ID.logon
Smart Authentication

ID.logon Smart Authentication
Bedienerhandbuch / User Guide

RFID-Medium als Logon-Key: Schnelle und einfache Windows-Anmeldung
für alle gängigen **125 KHz** und **13,56 MHz** RFID-Transponder

Impressum

MADA Marx Datentechnik GmbH
Hinterhofen 4 – 78052 Villingen-Schwenningen

Tel.: +49(0)7721/8848-0
Fax: +49(0)7721/8848-20

E-Mail: info@mada.de
Web: www.mada.de

Geschäftsführer: Patrick Marx
Amtsgericht Freiburg: HRB 600 578
Ust-ID Nr.: DE 142 986 958

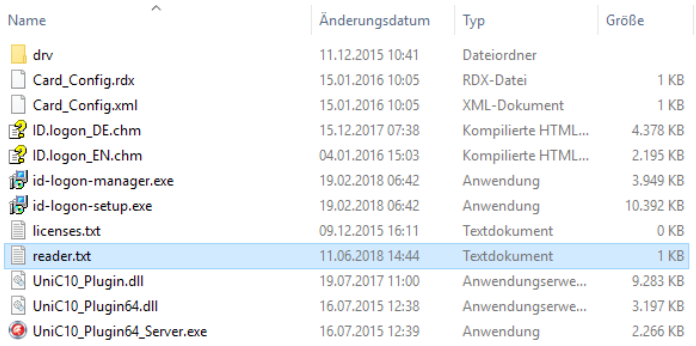
Inhalt

Installationsanleitung

Vorbereitung

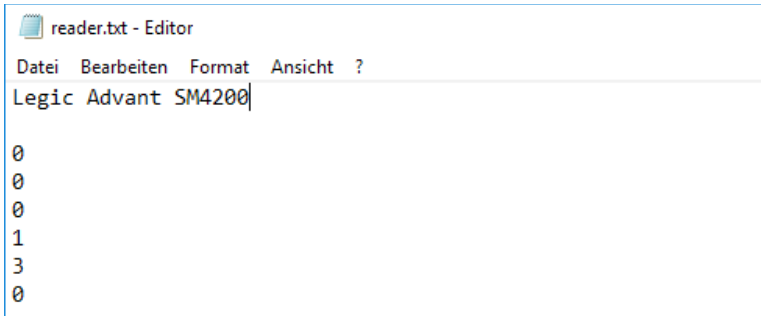
Schritt 1:
Stecken Sie den ID.logon USB-Stick in einen aktiven USB-Steckplatz Ihres PCs.

Schritt 2:
Öffnen Sie das Dateiverzeichnis des USB-Sticks.
Vor der eigentlichen Installation haben Sie die Möglichkeit, die Basisparameter bzw. Einstellungen für ID.logon festzulegen Doppelklicken Sie hierzu auf die Datei **„reader.txt“**.



Name	Änderungsdatum	Typ	Größe
drv	11.12.2015 10:41	Dateiordner	
Card_Config.rdx	15.01.2016 10:05	RDX-Datei	1 KB
Card_Config.xml	15.01.2016 10:05	XML-Dokument	1 KB
ID.logon_DE.chm	15.12.2017 07:38	Kompilierte HTML...	4.378 KB
ID.logon_EN.chm	04.01.2016 15:03	Kompilierte HTML...	2.195 KB
id-logon-manager.exe	19.02.2018 06:42	Anwendung	3.949 KB
id-logon-setup.exe	19.02.2018 06:42	Anwendung	10.392 KB
licenses.txt	09.12.2015 16:11	Textdokument	0 KB
reader.txt	11.06.2018 14:44	Textdokument	1 KB
UniC10_Plugin.dll	19.07.2017 11:00	Anwendungserwe...	9.283 KB
UniC10_Plugin64.dll	16.07.2015 12:38	Anwendungserwe...	3.197 KB
UniC10_Plugin64_Server.exe	16.07.2015 12:39	Anwendung	2.266 KB

1. Zeile:
Lesername (bereits voreingestellt)
z.B.: Legic advant SM4200



2. Zeile:
Diese ist nur relevant, wenn das Programm Key Manager erworben wurde. Diese beinhaltet die Adresse des Servers für die zentrale Speicherung der Schlüssel:
\\Server\profile path

3. Zeile:
Aktion bei Entfernen des RFID Mediums vom Leser:

- **0 = keine Aktion**
- 1 = Sperren
- 2 = Abmelden
- 3 = Herunterfahren
- 4 = Ruhezustand
- 5 = Bildschirmschoner aktivieren
- 6 = Benutzer wechseln

4. Zeile:
Anmelde-Optionen

- **0 = Alle User mit Passwort oder RFID Medium**
- 1 = nur mit RFID Medium
- 2 = Nur mit RFID Medium für Benutzer, die über ID.logon angelegt wurden, alle anderen mit Passwort
- 3 = Für ID.logon Benutzergruppen aus dem AD
- 4 = Remote Desktop Login
- 5 = Remote Desktop Login außerhalb des LAN

5. Zeile:
Authentifizierungsprüfung der Schlüsselnummer des RFID, die auf dem Client angelegt wurde. Alle anderen werden ignoriert. Diese Einstellung nicht verwenden, wenn Sie RFID Medien von anderen Clients importieren oder den Key Manager benutzen.

0 = Aus
1 = Ein

6. Zeile:
Verwendung RFID Medium im abgesicherten Modus:
0 = RFID Medium auch im abgesicherten Modus verwenden
1 = RFID Medium nicht im abgesicherten Modus verwenden

7. Zeile:
Maximale Anzahl an PIN Eingaben:
Eine Zahl von 0 bis 10 eingeben

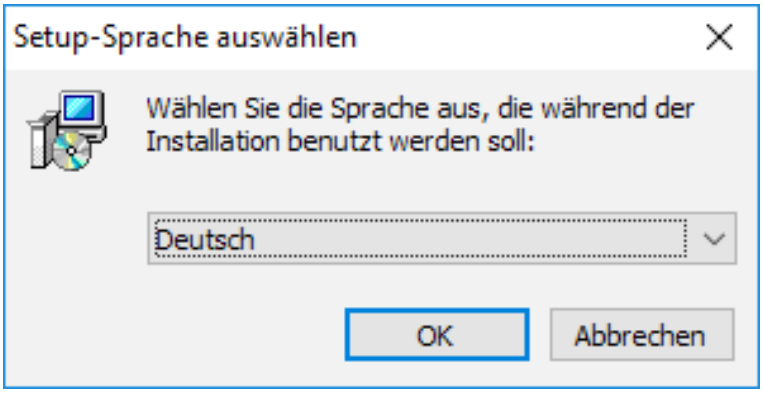
8. Zeile:
Automatisches Abmelden nach x Minuten:
0 = Aus
1 bis 15 Min. bis der Benutzer abgemeldet wird

Installationsanleitung

Installation

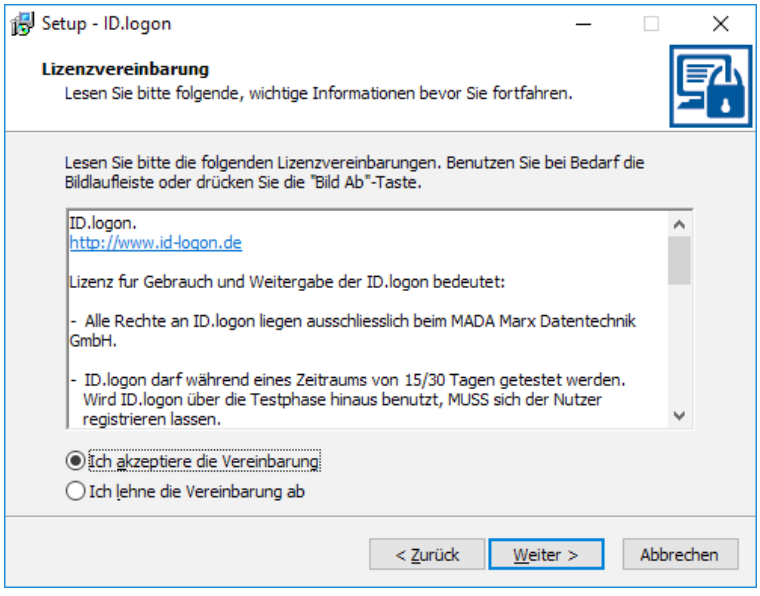
Schritt 3:
Starten Sie die ID.logon Installation durch Doppelklick auf **id-logon-setup.exe**.

