abylonsoft – Dr. Thomas Klabunde H	Homepage: <u>www.abylonsoft.de</u>	Erstellt am 18.12.2017
Zum Eichwald 43	Kontakt: <u>www.abylonsoft.de/impressum.htm</u>	Geändert am 01.06.2018
55444 Seibersbach A	Autor: Thomas Klabunde	Versionsnummer: 1.1

INHALTSVERZEICHNIS

1	C	Content	2
2	V	/erwendung von abylon logon business	3
	2.1	Unterstützte Token's	3
	2.2	Installation im Firmennetzwerk	4
	2	2.2.1 Administration im Domainumfeld	5
	2	2.2.2 Administration im Arbeitsgruppenumfeld	6
	2	2.2.3 Erweiterte Administration	8
	2.3	Umgebung prüfen	9
	2.4	Weitere Dokumente und FAQs	9

aby X onsoft	abylonsoft – Dr. Thomas Klabunde	Homepage: <u>www.abylonsoft.de</u>	Erstellt am 18.12.2017
	Zum Eichwald 43	Kontakt: <u>www.abylonsoft.de/impressum.htm</u>	Geändert am 01.06.2018
	55444 Seibersbach	Autor: Thomas Klabunde	Versionsnummer: 1.1

1 CONTENT

Dieses Whitepaper beschreibt die notwendigen Einstellungen für abylon LOGON BUSINESS, um die abylon LOGON – Kontendateien (Schlüsseldateien) zentral zu verwalten und auf den Clients im Netzwerk zu verteilen.

aby X onsoft	abylonsoft – Dr. Thomas Klabunde	Homepage: <u>www.abylonsoft.de</u>	Erstellt am 18.12.2017	
	Zum Eichwald 43	Kontakt: <u>www.abylonsoft.de/impressum.htm</u>	Geändert am 01.06.2018	
	55444 Seibersbach	Autor: Thomas Klabunde	Versionsnummer: 1.1	
WITHEPAPER – KONTENVERTEILUNG ABYLON LOGON BUSINESS				

2 VERWENDUNG VON ABYLON LOGON BUSINESS

Die Software abylon LOGON BUSINESS von abylonsoft dient als alternative Anmeldemöglichkeit mit diversen Hardwareschlüsseln (Token's) unter Windows XP, Windows 7, Windows 8 und Windows 10. Mit abylon LOGON BUSINESS ist es den Nutzern möglich, sich an Windowsclients ohne Kenntnis des Windows-Kennwortes nur mit Hilfe eines Token's anzumelden. Bei abylon LOGON BUSINESS werden die Anmeldedaten (Credentials) mit Hilfe des Token's verschlüsselt und lokal oder zentral auf einem Server gespeichert. Im Fall von USB-Sticks kann der Anwender wählen, ob die Schlüsseldateien direkt auf dem USB-Stick oder dem PC gespeichert werden.

2.1 Unterstützte Token's

■ • abylon LOGON	¥□- C⊯
 Logon Logon Konten Logon Einstellungen Logon Job Administration Administration Einstellungen 	Logon Konten Logon Einstellungen Logon Job ANY CARD READER Optionale Einschränkung für Kartenleser Auswahl der Middleware bei zertfikatsbasierten Token Für die Anmeldung zugelassene Medien Zertifikatschipkarte / Token Sonstige Schlüsselkarte Speicherchipkarte Externes Speichermedium (z. B. USB-Stick) mit Schlüsseldatei auf dem Medium Externes Speichermedium (z. B. USB-Stick) mit Schlüsseldatei auf dem Medium Externes Speichermedium (z. B. USB-Stick) mit Schlüsseldatei auf dem PC CD/DVD Kontaktlose RFID-Chipkarten (Lowlevel-Access, z. B.: MADA, INTERFLEX) Bluetoothgerat (z. B. Mobiltelefon) Merchesel zum normalen Loono mit Abbruch (FSC) im Anmeldemodus zulassen Wechsel zum normalen Loono mit Abbruch (FSC) im Anmeldemodus zulassen Wechsel zum normalen Loono mit Abbruch (FSC) im Anmeldemodus zulassen Wechsel zum normalen Loono mit Abbruch (FSC) im Anmeldemodus zulassen Wechsel zum normalen Loono mit Abbruch (FSC) im Anmeldemodus zulassen Wechsel zum normalen Loono mit Abbruch (FSC) im Anmeldemodus zulassen Mitter Schologon: «INAKTIV»
	✓ SERVICE: <installient> ✓ SERVICE: <installient> ✓</installient></installient>

