Anleitung
GiS WinLock Administrator

Manual
GiS WinLock Administrator

Version 3.00

GiS
Gesellschaft für Informatik
und Steuerungstechnik mbH

Höllochstrasse 1
D-73252 Lenningen
Tel. +49 (0)7026 606 0
Fax +49 (0)7026 606 66
Email rfid@gis-net.de
Homepage http://www.gis-net.de/rfid

Inhaltsverzeichnis

1. Einleitung

Das GiS WinLock System dient der Benutzerauthentifizierung von Microsoft Windows™ Computern. Hierbei werden die Betriebssysteme Windows 7™, Windows 8™, Windows 8.1™ und Windows 10™ unterstützt.

Die Benutzerauthentifizierung kann je nach verwendetem Gerät mit verschiedenen 125 kHz oder 13.56 MHz Transpondern erfolgen

1.1. Transponderformat

Mit der „GiS WinLock Administrator“ Software kann der verwendete Transpondertyp eingerichtet werden.
Bei Verwendung eines WinLock LF werden folgende Transpondertypen unterstützt:
Unique, Hitag1, Hitag2, HitagS, Hitagμ, ATA5577, Q5, Titan, EM4305 und EM4569.

Bei Verwendung eines WinLock HF werden folgende Transpondertypen unterstützt:
ISO15693 (ICode SLI, Tag-it, …) und ISO14443 (MIFARE®, MIFARE DESFire®, …).

Außerdem werden mit dieser Software, die zu den Transponder ID Nummern gehörigen Benutzerdaten in den GiS WinLock eingetragen.
In einem GiS WinLock können bis zu 30 Einträge (Benutzer mit der zugehörigen Transponder ID Nummer) gespeichert werden.

1.2. Betriebssysteme

Der GiS WinLock Schutz ist für Microsoft Windows 7™, Windows 8™, Windows 8.1™ und Windows 10™ verfügbar.

1.3. Einbindung im Betriebssystem

Bei der Benutzerauthentifizierung wird die Erkennung des Transponderlesers integriert.
Dies erfolgt durch Installation eines entsprechenden Moduls.

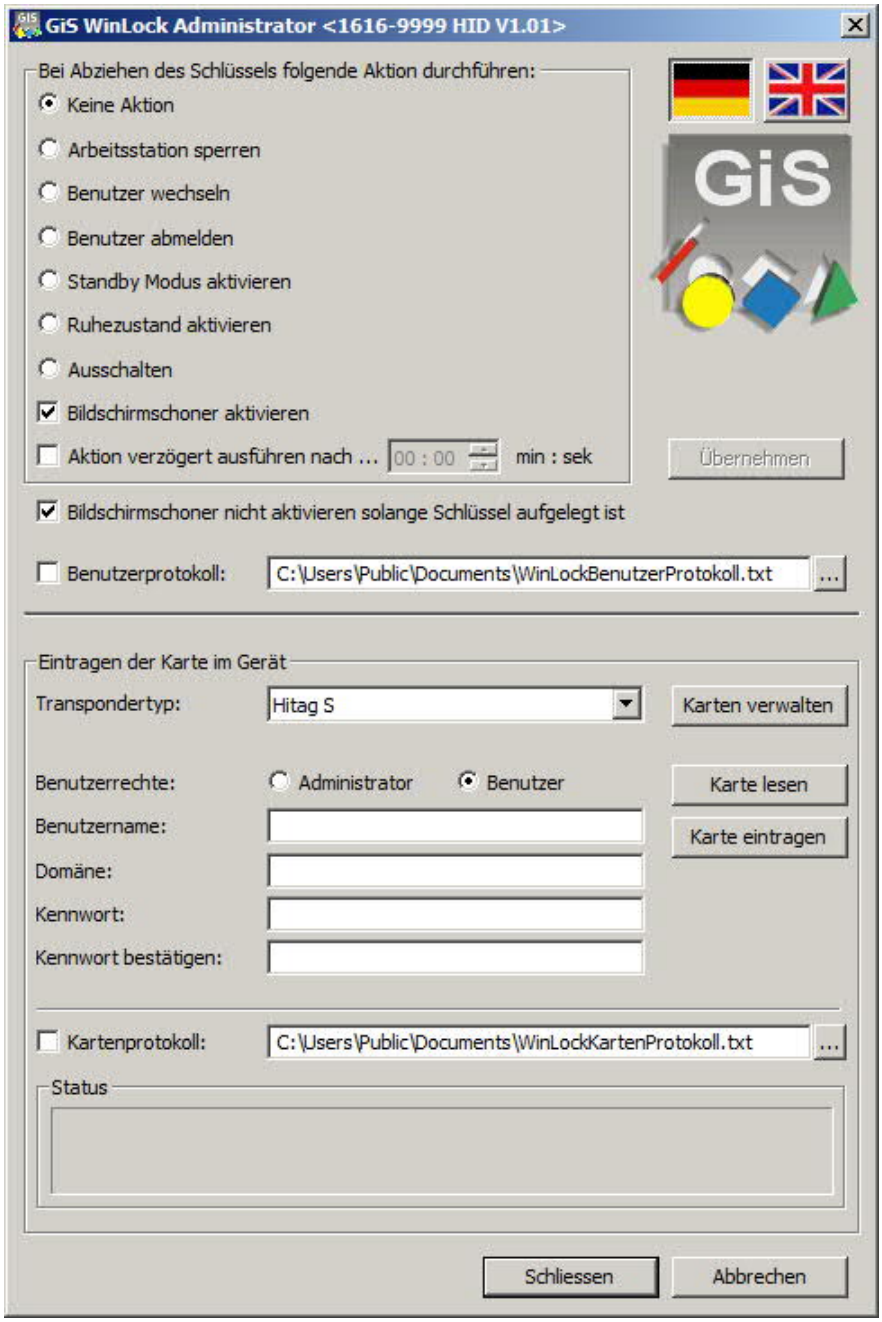
Die Benutzeranmeldung erfolgt automatisch durch den aufgelegten Transponderschlüssel, die Zugangsdaten des Benutzers sind im Lesegerät verschlüsselt gespeichert.