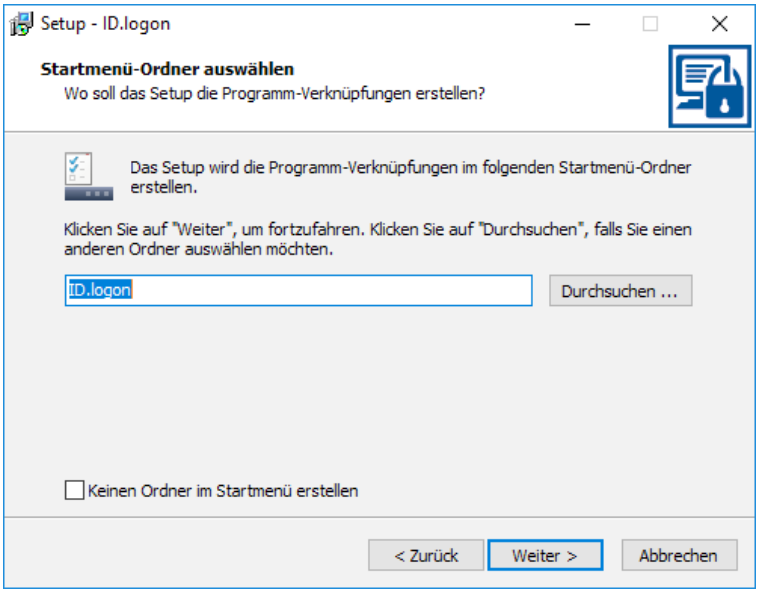
Bitte stellen Sie im Vorfeld einer ID.logon Installation immer sicher, dass alle Programme gespeichert und geschlossen sind. Nach erfolgter Installation von ID.logon muss das System neu gestartet werden.
Wählen Sie die bevorzugte Sprache aus. ID.logon ist in den Sprachen Englisch und Deutsch verfügbar.



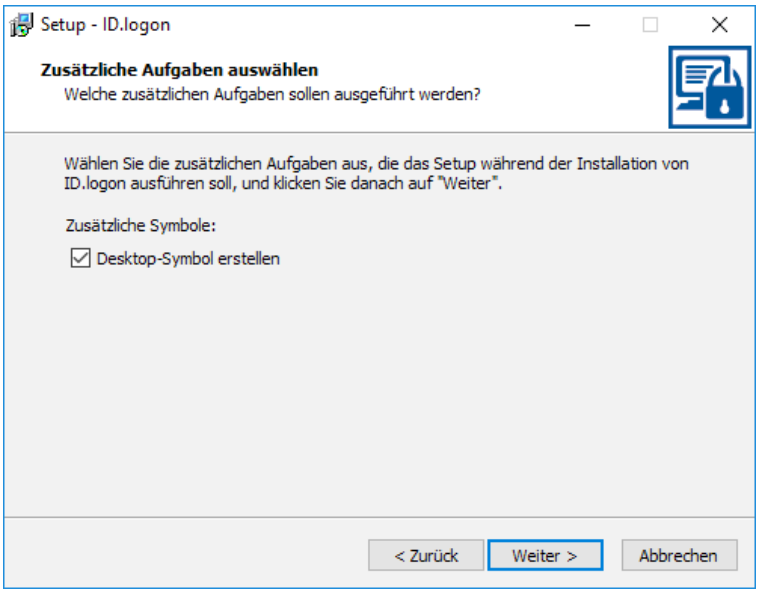
Hier werden Ihnen einige Informationen über ID.logon angezeigt. Klicken Sie auf **„Weiter >“** um mit der Installation fortzufahren

Auf dieser Seite des Assistenten wird die Lizenzvereinbarung angezeigt. Wenn Sie den Bedingungen zustimmen, wählen Sie bitte **„Ich akzeptiere die Vereinbarung“** und fahren Sie mit **„Weiter >“** fort. Wenn Sie nicht einverstanden sind, wählen Sie bitte **„Ich lehne die Vereinbarung ab“** und klicken Sie auf **„Abbrechen“**. Die Installation wird abgebrochen.

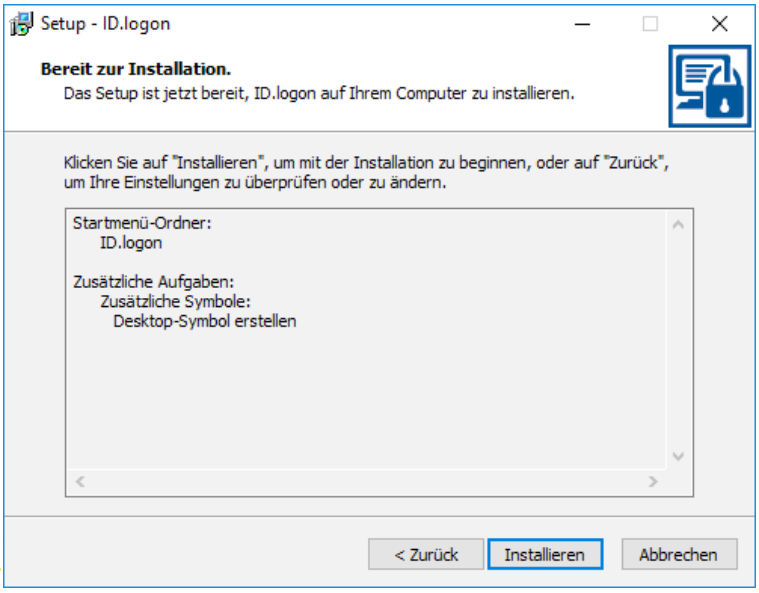




Alle ID.logon Installationen sind kompatibel zu den Windows-Standards. Als Standard-Zielordner ist **C:\Programme (x86)\ID.logon** definiert. Dieser Ordner wird bei der Installation automatisch erstellt. Klicken Sie auf die Schaltfläche **„Durchsuchen...“**, wenn Sie ID.logon an einem anderen Ort auf Ihrem System installieren möchten.



Nun können Sie auswählen, ob ein Desktop-Symbol erstellt werden soll. Klicken Sie anschließend auf **„Weiter >“** um fortzufahren.

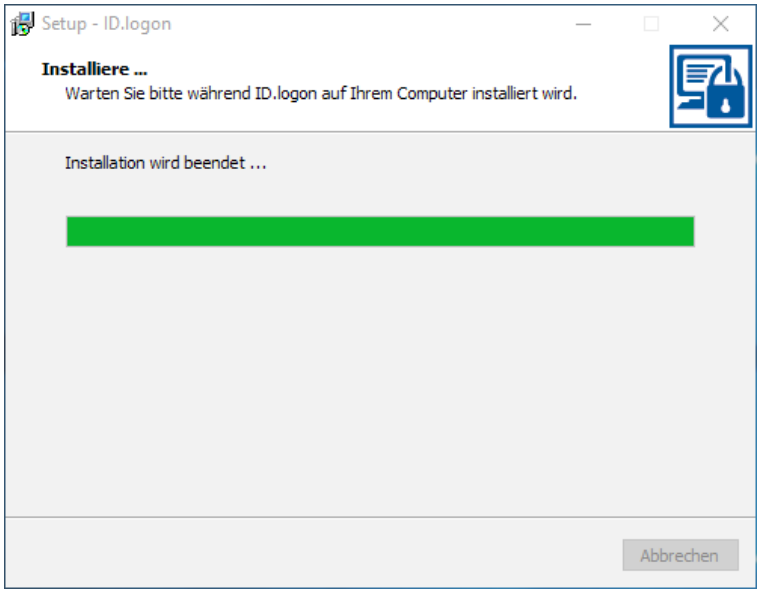


Der Installationsassistent von ID.logon hat alle benötigten Informationen, um mit der Installation zu beginnen. Klicken Sie auf **„Installieren“** um die Installation zu starten.

Installationsanleitung

Installation

Der Status zeigt den Fortschritt des Installationsprozesses. Die Installation kann jederzeit über **„Abbrechen“** beendet werden.