Die Vielzahl der Token's ist groß. Folgende Token's können mit der Software von abylonsoft verwendet werden:

- Alle Handelsüblichen USB-Sticks
- Alle weiteren **externen Speichermedien** die ein Laufwerk anlegen, wie z. B. SD-Card, CompactFlash, MemoryStick oder Multimedia-Karte
- CDs und DVDs
- Diverse Chipkarten (Smartcards)

aby X onsoft	abylonsoft – Dr. Thomas Klabunde	Homepage: <u>www.abylonsoft.de</u>	Erstellt am 18.12.2017	
	Zum Eichwald 43	Kontakt: <u>www.abylonsoft.de/impressum.htm</u>	Geändert am 01.06.2018	
	55444 Seibersbach	Autor: Thomas Klabunde	Versionsnummer: 1.1	
WITHEPAPER – KONTENVERTEILUNG ABYLON LOGON BUSINESS				

2.2 Installation im Firmennetzwerk

■ - abylon LOGON		」 □ ×□ ×
 Logon Logon Konten Logon Einstellungen Logon Job Administration Administration Einstellungen 	Logon Logon Konten L Logon-Konten anlegen und entfer Sonstige Schlüsse Sp-aspire-win Sp-aspi	ogon Einstellungen Logon Job Eingelegten Hardwareschlüssel testen Verschlüsselungs-Algorithmus HyBRID - AES (256 bit) • eelkarte ID: (01A5803F59C4EBA285E34A15205485CCAF0E0C0A08060402) • 7/trottel Für einen Hardwareschlüssel können mehrere Windows-Konten (auch unterschiedliche Rechner) angelegt werden remedium (z. B. USB-Stick) ID: (042BC2E7BD29ACBCC8AD5FA276D646B15D0E0C0A08060402) P/uwe Für ein Windows-Konto können auch mehrere Hardwareschlüssel angelernt werden
	Anmeldename: Anmeldekennwort: Domain: Encryption ALG:: Datei:	Alias: * C:\Users\Public\Documents\abylonsoft\apmLogon\DATA\LOGON\01A5803F59C4EBA285E34A152 Speicherort der Logon-Kontendatei

abylon LOGON BUSINESS muss auf jeden Client und auf dem Server installiert werden. Nach der Installation wird die Software automatisch aktiviert und ersetzt damit die bisherige Windowsanmeldung. Soll die Software auf dem Server nur zur Administration (Anlegen und Verwalten der Kontendateien) verwendet werden, so muss die Logon-Funktionalität auf dem Server nicht unbedingt aktiviert sein. Auch ohne Aktivierung lassen sich Logon-Konten anlegen.

Im Rahmen der Aktivierung prüft abylon LOGON BUSINESS, ob es sich in einem Arbeitsgruppenoder Domainumfeld befindet und nimmt alle Einstellungen automatisch vor. Ferner werden zwei Dienste (Systemkontext und Userkontext) installiert, die die Kontenverteilung im Firmennetzwerken vornehmen.

Für den Dienst im Userkontext wird ein spezielles Benutzerkonto neu angelegt, welches allein für die Netzwerkkommunikation und der LOGON-Konten-Synchronisation verwendet wird. Dieses Konto benötigt keine besonderen Rechte und sollte mit den Zugriffsrechten auf das Minimum beschränkt bleiben. Der Nutzer und das Kennwort für das SYNC-Konto können beliebig gewählt werden. Einzige Voraussetzung ist, der Anmeldename und das Kennwort müssen auf allen Clients und dem Server identisch sein.

aby X onsoft	abylonsoft – Dr. Thomas Klabunde	Homepage: <u>www.abylonsoft.de</u>	Erstellt am 18.12.2017	
	Zum Eichwald 43	Kontakt: <u>www.abylonsoft.de/impressum.htm</u>	Geändert am 01.06.2018	
	55444 Seibersbach	Autor: Thomas Klabunde	Versionsnummer: 1.1	
WITHEPAPER – KONTENVERTEILUNG ABYLON LOGON BUSINESS				

2.2.1 Administration im Domainumfeld

abylon LOGON BUSINESS erkennt, ob es sich in einem Domainumfeld befindet. In diesem Fall wird die Kontensynchronisation automatisch aktiviert und auf den Clients die Domain als Server verwendet.