Das Verhalten des Betriebssystems nach Abzug des Transponderschlüssels kann über die "GiS WinLock Administrator" Software eingestellt werden. Diese Anwendung kann nur von Administratoren aufgerufen und die Einstellungen verändert werden.

2. WinLock Administrator

Das Dienstprogramm „GiS WinLock Administrator“ dient der Einstellung der Aktionen, die abhängig vom Transponderschlüssel erfolgen sollen sowie der Einrichtung der Benutzerkarten.

Achtung: „GiS WinLock Administrator“ benötigt zur Ausführung Administratorrechte. Ist die Benutzerkontensteuerung aktiv, oder der angemeldete Benutzer kein Administrator, so kann „GiS WinLock Administrator“ im Administratormodus gestartet werden, indem mit rechter Maustaste auf das Symbol geklickt wird und „Starten als Administrator“ gewählt wird.
Es muss dann ein gültiges Administratorkonto angegeben werden.



2.1. Aktionsauswahl

Aus den ersten sieben Einstellungen kann immer nur eine Aktion aktiv sein.
Die beiden Einstellungen für das Verhalten eines Bildschirmschoners sind separat einstellbar.

Keine Aktion
Die Arbeitsstation wird nicht gesperrt. Nach Entfernen des Schlüssels kann an dem Computer weitergearbeitet werden, der Schlüssel wird nur zur Benutzeranmeldung verwendet, jedoch nicht zur Zugriffssicherung nach der Anmeldung.

Arbeitsstation sperren
Sobald der Schlüssel abgezogen wird, wird die Arbeitsstation ***gesperrt***. Damit ist der Computer vor Zugriff durch unautorisierte Personen geschützt. Der aktuelle Benutzer bleibt weiterhin angemeldet, alle Applikationen des Benutzers bleiben geöffnet, sobald der Schlüssel wieder aufgelegt wird ist der Computer wieder bereit. Vorteil dieser Variante ist, dass die Applikationen des Benutzers geöffnet bleiben, Nachteil ist, dass nur dieser Benutzer die Sperrung des Computers wieder aufheben kann, es ist also kein Benutzerwechsel möglich.

Benutzer wechseln
Sobald der Schlüssel abgezogen wird, wird die Arbeitsstation ***gesperrt*** und der Benutzerwechseldialog aufgerufen. Auch hier ist der Computer sicher geschützt. Der aktuelle Benutzer bleibt weiterhin angemeldet, alle Applikationen des Benutzers bleiben geöffnet, sobald der Schlüssel wieder aufgelegt wird ist der Computer wieder bereit. Es kann jedoch auch durch Auflegen eines anderen gültigen Schlüssels ein anderer Benutzer angemeldet werden. Vorteil dieser Variante ist, dass sowohl die Applikationen geöffnet bleiben also auch beliebige Benutzer sich anmelden können.

Benutzer abmelden
Sobald der Schlüssel abgezogen wird, wird der aktuelle Benutzer ***abgemeldet***. Auch hier ist der Computer sicher geschützt. Wird ein gültiger Schlüssel aufgelegt, so wird der entsprechende Benutzer angemeldet. Vorteil dieser Variante ist, dass beliebige Benutzer sich anmelden können. Nachteil ist, dass alle geöffneten Applikationen bei der Abmeldung geschlossen werden. Gegebenenfalls können nicht gespeicherte Informationen verlorengehen.