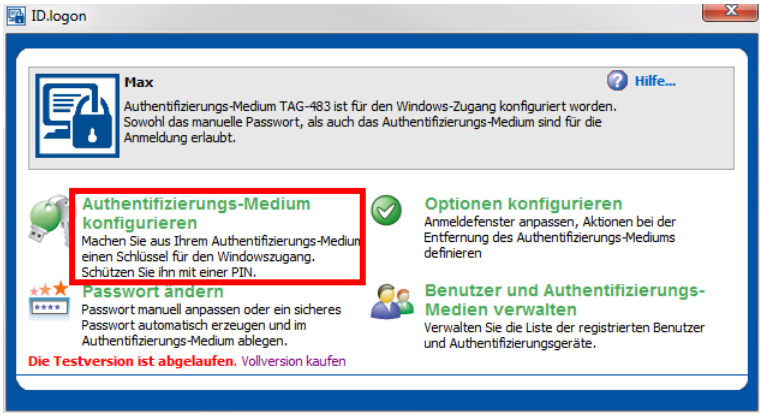


Wenn die Installation erfolgreich abgeschlossen wurde, können Sie wählen, ob das System neu gestartet werden soll **„Ja, Computer jetzt neu starten“** oder ob Sie zu einem späteren Zeitpunkt manuell neu starten **„Nein, ich werde den Computer später neu starten“** wollen.

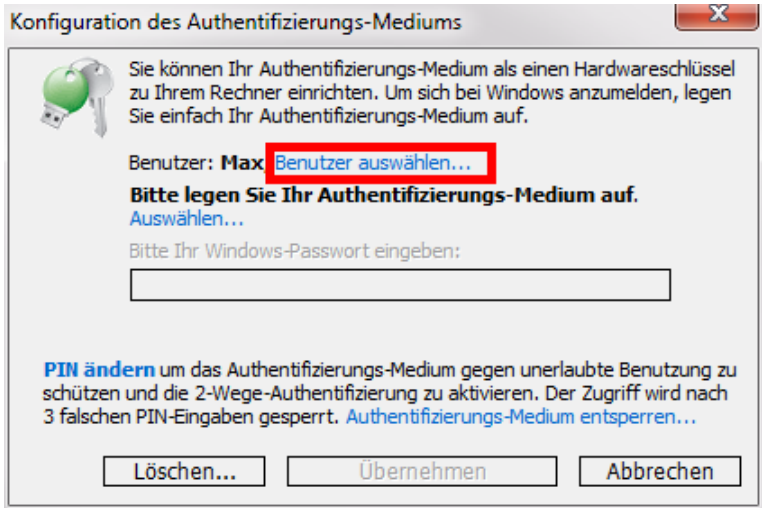
Klicken Sie anschließend auf **„Fertigstellen“** um den Installer zu schließen. Alle temporären Dateien werden von Ihrem System entfernt. Sie können ID.logon durch Doppelklick auf das Desktop-Symbol ausführen oder wählen Sie die Anwendung aus dem Windows-Startmenü.

Konfigurationsanleitung

Authentifizierungs-Medium einrichten



Öffnen Sie ID.logon und klicken Sie auf **„Authentifizierungs-Medium konfigurieren“.**



Wählen Sie den Benutzernamen für das Authentifizierungs-Medium aus. Als Standard Benutzername wird der Benutzer, der gerade an Windows angemeldet ist, ausgewählt. Möchten Sie den Benutzer ändern, klicken Sie auf **„Benutzer auswählen...“** und ändern Sie den Benutzer. Dieser kann sich auch im AD befinden.

Legen / Stecken Sie Ihr Authentifizierungs-Medium ein. Das Programm wird dann automatisch das Authentifizierungs-Medium erkennen.

Konfigurationsanleitung

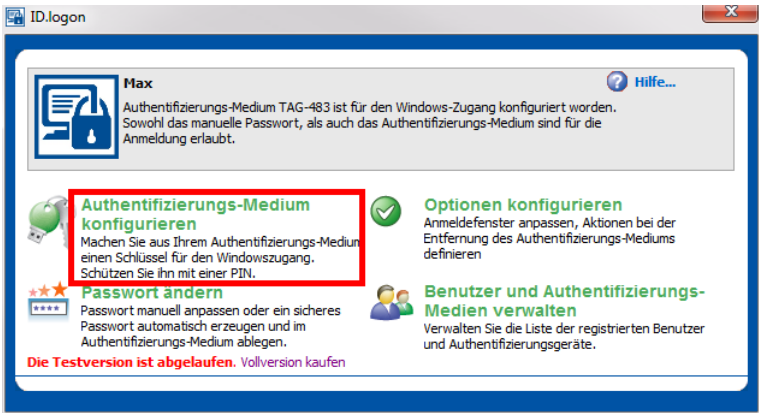
Authentifizierungs-Medium Sicherheit

ID.logon besitzt eigene Sicherheitsstandards für Authentifizierungs-Medien:

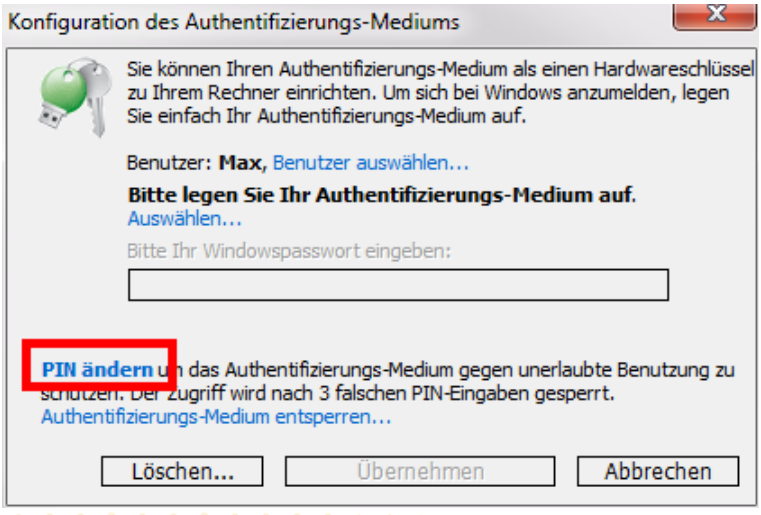
- Ein Authentifizierungs-Medium kann nicht dupliziert werden. Es ist unmöglich ein Duplikat zu erstellen oder Dateien auf ein anderes Authentifizierungs-Medium zu kopieren, weil die Anmeldedateien mit einer eindeutigen Nummer des Authentifizierungs-Mediums verbunden sind.
- Standardmäßig werden alle Anmeldedateien verschlüsselt. Auf Ihrem Authentifizierungs-Medium wird kein Windows Passwort in einfacher Form abgespeichert. Das Passwort wird aus einer Kombination von Seriennummer, Passwort und einem zusätzlichen Schlüssel, verschlüsselt auf dem Authentifizierungs-Medium abgelegt. Bei der Anmeldung entschlüsselt ID.logon das Passwort wieder.
- Sie können einen **2-Faktor Authentifizierungs** PIN Code für Ihr Authentifizierungs-Medium einstellen - Der PIN besteht aus Zahlen von 0-9. Diese PIN müssen Sie jedes Mal eingeben, wenn Sie sich bei Windows anmelden möchten.

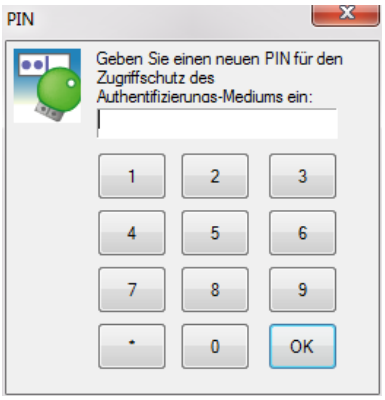
PIN-Code erstellen

Das Authentifizierungs-Medium kann mit einem PIN-Code aus den Zahlen 0-9 versehen werden, um das Authentifizierungs-Medium gegen unbefugte Nutzung für die Anmeldung zu schützen. Sie müssen den gültigen PIN-Code jedes Mal wenn Sie sich anmelden, eingeben. Wenn Sie den PIN-Code öfter als 3 Mal falsch eingeben, wird das Authentifizierungs-Medium blockiert und Sie können es nicht mehr für die Anmeldung verwenden.
Öffnen Sie ID.logon und klicken Sie auf **„Authentifizierungs-Medium konfigurieren“.**



Wählen Sie dann **„PIN ändern“** aus, um den Authentifizierungsmedium einen PIN-Code zuzuordnen.