■ abylon LOGON Einstellut	ngen auf dem Se	rver!	₩ 0 - □ ×	
🗏 📌 Logon	Administration Administrati	on Einstellungen		
🔏 Logon Konten	Admin-Diens	t Synchronistations-Dienst		
🙀 Logon Job	Registry (HKLM) auf dem S	Server für administrative Einstellungen der Anwender verwenden		
= 🔀 Administration	Administrationsserver: S	P-V3-UWE		
🔀 Administration Einstellungen		Admin-Einstellungen (Info! Nicht für die synchronisation erforderlich		
	Public Account-Path:	C:\Users\Public\Documents\abylonsoft\apmLogon\DATA\LOGON		
	Private Account-Path	C:\Users\uwe\Documents		
	Benutzerdienst	Voreinstellung Synchronisations-Einstellungen		
	Benutzername	LELogonUser_Sync		
	Passwort	********		
	Domain	abylon-home.de		
	Public Account-Path:	C:\abylonsoft\LOGONACCOUNTs Wichtig! Auch dem Server lokales Verzeichnis		
■ abylon LOGON Einstellungen	≡ - abylon LOGON Einstellungen auf dem Client 🗦 🖉 🖓 _ □ ×			
😑 🔏 Logon	Administration Administrati	on Einstellungen		
🙀 Logon Konten	Admin-Diens	Synchronistations-Dienst		
🙀 Logon Job	Registry (HKLM) auf dem S	Server für administrative Einstellungen der Anwender verwenden		
= 🔀 Administration	Administrationsserver: 5	P-V3-UWE		
🕺 Administration Einstellungen	,			
		Admin-Einstellungen (Info! Nicht für die synchronisation erforderlich		
	Public Account-Path:	Admin-Einstellungen (Info! Nicht für die synchronisation erforderlich C:\Users\Public\Documents\abylonsoft\apmLogon\DATA\LOGON		
	Public Account-Path:	Admin-Einstellungen (Info! Nicht für die synchronisation erforderlich C:\Users\Public\Documents\abylonsoft\apmLogon\DATA\LOGON C:\Users\uwe\Documents		
	Public Account-Path: Private Account-Path Benutzerdienst	Admin-Einstellungen (Info! Nicht für die synchronisation erforderlich C:\Users\Public\Documents\abylonsoft\apmLogon\DATA\LOGON C:\Users\uwe\Documents Voreinstellung Synchronisations-Einstellungen		
	Public Account-Path: Private Account-Path Benutzerdienst Benutzername	Admin-Einstellungen (Info! Nicht für die synchronisation erforderlich C:\Users\Public\Documents\abylonsoft\apmLogon\DATA\LOGON C:\Users\uwe\Documents Voreinstellung LELogonUser_Sync		
	Public Account-Path: Private Account-Path Benutzerdienst Benutzername Passwort	Admin-Einstellungen (Info! Nicht für die synchronisation erforderlich C:USers\Public\Documents\abylonsoft\apmLogon\DATA\LOGON C:USers\uwe\Documents Voreinstellung LELogonUser_Sync 		
	Public Account-Path: Private Account-Path Private Account-Path Private Account-Path Private Account-Path Passwort Benutzername Passwort Domain	Admin-Einstellungen (Infol Nicht für die synchronisation erforderlich C:\Users\Public\Documents\abylonsoft\apmLogon\DATA\LOGON C:\Users\uwe\Documents Voreinstellung LELogonUser_Sync abylon-home.de		
	Public Account-Path: Private Account-Path Private Account-Path Private Account-Path Paswort Benutzername Passwort Domain Public Account-Path:	Admin-Einstellungen (Infol Nicht für die synchronisation erforderlich C:\Users\Public\Documents\abylonsoft\apmLogon\DATA\LOGON C:\Users\uwe\Documents Voreinstellung LELogonUser_Sync abylon-home.de \\SP-server\LOGONACCOUNTs Wichtig! Auf dem Client UNC-Pfad		

Auf der Domain selber legt die Software auf dem Laufwerk C: ein Verzeichnis (C: \abylonsoft\LOGONACCOUNTs) mit Freigabe (LOGONACCOUNTs) im Netzwerk an. In diesem Verzeichnis sollten nur die Kontendateien abgelegt sein und auf keinem Fall sicherheitskritische Daten. Die Kontendateien selber sind nicht Sicherheitskritisch, weil diese mit den Token's verschlüsselt sind. Die Freigabe ist für die Synchronisation der Konten unabdingbar.

