:	
			F	Refresh
Credentials				
Username:	wrocklage			
Domain:	stefan			
Password:	*****			
Confirm Password:	*****			
	Save			
	Validate			

#### Automatic updating of Softtoken

The Softtoken Files need to be updated as soon the assigned user changes the password. With the password hook that can be carried out fully automatic.

The password hook needs to be activated on the machine were the password is physically stored. In a domain that is the domain controller. Local Users are stored always on the local machine.

To install and activate the hook please make sure that Smartlogin is installed. You will find the tool **PasswdHK.exe in <InstallDir>\PasswdHK.exe** 

Call the tool with right click -> "Run as Administrator". Choose the tab "Activate Password Hook" as shown below:

🚪 Aloaha Password	Hook	×
Set initial Password	Activate Password Hook	
Enable REBOOT requi	Disable red after action change!	

Now please press "Enable" and reboot the machine to activate the hook. Whenever a user now changes the password the Softtoken will automatically updated.

#### Sharing of Softtoken via Network Share

It is possible to change the location of the Softtoken. Per default it is <Installdir>\CredentialStore. You can change that location in the registry in **HKLM\SOFTWARE\<Wow6432Node>\Aloaha\CSP\ CredentialStore** and point it to a network share. But please keep in mind that the logon process is running under local system credentials and thus the share needs to give local system the required permissions.

#### Sharing of Softtoken via Active Directory

In case your machines are part of an Active Directory Domain it is suggested to roam the token via AD.

Aloaha is using a dedicated Active Directory Application Partition to store its data. To create the partition please follow the steps below:

- 1. Make sure you are logged on with a user with Schema-Admin rights
- 2. Create the value ForceCreate in HKLM\SOFTWARE\<Wow6432Node>\Aloaha\AD and assign the value 1.
- 3. Download and run **AloahaADSI** from: <u>https://dl.dropboxusercontent.com/u/20338532/neverdelete/AloahaADSI.zip</u>
- 4. Choose the **"Settings"** tab and fill in your Schema-Admin Username and Password and click "Save". The Password fields will show empty after the **save**.

2	ADSI			×
	Test	Settings	AD INI Files Schema	
		Credentials - Usemame: Password: Password:	wrocklage\stefan	
			Save	

5. Open the **"Schema"** Tab and press "Create Schema". You should see the output as in the screenshot below if everything was created properly.

Nadsi 🛃 🛃 🛃 🛃 🛃 🛃 🛃 🛃 🔤 🔤 🔤 🔤 🔤 🔤 🔤 🔤 🔤 🔤 🔤 🔤 🔤	×
Test Settings AD INI Files Schema	_
Create Schema	
AD Application Partition created or exists SoftToken Object created or exists Schema Attribute created or exists Schema Class created or exists Config Object created or exists	

6. Quit the tool and delete **HKLM\SOFTWARE\<Wow6432Node>\Aloaha\AD\ForceCreate** to hide the Schema Tab.

You created now the required Application Partition to share your Softtoken across the domain.

Now you need to enable sharing on EVERY client machine with setting the value **enabled** to **1** in **HKLM\SOFTWARE\<Wow6432Node>\Aloaha\AD** (please create if not exist)

## PKCS #11 Token

If you opt to use a PKCS #11 Token to logon to your machine, your credentials will be saved encrypted on the token itself. It is essential that you make sure that the PKCS #11 Library of your token is installed!

To save your credentials on your token please start "PKCS #11 Credentials" from the Windows start menu or Aloaha System tray.

PKCS #11 Credentials 5.0.300		×
		Import License
PKCS #11 Library C:\Windows\System32\vendor_pkcs11.dll Gemalto USB Key Smart Card Read	Usename: Password: repeat Password:	wrocklage\stefan

- 1. Choose your vendors PKCS #11 Library
- 2. Now your token should be listed. Please choose the token to be used.
- 3. Enter <domain>\User and Password.
- 4. Press "Save" to save the encrypted credentials to your token. Click "Validate" to simulate a logon.

# **Plain USB Memory Stick**

It is also possible to use a plain USB Memory Stick as a logon token. Your credentials will be saved encrypted on the portable memory.

Please note that USB Memory Sticks are LESS secure than real smart cards since they do not use a dedicated crypto processor!

🕌 Drive Logon Creden	tials 🔀
	Import License
Stick Removal Action:	Lock Screen
Drives:	F:\ 💌
User:	stefan
Domain:	wrocklage
Password:	******
Password:	*******
USB PIN:	NNNN
USB PIN:	××××
V	alidate Save

You need to supply the USB drive letter, your username, optional your domain and the windows password. It is also essential that you define a USB PIN. That USB PIN will be later on your logon PIN. The PIN will also form part of the credential encryption key.