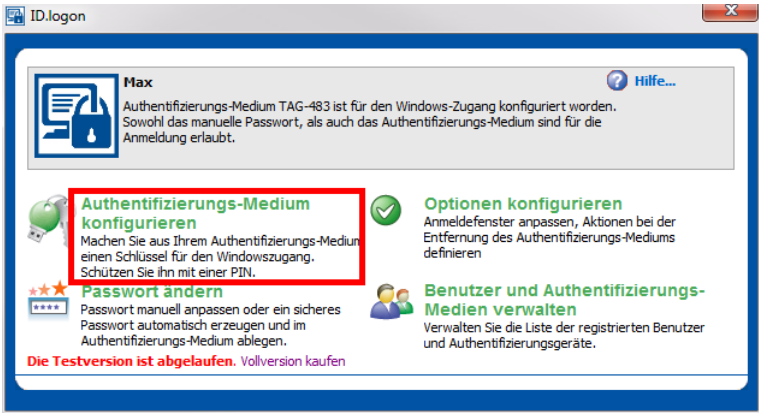
Wurde bereits ein PIN-Code erstellt, so muss zuerst der alte PIN eingegeben werden, bevor dann 2 -Mal der neue PIN-Code eingegeben werden kann.
Geben Sie nun einen PIN-Code ein und klicken Sie auf **„OK“**.
Wiederholen Sie die Eingabe und klicken Sie erneut auf **„OK“**.

Konfigurationsanleitung

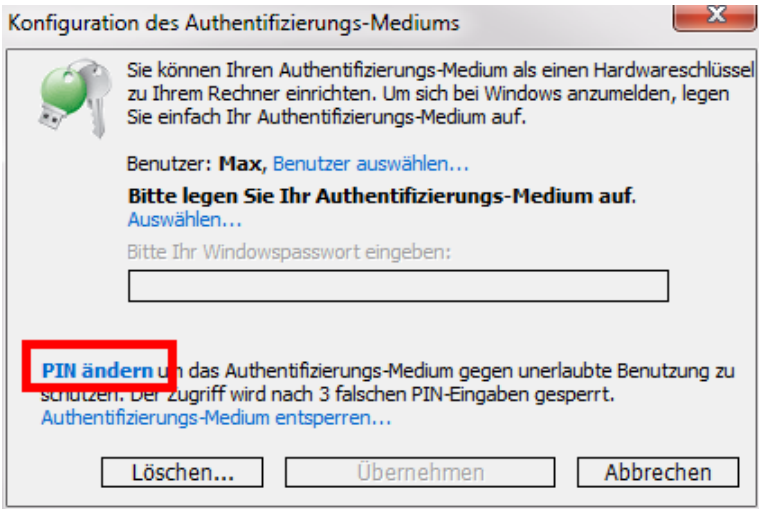
Authentifizierungs-Medium Sicherheit

PIN-Code ändern

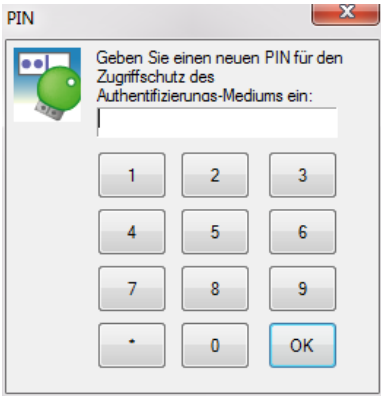
Öffnen Sie ID.logon und klicken Sie auf **„Authentifizierungs-Medium konfigurieren“.**



Wählen Sie dann **„PIN ändern“** aus, um den Authentifizierungsmedium einen PIN-Code zuzuordnen.



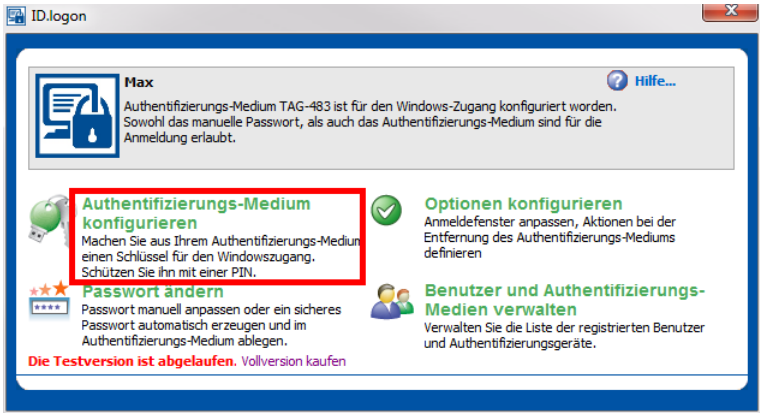
Wurde bereits ein PIN-Code erstellt, so muss zuerst der alte PIN eingegeben werden, bevor dann 2-mal der neue PIN-Code eingegeben werden kann.
Geben Sie nun einen PIN-Code ein und klicken Sie auf **„OK“**.
Wiederholen Sie die Eingabe und klicken Sie erneut auf **„OK“**.



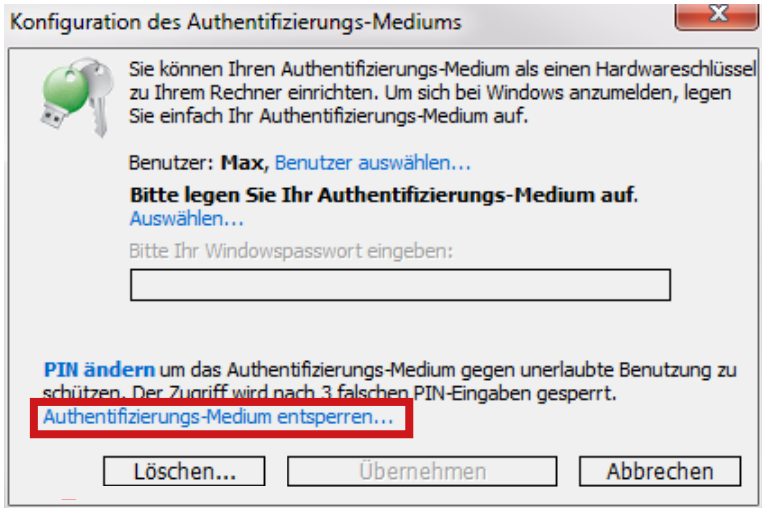
Warnung:
Bei 3 falschen PIN Eingaben wird der Zugang mit dem Authentifizierungs-Medium gesperrt. Der User kann sich dann nur noch mit der Notanmeldung einloggen.

* Default PIN für Authentifizierungs-Medien – wenn Sie 1111 oder 0123456789 (andere Token) als PIN eingeben, wird ID.logon die PIN Abfrage nicht mehr anzeigen.

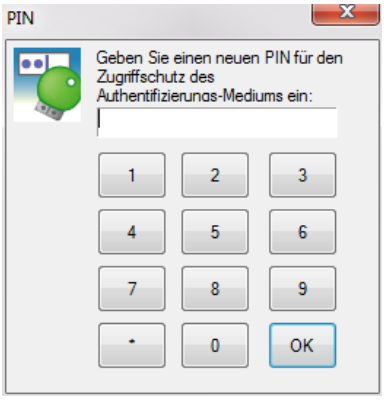
Authentifizierungs-Medium entsperren



Öffnen Sie ID.logon und klicken Sie auf **„Authentifizierungs-Medium konfigurieren“.**



Wählen Sie dann **„Authentifizierungs-Medium entsperren...“** aus, um das Medium zu entsperren.



Geben Sie Ihren PIN-Code für Ihr Authentifizierungs-Medium ein und klicken Sie auf **„OK“**.