Wird auf dem Server (Domain) mit abylon LOGON BUSINESS ein Konto angelegt, so wird dieses verschlüsselt in dem Freigabeverzeichnis gespeichert. Vor dort verteilen die Clientdienste automatisch die Dateien im Netzwerk, sodass diese auf den Clients lokal verfügbar sind. Sollte die Domain bzw. Server nicht erreichbar sein (OFFLINE), so wird das lokal auf den Clients gecachte Konto verwendet.

[©] abylonsoft (www.abylonsoft.de) – Ohne Befugnis durch den Autor ist die Vervielfältigung, Verwendung oder Weitergabe dieses Dokuments und dessen Inhaltes nicht gestattet!

aby X onsoft	abylonsoft – Dr. Thomas Klabunde	Homepage: <u>www.abylonsoft.de</u>	Erstellt am 18.12.2017
	Zum Eichwald 43	Kontakt: <u>www.abylonsoft.de/impressum.htm</u>	Geändert am 01.06.2018
	55444 Seibersbach	Autor: Thomas Klabunde	Versionsnummer: 1.1

Im Fall, dass die Nutzer selber ihre Konten anlegen, werden diese auf dem Server zurück gespeichert und von hier wiederrum auf die anderen Clients verteilt. Dies bedeutet, dass ein Nutzer, der am Client A ein Konto angelegt hat, dieses direkt auf allen anderen Clients (B, C, etc.) verwenden kann.

Wird auf dem Server ein Konto entfernt, so wird dieses auch auf den Clients entfernt und steht nicht mehr für die Anmeldung zur Verfügung. Für Clients, die sich zeitweise NICHT im Domainumfeld befinden und mit dem lokalen Konto arbeiten, wird die Synchronisation automatisch vorgenommen, wenn der Client sich wieder im Domainumfeld befindet.

2.2.2 Administration im Arbeitsgruppenumfeld

In contrast to the domain environment abylon LOGON BUSINESS does NOT activate the account synchronization automatically. To do this, the administrator must first define a client as server in the workgroup. This is done on the "Logon" settings page:

abylon LOGON) ×
🗏 👔 Logon	Logon Konten Logon Enstellungen Logon Job
Logon Konten Logon Einstellungen Logon Job Administration Administration Einstellungen	 Zum Ein- oder Ausschalten HIER KLICKEN! Durch Aktivierung dieser Option kann die Passworteingabe während Ihrer Windowsanmeldung automatisiert bzw. die Sicherheit deutlich erhöht werden. Bei aktiviertem Logon wird beispielsweise während der Windowsanmeldung zum Stecken von einem USB-Stick oder Chipkarte (Schlüsselkarte) aufgefordert, mit deren Hilfe Ihre Anmeldedaten verschlüsselt und nach dem Einlegen entschlüsselt und eingetragen werden. Neu anlegen HIER KLICKEN! Mit dieser Option können Sie neue Windows-Anmeldedaten automatisch und sicher für Ihre Windowsanmeldung zu verwenden. Bei diesem Vorgang müssen Sie einmalig Ihre reallen Anmeldedaten (Name und Passwort) angeben, die mit dem eingelegten USB-Stick oder Chipkarte verschlüsselt werden.
	2. Einmal Klicken, um die Einstellungen vorzunehmen Vorbereitung der Umgebung für die Client-Server-Syncronisation. In diesem Fall werden die Logon-Konten zwischen dem Server und den Clients syncronisiert
	SERVER (IP / UNC): SP-SERVER 1. Servernamen eintregen

Zunächst wird der Rechnername eingegeben, der im Arbeitsgruppenumfeld als Server dienen soll. Durch Drücken des darüber liegenden Schalters nimmt die Software automatisch alle Einstellungen vor.