# **UserPass.ini Settings**

## **Hide Username Field**

The Username field of the logon tile can be left empty. Aloaha will then try to guess the right username based on the certificate of the card. You can also disable and hide the username field.

#### <Installdir>UserPass.ini



PIN

## **Aloaha Credential Provider Filter**

Username

.....

It is possible to hide any Logon Tile via the Aloaha Credential Provider Filter:

Card PIN

In some cases Credential Providers should be hidden from the Logon User Interface BUT still usable from within the session. For example someone might not want to see the Username/Password Tile during logon but obviously still requires it when mounting a network drive or connecting via RDP to another machine. In that case you cannot hide/disable the providers via windows group policy but a Credential Provider Filter is required.

Aloaha Smartlogin comes with an integrated Credential Provider Filter to be able to hide Tiles from the Windows Logon Interface WITHOUT removing its functionality inside the session.

To activate the Aloaha Credential Provider Filter you need to open the file **UserPass.ini** in the installation folder. In the section **CredentialProviders** you can configure different filter for different provider. To enable a filter please set it to 1. Set all the keys as shown below in order to disable ALL non-Aloaha CredentialProviders:

#### [CredentialProviders]

```
25CBB996-92ED-457e-B28C-4774084BD562=1
3dd6bec0-8193-4ffe-ae25-e08e39ea4063=1
503739d0-4c5e-4cfd-b3ba-d881334f0df2=1
6f45dc1e-5384-457a-bc13-2cd81b0d28ed=1
8bf9a910-a8ff-457f-999f-a5ca10b4a885=1
```

```
94596c7e-3744-41ce-893e-bbf09122f76a=1
AC3AC249-E820-4343-A65B-377AC634DC09=1
e74e57b0-6c6d-44d5-9cda-fb2df5ed7435=1
F8A0B131-5F68-486c-8040-7E8FC3C85BB6=1
```

## **Card Removal Action**

Per default Aloaha reads the Machines or Domains Card Removal policy. It can be fine-tuned and overwritten with:

[AutoLock]
PolicyAction=1
RemoveActionM=1

Furthermore you need to set HKLM\Software\Aloaha\CSP\RemoveAction=1 1 = Lock Screen, 2 = Lock Off, 3 = Reboot

ForceCRLChecks [Generic] ForceCRLChecks=1

This if this key is set to 1 it enforces CRL Checking. If this key is set to 1 it CANNOT be deactivated with any other CRL setting.

#### **Emergency Logon**

[Generic] AllowUP=1

If AllowUP is activated (default) the user can logon to the machine if he knows the valid user password. He has to add up: for username/password to his username and enter the password instead of the PIN.

For example instead of entering JohnDoe into the Username field you would enter up:JohnDoe

Instead of the PIN 0815 you would enter his password LetMeIn

#### If this emergency logon is NOT required please deactivate it!

# **Registry Settings**

#### **Checking of Certificate Revocation Lists**

If you have a fresh install of Aloaha Smart Login it will make only very basic checks on the certificate used. Revocation lists will NOT be used.

There are several reasons why revocation checking is disabled by default:

1. When evaluating Aloaha customer usually use test certificates without any valid CA behind. Checks would fail in that case and the customer might not be able to log on by smart card.  In case a user reports his smart card as lost the admin could just delete the softtoken to block the lost smart card. The same effect would have been a change of the user's password. That would lock out immediately the lost smart card but would still allow the user to logon with his new smart card and certificate.

The second point shows that revocation lists are just an extra layer of security but they are not really required. Even without revocation lists cards can be blocked.

#### Enable/Disable CRL checking

With the key HKLM\SOFTWARE\<Wow6432Node>\Aloaha\CSP\CertificateAlwaysValid the user can enable or disable the CRL checking. Default is disabled.

#### **CRL checking parameter**

Only certificates chaining up to the root are valid: HKLM\<Wow6432Node>\Software\Aloaha\CSP\EnforceChain

HKLM\<Wow6432Node>\Software\Aloaha\CSP\ ForceCRLChecks See also in Chapter: **ForceCRLChecks** 

#### Define CRL Type:

HKLM\<Wow6432Node>\Software\Aloaha\CSP\ForceCRL HKLM\<Wow6432Node>\Software\Aloaha\CSP\offCRL HKLM\<Wow6432Node>\Software\Aloaha\CSP\onICRL HKLM\<Wow6432Node>\Software\Aloaha\CSP\ForceOCSP

#### Consider unknown status as valid:

HKLM\<Wow6432Node>\Software\Aloaha\CSP\UnknownCertStatusIsValid

#### Accept expired certificates:

HKLM\<Wow6432Node>\Software\Aloaha\CSP\IgnoreCertTime

## Windows XP/2003 and GINA

On Windows XP/2003 Aloaha will install a GINA dll instead of the credential provider. In some cases it might be required to deactivate or remove the GINA. In that case you need to remove GinaDLL from HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion.