* Nur wenn Sie die ID.Logon Enterprise Version haben, ist diese Funktion freigeschaltet

Konfigurationsanleitung

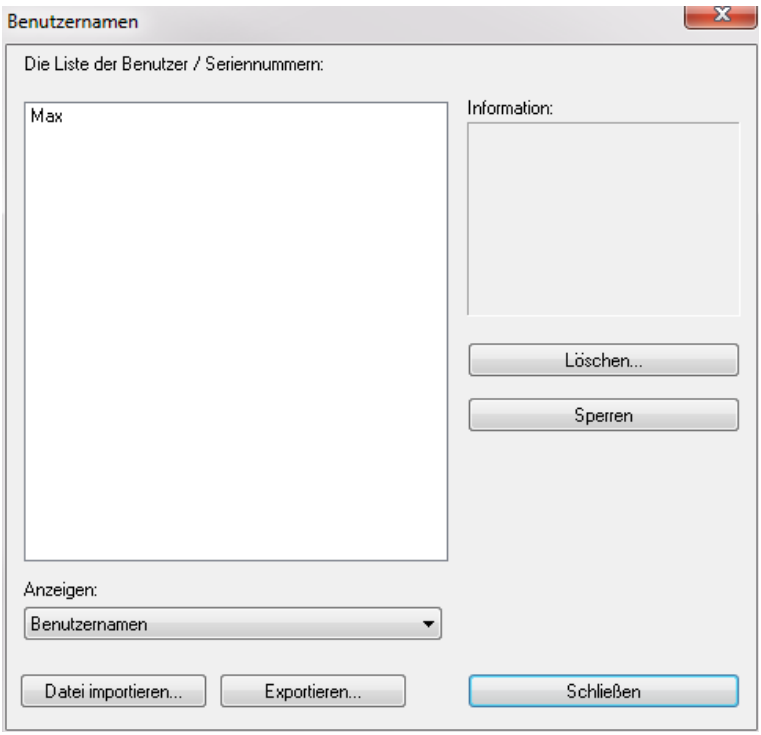
Authentifizierungs-Medium Verwaltung

Liste mit Benutzer und Authentifizierungs-Medien

Klicken Sie im Hauptfenster auf **„Benutzer und Authentifizierungs-Medien verwalten“** und ein Dialogfenster öffnet sich. In diesem Fenster sind alle angelegten Benutzer und Authentifizierungs-Medien, die auf diesen Computer Zugriff haben, hinterlegt. Wählen Sie einen beliebigen Benutzer aus und im Fenster **„Informationen“** werden die Seriennummer des Authentifizierungs-Mediums und der vollständige Benutzernamen angezeigt, z.B. Benutzername@Computername oder Benutzername@Domäne.

Werden mehrere Benutzernamen angezeigt, bedeutet das, dass das Authentifizierungs-Medium mehrere Benutzer Profile gespeichert hat und man sich mit diesem Authentifizierungs-Medium mit unterschiedlichen Benutzern anmelden kann.

Unter **„Anzeigen“** können Sie **„Seriennummer“** oder **„Benutzernamen“** auswählen. Haben Sie **„Seriennummer“** ausgewählt, wird anstatt der Liste der Benutzernamen die Liste mit Seriennummern der Authentifizierungs-Medien, die für den Login auf diesem Computer verwendet werden, angezeigt.

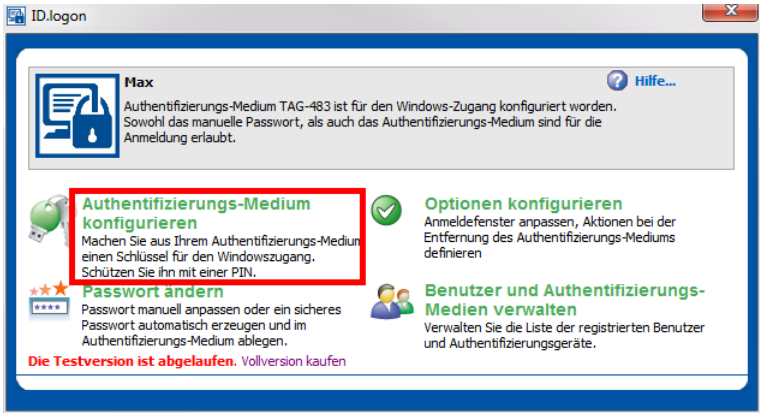


Mit einem Klick auf **„Löschen“**, können Sie den Benutzernamen oder das Authentifizierungs-Medium aus der Liste löschen. Klicken auf die Schaltfläche **„Sperren“**, können Sie temporär ein Authentifizierungs-Medium sperren. Dabei ändert sich die Schriftfarbe auf Rot. Um das Authentifizierungs-Medium zu entsperren, wählen Sie das Authentifizierungs-Medium oder Benutzernamen aus und klicken Sie auf **„Entsperren“**.

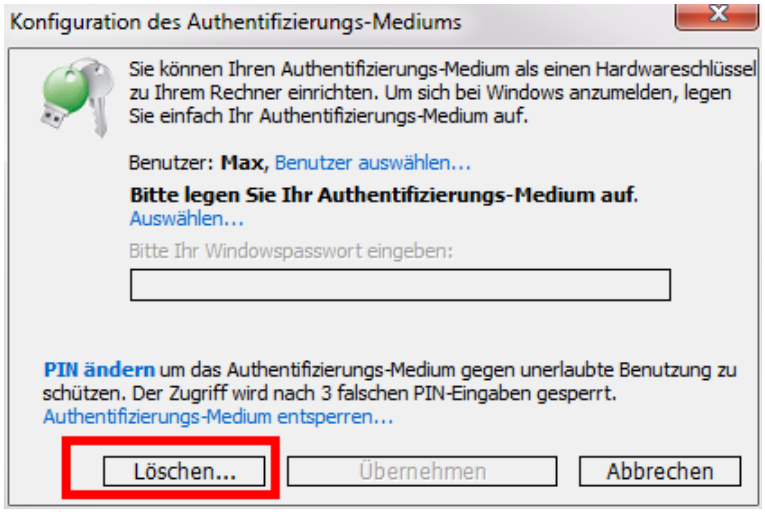
Um die Liste der Authentifizierungs-Medien auf einen anderen Computer zu kopieren, verwenden Sie **„Exportieren...“** und **„Datei importieren...“**.

Achtung:
Die Liste der Authentifizierungs-Medien ist für die Sicherheit sehr wichtig. Wenn die Option **„Authentifizierungsprüfung der Schlüsselseriennummer“** eingeschaltet ist, wird ID.logon Authentifizierungs-Medien, die nicht in der Liste sind nicht zulassen. Ist diese Einstellung nicht gesetzt, können auch Authentifizierungs-Medien die zentral angelegt wurden, sich an diesem System anmelden.

Authentifizierungs-Medium löschen



Öffnen Sie ID.logon und klicken Sie auf **„Authentifizierungs-Medium konfigurieren“.**



Wenn Sie alle Dateien vom Authentifizierungs-Medium löschen wollen, die ID.logon installiert hat, klicken Sie **„Löschen...“**.

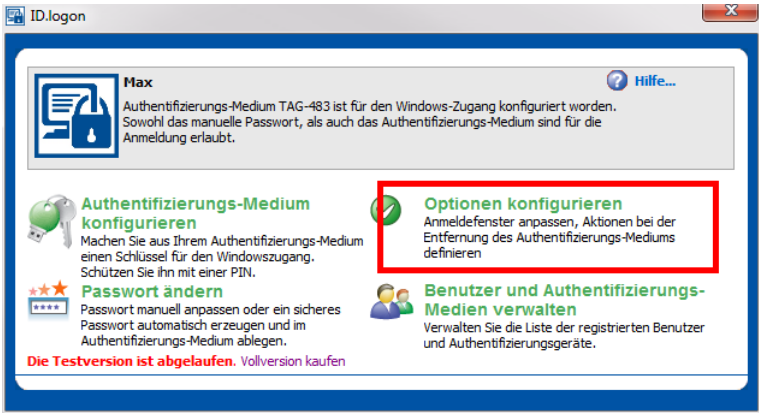
ID.logon wird beim Löschen des letzten Authentifizierungs-Mediums auch die Einstellung
„Erlaube Anmeldung: Für alle Benutzer nur mit Authentifizierungs-Medium“ löschen.

Konfigurationsanleitung

Authentifizierungs-Medium Verwaltung

Optionen konfigurieren

Mit einem Klick auf **„Optionen konfigurieren“** können Sie den Typ des Authentifizierungs-Mediums auswählen, die Aktion, die nach der Entfernung des Authentifizierungs-Mediums durchgeführt wird, die Art der Anmeldung, Spracheinstellungen u.v.m. nach Ihren Bedürfnissen einstellen.



ID.logon Anmeldefenster (gina.dll)

ID.logon installiert sein eigenes Anmeldefenster ähnlich zum Windows Anmeldefenster:

- Es besteht die Möglichkeit das Hintergrundbild auszublenden

Standardanmeldung von Windows (msgina.dll)

Die beste Konfiguration für:

- Windows 2008, 2012, 2016 Server (wenn Sie einen Zugang zu einem Remotedesktop mit Hilfe von Authentifizierungs-Medien vorhaben)
- Windows 2000/ Workstations mit Windows Domäne oder Novell Netzwerk.