Dieser Vorgang wird auf allen Rechnern wiederholt.

Weitere Einstellungen sind in der Regel nicht notwendig. Auf der Einstellungsseite "Administration->Erweitert" werden die Einstellungen noch einmal angezeigt, wie in den folgenden Screenshots zu sehen. Hier sollten nur versierte Anwender Änderungen vornehmen.

aby Consoft 2u	bylonsoft – Dr. Thomas Klabunde	Homepage: <u>www.abylonsoft.de</u>	Erstellt am 18.12.2017
	um Eichwald 43	Kontakt: <u>www.abylonsoft.de/impressum.htm</u>	Geändert am 01.06.2018
	5444 Seibersbach	Autor: Thomas Klabunde	Versionsnummer: 1.1

	en auf dem Server!		
😑 🚰 Logon 🛛 🗛 🗛	inistration Administration Einstell	ungen	
🚰 Logon Konten	Admin-Dienst Syncl	The second secon	
🚰 Logon Job	egistry (HKLM) auf dem Server für a	dministrative Einstellungen der Anwender	verwenden
Administration	dministrationsserver: SP-V3-UW	1	
🔀 Administration Einstellungen	Admin-	Einstellungen (Info! Nicht für die synch	ronisation erforderlich
F F	ublic Account-Path: C:\Users\l	Public\Documents\abylonsoft\apmLogon\E	ATAILOGON
F	rivate Account-Path C:\Users\	uwe\Documents	
E	enutzerdienst Voreir	Synchron	nisations-Einstellungen
E	enutzername LELogon	User_Sync	
F	asswort ********	*****	
	erver: SP-V3-U	WE	Active-Sync-Service
· · · · · · · · · · · · · · · · · · ·	ublic Account-Path: C:\abylon: Wichtig!	soft\LOGONACCOUNTs Auch dem Server lokales Verzeichnis	
Einstellungen au	f dem Client		¥ □ - ○ ¥
😑 🙀 Logon 🛛 🗛	inistration Administration Einstell	ungen	
🚰 Logon Konten	Admin-Dienst	Tronistations-Dienst	
	egistry (HKLM) auf dem Server für a	dministrative Einstellungen der Anwender	verwenden
Administration	dministrationsserver: SP-V3-UW		
📩 Administration Einstellungen	Admin-	Einstellungen (Info! Nicht für die synch	ronisation erforderlich
F	ublic Account-Path: C:\Users\l	Public\Documents\abylonsoft\apmLogon\E	DATA\LOGON
F		dwelbocuments	
F	enutzerdienst Voreir	Instellung Synchroi	nisations-Einstellungen
E	enutzerdienst Vorein LELogon	Istellung Synchron	nisations-Einstellungen
F E F	enutzerdienst Vorein enutzername LELogon asswort	Instellung Synchron	nisations-Einstellungen
F F F	enutzerdienst Vorein enutzername LELogon asswort erver: SP-SERV	Instellung Synchron User_Sync	Isations-Einstellungen Zur Sychronisation aktivieren! Active-Sync-Service
F 5 5	enutzerdienst Vorei enutzername LELogon asswort erver: SP-SERV ublic Account-Path: VSP-serv Wichtig!	Istellung Synchron User_Sync /ER arlLOGONACCOUNTs Auf dem Client UNC-Pfad	Isations-Einstellungen Zur Sychronisation aktivieren! Active-Sync-Service

Auf dem als Server festgelegten Client (UNC-Name oder IP) legt die Software auf dem Laufwerk C: ein Verzeichnis (C:\abylonsoft\LOGONACCOUNTs) mit der Netzwerk-Freigabe (LOGONACCOUNTs) an. In diesem Verzeichnis sollten nur die Kontendateien abgelegt sein und auf keinem Fall sicherheitskritische Daten. Die Kontendateien selber sind nicht Sicherheitskritisch, weil diese mit den Token's verschlüsselt sind. Die Freigabe ist für die Synchronisation der Konten unabdingbar.

Im Arbeitsgruppenfeld sollte nach Aktivierung geprüft werden, ob das Kontenverzeichnis erfolgreich auf dem Server angelegt und freigegeben wurde.