Edit View Favorites Help					
Ports	~	Name	Туре	Data	
Prefetcher		achedlogonscount	REG_SZ	10	
🕀 🧰 Print		CachePrimaryDo	REG_SZ	WROCKLAGE	
🗈 🧰 ProfileGuid		ChangePassword	REG_DWORD	0×00000001 (1)	
😨 💼 ProfileList		👸 DCacheUpdate	REG_BINARY	b0 43 29 99 d5 51 cf 01	
		DebugServerCom	REG_SZ	no	
i → j Setup		DefaultDomainNa	REG_SZ	WROCKLAGE	
B SvcHost		all DefaultUserName	REG_SZ	stefan	
🕢 🛄 SystemRestore		30 DisableCAD	REG_DWORD	0×00000000 (0)	
🗄 🧰 Terminal Server		Bigforceunlocklogon	REG_DWORD	0×00000000 (0)	
🗄 🦲 Time Zones		👜 GinaDLL	REG_SZ	C:\WINDOWS\system32\ginafull.dll	
😥 🦲 Tracing		👸 Hibernation Previ	REG_DWORD	0×00000001 (1)	
🕀 🧰 Type 1 Installer		LegalNoticeCaption	REG_SZ		
🚞 Userinstallable.drivers		LegalNoticeText	REG_SZ		
- 📄 Windows		BLogonType	REG_DWORD	0×00000000 (0)	
😟 🔄 Winlogon		📖 passwordexpiryw	REG_DWORD	0x0000000e (14)	
🗈 🦲 wow	-	DowerdownAfter	REG_SZ	0	
WPAEvents	×	ReportBootOk	REG_SZ	1	
	>	20 coremoveration	DEC DWODD	0~0000001 (1)	

# SSO for legacy applications

Please read the following documentation:

PDF: http://www.aloaha.com/handbuecher/l\_sso.pdf

DOCX: <u>http://www.aloaha.com/handbuecher/l\_sso.docx</u>

## **Single Sign-On for Web Applications**

PDF: http://www.aloaha.com/handbuecher/HTML\_SSO.pdf

DOCX: http://www.aloaha.com/handbuecher/HTML\_SSO.docx

# **Other useful applications**

Aloaha offers a couple of small and portable applications for Aloaha user.



#### AloahaZIP

With AloahaZIP you can certificate encrypt your ZIP documents:

http://www.aloaha.com/download/aloahazip.zip

## **PDFCrypter.NET**

Files Permissions   Certicate Encryption   Password Encryption   Files	Files Permissions Cerificate Encryption Password Encryption
Files	
C·Uleers\stefan WROCKLAGE\Desktop\amsQ12014.pdf C·Uleers\stefan WROCKLAGE\Desktop\atmachangle C·Uleers\stefan WROCKLAGE\Desktop\atmachangle C·Uleers\stefan WROCKLAGE\Desktop\sta_jeur_en.pdf	Encryption Certificates [Subject] CN-John Doel[ssuer] CN-John Doe[Settal Number] 4AAD2A7669A91D994E4679905E: [Subject] CN-Stafen@wnocklage.de. CN-Safan Engelbert. OLI-NorhaBenutzer. DC-wnocklage. DC [Subject] CN-test [Ibsuer] CN-test [Senia Number] 77A40980870567984FE7C9D09DC6907C[N [Subject] CN-test [Ibsuer] CN-test 2[Senia Number] 1AE695853965058843DAD11E1A3D4381[N
Add PDF Files Add PDF Folder Next with file permissions Output Path: Choose	Add Remove Encrypt Files

With the PDFCrypter.NET you can encrypt your PDF documents with a password or certificates: <a href="http://www.aloaha.com/download/AloahaPDFCrypter.NET.zip">http://www.aloaha.com/download/AloahaPDFCrypter.NET.zip</a>

Create digital certificates



To create quickly exportable or non-exportable certificates please use the following tool:

http://www.aloaha.com/download/AloahaCertificateCreator.zip

# Aloaha Crypt Disk

With Aloaha Crypt Disk you can create a certificate or smart card encrypted drive container:

http://www.aloaha.com/download/AloahaCrypt%20Setup1.3b.zip

AloahaCrypt	AloahaCrypt Volume Creation Wizard	_ 🗆 🗙
Values	Volume Card Encryption Please insert the card with which you with to encrypt the volume unempty being created and press next.	
Ocate Induce         Vision Properties         Preferences           Value         Value         Value         Select Plan           P fracer size hatery         Marct         Demount All         Ext	Heb Cad Next> Ca	ncel