In diesem Fall ersetzt ID.logon GINA.dll das Windows Anmeldefenster nicht und lässt das Sicherheitssystem unverändert. ID.logon unterstützt die Integration mit msgina.dll, nwgina.dll, ctxgina.dll.

ID.logon Credential Provider in Windows

Die neue Komponente ID.logon Credential Provider, die speziell ab Windows Vista entwickelt wurde, integriert sich ins Interface des Betriebssystems und wird als Bestandteil des Betriebssystems betrachtet. ID.logon Credential Provider wird im Anmeldefenster von Windows mit einem eigenen Icon und Namen **„Anmelden mit Authentifizierungs-Medium“** dargestellt. Beim Einstecken/Auflegen des konfigurierten Authentifizierungs-Mediums liest das Programm die Daten des Benutzerskontos und das Passwort für die Anmeldung aus. Wurde zusätzlich eine PIN Abfrage eingestellt, so wird diese von dem Authentifizierungs-Medium angefordert.

- ID.logon Credential Provider unterstützt x86, x64 Systeme.
- Wenn Sie die Funktion **„Für alle Benutzer nur mit Authentifizierungs-Medium“** wählen, wird der Standard Credential Provider ausgeschaltet.

Anmerkung: Beim Einstellen der Funktion **„Für alle Benutzer nur mit Authentifizierungs-Medium“** werden alle Benutzerkonten deaktiviert, aktiv bleibt nur der ID.logon Credential Provider.

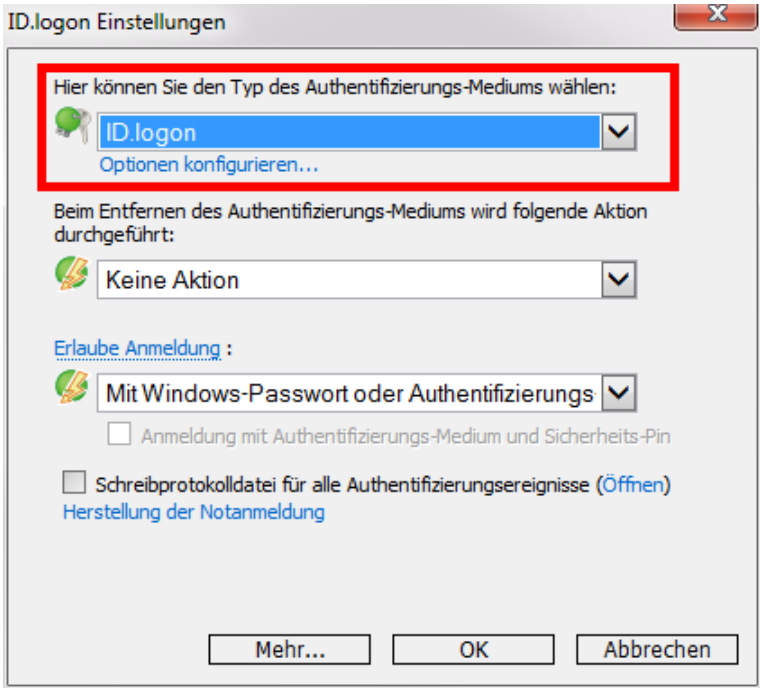
Typen des Authentifizierungs-Mediums

Das Programm ID.logon unterstützt alle gängigen 125 kHz und 13,56 MHz RFID-Transponder:

Mifare	LEGIC	HITAG	EM	I-Code	Temic	TI
Classic	prime	HITAG 1	4450	SLI S20	Q5	TAG IT
DESFire	advant	HITAG 2	4102/4200		ATA 5577	
Ultralight	CTC 4096	HITAG-S	4150			

ID.logon unterstützt:

- RFID Transponder
- RFID Reader
- USB Sticks
- Bluetooth Geräte
- biometrische USB Sticks
- PKCS#11 security module
- YubiKey
- Swekey
- Easyident/Addimat
- RFID CR10MW
- PC Lock USB Dongle
- JCard V2M
- Google Authenticator (OATH)
- Mobile phone (Android/iOS)



Als Default Einstellung verwendet ID.logon, das von Ihnen gekaufte Authentifizierungs-Medium als Indentifikation für den Zugang zum PC.
Für Bluetooth Einrichtungen unterstützt das Programm die Funktion der 2-Faktor Authentifizierung nicht.

Für USB Tokens:

- Das Programm ID.logon verlangt 1-3 KB an Speicher.
- Falls das Authentifizierungs-Medium nach drei erfolglosen Versuchen gesperrt wurde, kann das Authentifizierungs-Medium nur von einem Administrator entsperrt werden.

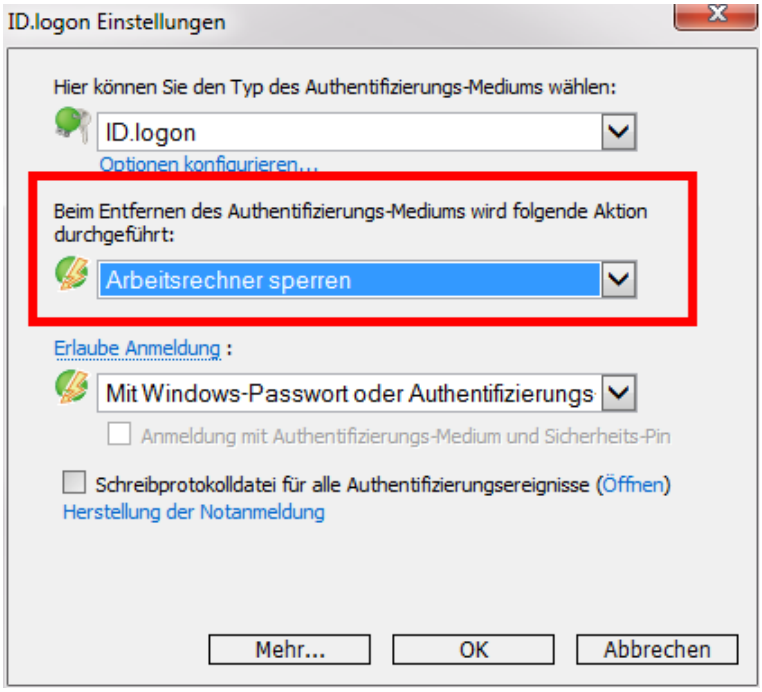
Konfigurationsanleitung

Authentifizierungs-Medium Verwaltung

Verhalten beim Entfernen des Authentifizierungs-Mediums

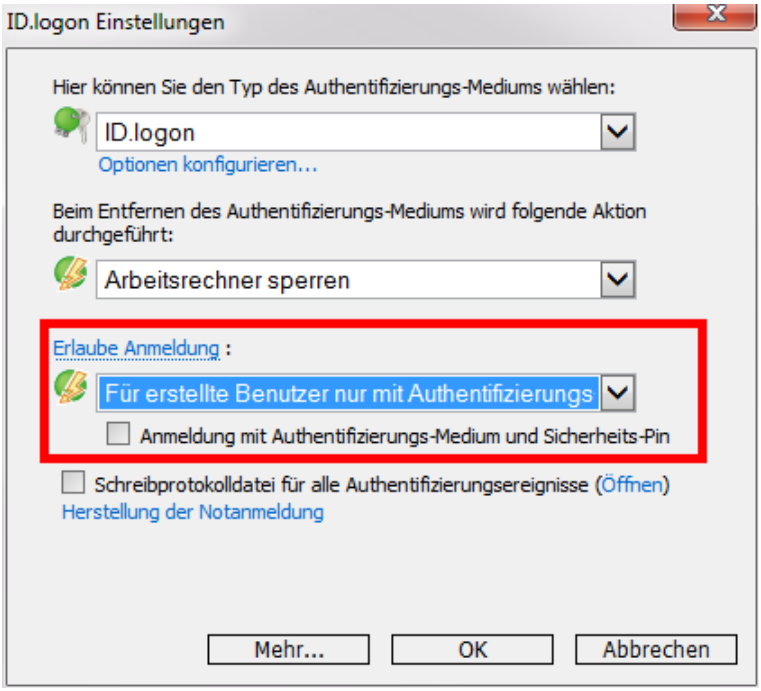
Wenn Sie ein Authentifizierungs-Medium zum Anmelden an Windows verwenden, kann ID.logon folgende Aktionen beim Entfernen des Authentifizierungs-Mediums durchführen:

- Keine Aktion
- Arbeitsrechner sperren
- Sitzung beenden (Abmelden)
- Rechner ausschalten
- Rechner in Ruhestand versetzen
- Bildschirmschoner aktivieren
- Benutzer wechseln



Anmerkung:
Die gewählte Aktion wird automatisch durchgeführt, wenn Sie Ihr Authentifizierungs-Medium entfernen. Durch Auflegen Ihres Authentifizierungs-Mediums können Sie sich dann wieder anmelden.