Auf den Clients muss die Synchronisation unter Administration->Erweitert gleichfalls aktiviert werden und als Server der UNC-Name oder IP des als Server definierten Clients angegeben werden.

Wird auf dem Server (Arbeitsplatz-Rechner) mit abylon LOGON BUSINESS ein Konto angelegt, so wird dieses verschlüsselt in dem Freigabeverzeichnis gespeichert. Vor dort verteilen die Clientdienste automatisch die Dateien im Netzwerk, sodass diese auf den Clients lokal verfügbar sind. Sollte der Server (Arbeitsplatz-Rechner) nicht erreichbar sein (OFFLINE), so wird das lokal auf den Clients gecachte Konto verwendet.

aby X onsoft	abylonsoft – Dr. Thomas Klabunde	Homepage: <u>www.abylonsoft.de</u>	Erstellt am 18.12.2017			
	Zum Eichwald 43	Kontakt: <u>www.abylonsoft.de/impressum.htm</u>	Geändert am 01.06.2018			
	55444 Seibersbach	Autor: Thomas Klabunde	Versionsnummer: 1.1			
WITHEPAPER – KONTENVERTEILUNG ABYLON LOGON BUSINESS						

Im Fall, dass die Nutzer selber ihre Konten anlegen, werden diese auf dem Server zurück gespeichert und von hier wiederrum auf die anderen Clients verteilt. Dies bedeutet, dass ein Nutzer, der am Client A ein Konto angelegt hat, dieses direkt auf allen anderen Clients verwenden kann.

Wird auf dem Server ein Konto entfernt, so wird dieses auch auf den Clients entfernt und steht nicht mehr für die Anmeldung zur Verfügung. Für Clients, die sich zeitweise NICHT im Domainumfeld befinden und mit dem lokalen Konto arbeiten, wird die Synchronisation automatisch vorgenommen, wenn der Client sich wieder im Domainumfeld befindet.

2.2.3 Erweiterte Administration

Eine erweiterte Administration (z. B. Sperrung von Konten) ist in der Version 16.50.3 von abylon LOGON BUSINESS noch nicht möglich, wird aber für zukünftige Versionen berücksichtigt.

	aby X onsoft	abylonsoft – Dr. Thomas Klabunde Zum Eichwald 43 55444 Seibersbach	Homepage: <u>www.abylonsoft.de</u> Kontakt: <u>www.abylonsoft.de/impressum.htm</u> Autor: Thomas Klabunde	Erstellt am 18.12.2017 Geändert am 01.06.2018 Versionsnummer: 1.1
--	---------------------	--	---	---

2.3 Umgebung prüfen

Wird abylon LOGONBUSINESS mit aktivierter Kontensynchronisation genutzt, sollten folgende Bedingungen geprüft werden:

- abylon LOGON BUSINESS ist auf allen Clients und am Server installiert und aktiviert (Die Aktivierung am Server ist optional).
- Auf allen Clients und am Server sollte sich das Benutzerkonto "LELogonUser_Sync" mit identischem Passwort befinden. Bitte das Passwort oder Benutzername nicht manuell in den Windows-Benutzerkontenmanagement ändern. Änderungen dürfen nur in der Administrationsmaske von abylon LOGONBUSINESS vorgenommen werden.
- Bei aktivierten Logon sollten auf den Clients (Server optional) zwei Dienste laufen (LogonLEService). Ein Dienst sollte im Kontext des System-Users laufen und er andere Dienst im Kontext des "LELogonUser_Sync".
- Das Benutzerkonto "LELogonUser_Sync" muss Schreib- und Leserechte auf NTFS- und Freigabebasis auf alle Kontenverzeichnisse haben.
- Nach Ablauf der 30-Tage Testphase beendet sich der Synchronisationsdienst automatisch und die Funktion wird bis zur erfolgreichen Registrierung deaktiviert.

2.4 Weitere Dokumente und FAQs

Weitere Dokumente und FAQs (Frequently Ask Questions) finden Sie auf unserer Homepage im Download- und Support-Bereich: <u>http://www.abylonsoft.de</u>

Bei Fragen zur Software und speziellen Funktionswünschen können Sie sich jederzeit gerne an uns wenden. Die Email-Adresse und Telefonnummer finden Sie auch bei uns auf der Homepage im Impressum.