Erlaube Anmeldung:



- **Mit Windows-Passwort oder mit Authentifizierungs-Medium** – jeder Benutzer kann sich entweder durch die Verwendung eines Authentifizierungs-Mediums oder durch manuelle Eingabe des Benutzernamens und Passwortes anmelden.
- **Für alle Benutzer nur mit Authentifizierungs-Medium** – jeder muss ein Authentifizierungs-Medium auflegen, die Anmeldung ohne Authentifizierungs-Medium ist nicht mehr aktiv.
- F**ür erstellte Benutzer nur mit Authentifizierungs-Medium** – Benutzer aus der Liste **„Benutzer und Authentifizierungs-Medium verwalten“** können Sie sich nur noch mit einem Authentifizierungs-Medium anmelden. Alle Benutzer, die nicht auf der Liste stehen, können sich wie gewohnt mit Benutzername und Passwort anmelden.
- **Für ID.logon Benutzergruppe im Active Directory** – Mitglieder der **„ID.logon“** Benutzergruppe müssen Authentifizierungs-Medien nutzen, um auf ihre Konten von Workstations zugreifen zu können.
- **Für Remote Desktop Login** – nur mit Authentifizierungs-Medien ist die Remote-Desktop-Anmeldung möglich.
- F**ür Remote Desktop Login außerhalb LAN** – nur mit Authentifizierungs-Medien ist die Remote-Desktop-Anmeldung (außerhalb des lokalen Netzwerks, aus dem Internet) möglich.

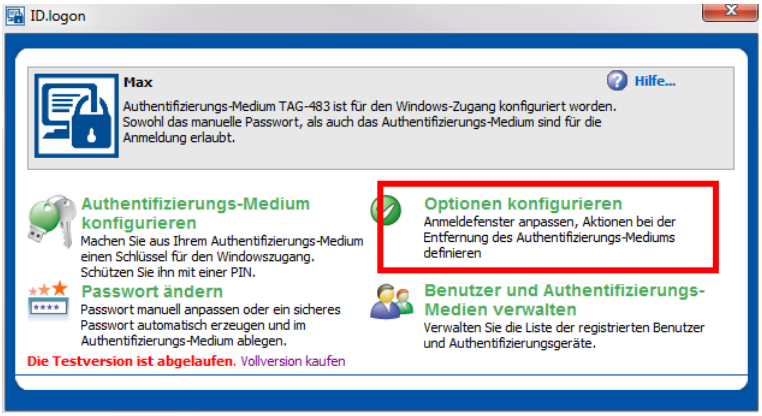
Konfigurationsanleitung

Authentifizierungs-Medium Verwaltung

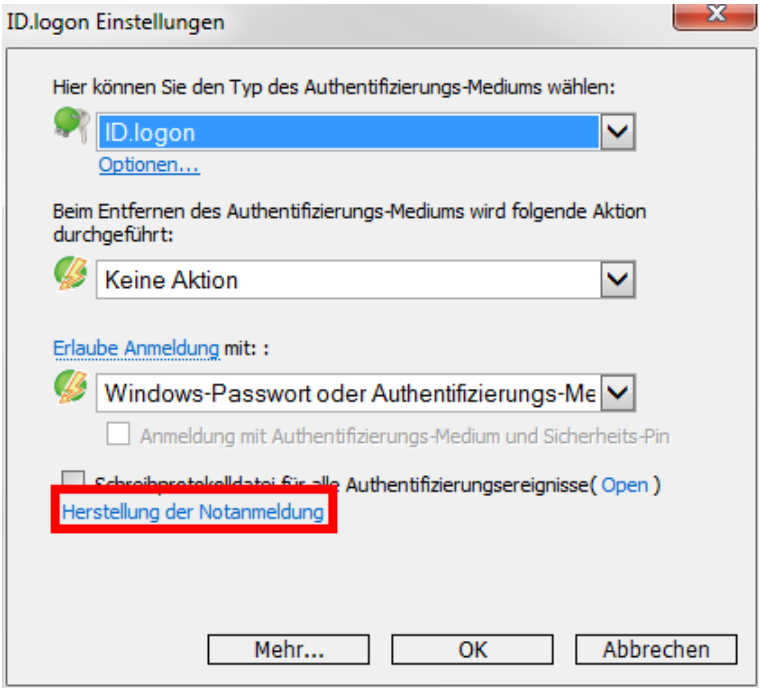
Notanmeldung

Die Notanmeldung ermöglicht den Zugang zu Ihrem Windows, falls das Authentifizierungs-Medium verloren oder beschädigt ist, oder wenn Sie die PIN vergessen haben.

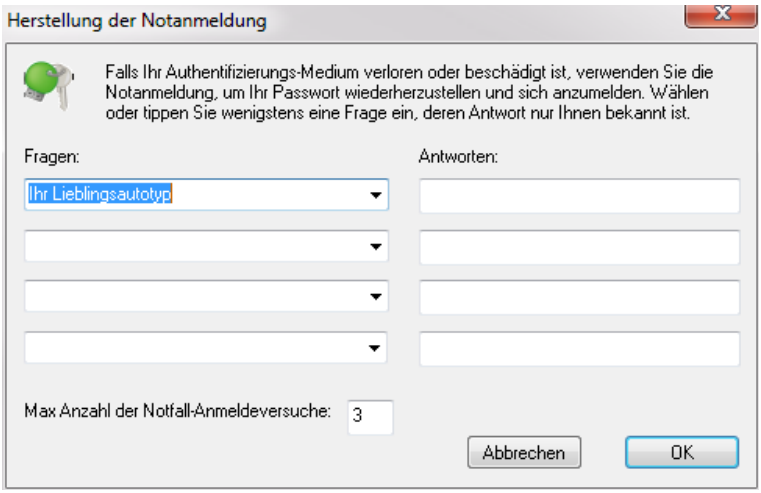
Öffnen Sie ID.logon, klicken SIe auf **„Optionen konfigurieren“**



Anschließend auf **„Herstellung der Notanmeldung“** klicken.



Wählen Sie in der linken Spalte eine vordefinierte Frage (oder geben Ihre eigene ein) aus und beantworten Sie diese in der rechten Spalte.
Wiederholen Sie das Ganze bis zu viermal (der Benutzer kann eine, zwei, drei oder alle vier Fragen beantworten). Wenigstens zwei Fragen werden empfohlen.
Geben Sie eine Zahl für die **„Max Anzahl der Notfall-Anmeldeversuche“** ein.



Achtung:

Zu jeder Zeit können Sie die Notanmeldung neu konfigurieren. Das beeinträchtigt die Sicherheit des Systems oder des Authentifizierungs-Mediums nicht.

Bei jeder Notanmeldung haben Sie genau die Anzahl an Versuchen, die Sie zuvor eingestellt haben, um die richtigen Antworten einzugeben. Danach wird das Notanmeldefenster gesperrt.

Die misslungenen Versuche werden von ID.logon aufgenommen und Ihnen mitgeteilt. Somit sehen Sie, wenn sich eine unbefugte Person, Zugang zu Ihrem Login verschaffen wollte.

In einem Notfall (wenn das Authentifizierungs-Medium verloren oder beschädigt ist)

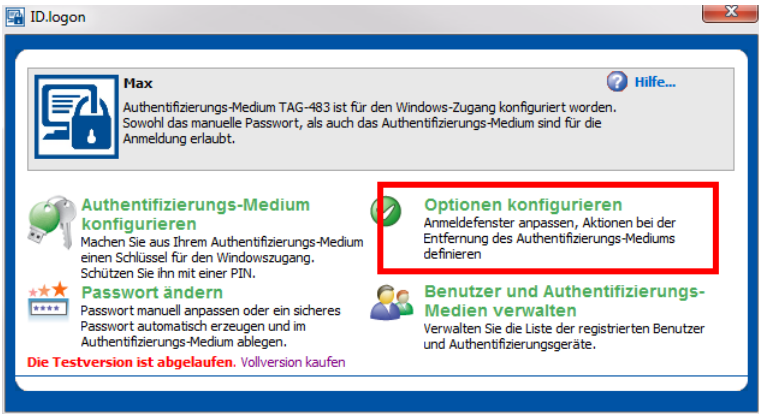
- Klicken Sie zweimal auf das blaue ID.logon Icon im Anmeldefenster und geben Sie Ihren Benutzernamen und danach die richtigen Antworten auf die Fragen ein.
- Die Eingabe der Antworten ist nicht sensibel, Sie können z.B. „Green“ oder „green“ antworten.
- Danach können Sie entweder ein neues Passwort eingeben oder das alte Passwort beibehalten. Mit dem Passwort können Sie sich dann wieder manuell bei Windows anmelden.

Konfigurationsanleitung

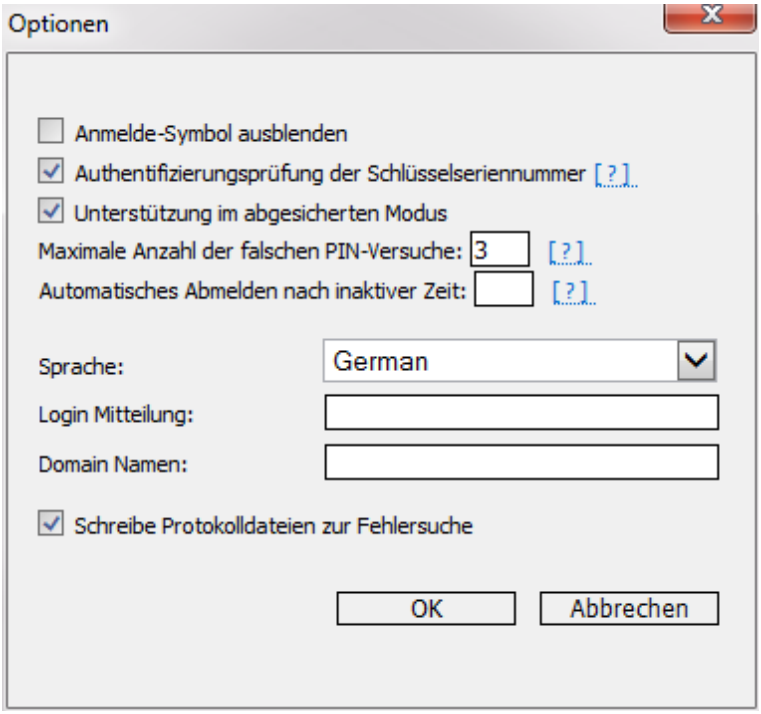
Authentifizierungs-Medium Verwaltung

Weitere Optionen

Klicken Sie auf **„Optionen konfigurieren“**



Klicken Sie anschließend auf **„Mehr...“**:



- **Anmelde Symbol ausblenden**: Das Anmelde-Symbol wird beim Setzen des Hackens ausgeblendet.
- **Authentifizierungsprüfung der Schlüsselseriennummer**: Nur Authentifizierungs-Medien aus der Liste der **„Benutzer und Authentifizierungs-Medium verwalten“** können an diesem Computer verwendet werden. Diese Liste kann von einem anderen Computer importiert werden. Ist diese Einstellung nicht gesetzt, können sich auch Authentifizierungs-Medien die zentral angelegt wurden, an diesem System anmelden.
- **Authentifizierungs-Medium im Abgesicherten Modus**: Es ist möglich sich im Abgesicherten Modus ebenfalls mit einem Authentifizierungs-Medium anzumelden. Wenn dazu noch die Funktion **„Für alle Benutzer nur mit Authentifizierungs-Medium“** unter **„Erlaube Anmeldung:“** aktiviert ist, dann ist die Eingabe des Passwortes im Abgesicherten Modus auch verboten. Das heißt, man kann sich dann nur noch mit Authentifizierungs-Medium im Abgesicherten Modus anmelden.
- **Maximale Anzahl der falschen PIN Versuche**: Bevor das Authentifizierungs-Medium gesperrt wird
- **Automatisches Abmelden nach Inaktiver Zeit:** Nach der Eingestellten Zeit wird der Benutzer automatisch abgemeldet
- **Sprache**: Sprachauswahl des Programms (Englisch oder Deutsch)
- **Login Mitteilung**: Mitteilung beim Einloggen jedes Benutzers
- **Domain Namen**: Name der Domäne

Windows Passwort ändern

Hinweis:
Passwort kann nur Lokal geändert werden wenn ID.logon Key Manager nicht im Einsatz ist. Wird ID.logon Key Manager verwendet dann schauen Sie bitte unter Key Manager.

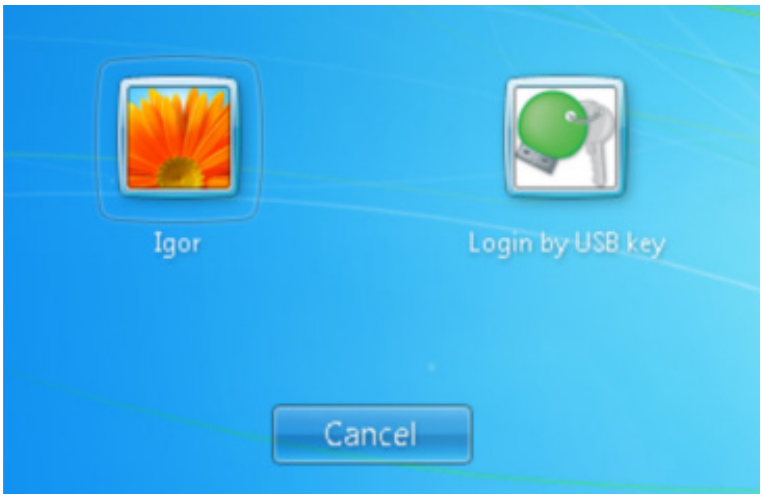
Es gibt zwei Möglichkeiten, um das Windows Passwort zu ändern:

1. Für Windows Vista und neuer

Drücken Sie **Alt + Strg + Entf**, wählen Sie Passwort ändern

Klicken Sie auf **„Andere Anmeldeinformationen“**

Klicken Sie auf **„Login von Authentifizierungs-Medium“**



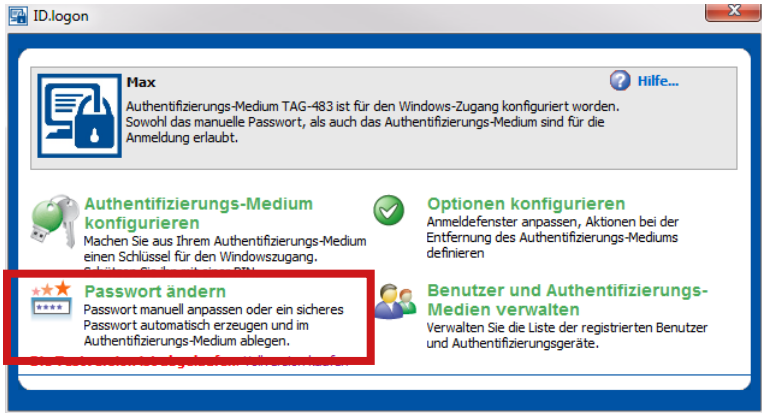
Konfigurationsanleitung

Authentifizierungs-Medium Verwaltung

Stecken / Legen Sie Ihr Authentifizierungs-Medium auf, geben Sie Ihr neues Kennwort ein und klicken Sie auf **„bestätigen“**.

2. Für alle Versionen von Windows:

Starten Sie ID.logon und wählen Sie **„Passwort ändern“**.



Sie müssen Ihr aktuelles Windows Passwort eingeben und im nächsten Feld geben Sie ein neues Windows Passwort ein. Diese Eingabe wiederholen Sie in dem Feld **„Bestätigung“**.
Klicken Sie auf den Link **„Anzeigen“**, um das Kennwort, dass Sie eingegeben haben in Reinschrift anzuzeigen.
Klicken Sie **„Passwort ändern“** und das Passwort wird gespeichert. Sowohl auf dem Authentifizierungs-Medium als auch direkt in Windows.

WARNUNG:
„Sicheres Passwort“ generiert ein Passwort aus zufälligen Kombination von Symbolen. Dieses Passwort kann leicht vergessen werden, da es sehr komplex ist. Bitte verwenden Sie es nur, wenn Sie eine **Notfall-Anmeldung** bereits konfiguriert haben.

ID.logon

Smart Authentication

Scan mich!

www.id-logon.de