Standby Modus aktivieren
Hier wird der Computer in den ***Standby Modus*** versetzt, sobald der Schlüssel entfernt wurde. Zum Einschalten des Computers muss der Einschaltknopf betätigt werden. Nach dem Einschalten ist der zuletzt aktive Benutzer angemeldet und die Arbeitsstation gesperrt. Ist der Schlüssel aufgelegt, so wird die Sperre automatisch aufgehoben. Diese Option ist nur aktivierbar, wenn die Unterstützung des Standby Modus aktiviert ist. Aktivieren mit Schlüssel ist nur möglich, wenn im Gerätemanager für das WinLock Gerät das aktivieren des Computers aus dem Ruhezustand eingerichtet ist.

Ruhezustand aktivieren

Hier wird der Computer in den ***Ruhezustand*** versetzt, sobald der Schlüssel entfernt wurde. Zum Einschalten des Computers muss der Einschaltknopf betätigt werden. Nach dem Einschalten ist der zuletzt aktive Benutzer angemeldet und die Arbeitsstation gesperrt. Ist der Schlüssel aufgelegt, so wird die Sperre automatisch aufgehoben. Diese Option ist nur aktivierbar, wenn die Unterstützung des Ruhezustandes aktiviert ist. Aktivieren mit Schlüssel ist nur möglich, wenn im Gerätemanager für das WinLock Gerät das Aktivieren des Computers aus dem Ruhezustand eingerichtet ist.

Ausschalten

Hier wird der Computer ***ausgeschaltet***, sobald der Schlüssel entfernt wurde. Zum Einschalten des Computers muss der Einschaltknopf betätigt werden.

Bildschirmschoner aktivieren

Mit dieser Option wird erreicht, dass der eingestellte Bildschirmschoner sofort aktiviert wird, wenn der Schlüssel abgezogen wird. Wird der Schlüssel wieder aufgelegt, so wird der Bildschirmschoner deaktiviert. Diese Option allein bietet keine Sicherheit für die Zugriffe auf den Computer. Diese Option hat natürlich nur dann eine Wirkung, wenn auch ein Bildschirmschoner für den angemeldeten Benutzer eingerichtet ist.

Aktion verzögert ausführen nach …

Hiermit kann die oben gewählte Aktion um eine gewisse Zeit verzögert ausgeführt werden. Die Zeit wird in dem rechten Eingabefeld in Minuten : Sekunden eingestellt. Damit kann z.B.: der Bildschirmschoner erst nachdem der Transponder für 20 Sek. entfernt wurde, aktiviert werden.

Bildschirmschoner nicht aktivieren solange Schlüssel aufgelegt ist.

Hiermit wird der Bildschirmschoner solange unterdrückt solange der Schlüssel aufgelegt ist.

Benutzerprotokoll

Durch Aktivieren von „**Benutzerprotokoll**“ kann ein Protokoll aller Benutzervorgänge, das heißt jedes Auflegens und Abziehens eines Transponders angelegt werden. Der Speicherort für die Datei wird im Eingabefeld festgelegt.
Das Benutzerprotokoll hat folgenden Aufbau:

Datum und Uhrzeit	*Gerätename*	*Transponder ID*	*Benutzername*	*Aktion*
01.01.2012 07:12:48	1616-0001			gestartet
01.01.2012 07:12:48	1616-0001	00000101	Max Mustermann	kommt
01.01.2012 17:20:48	1616-0001	00000101	Max Mustermann	geht
01.01.2012 17:23:35				beendet

Hierbei werden die unteren 8 Stellen der Transponder ID gespeichert. Im Gegensatz zum Kartenprotokoll in dem alle 16 möglichen Stellen der Transponder ID gespeichert sind.
Dies bedeutet normalerweise keine Einschränkung, da nur bei ATA5577, Unique, ISO15693 und IS14443 überhaupt Nummern mit mehr als 8 Stellen möglich sind, und auch dort sich die Nummern üblicherweise nur in den unteren 8 Stellen unterscheiden.

Die Spalten im Protokoll sind mit TAB getrennt.
Folgende Aktionen können auftreten:

gestartet	Der Computer wurde gestartet
beendet	Der Computer wurde heruntergefahren
kommt	Der angegebene Benutzerschlüssel wurde aufgelegt
geht	Der angegebene Benutzerschlüssel wurde abgenommen
Leser entfernt	Der WinLock Leser wurde entfernt
Leser vorhanden	Der WinLock Leser wurde angeschlossen

2.2. LED's

	Grün (**an**)	Versorgungsspannung liegt an
	Gelb (**aus**)	Gerät wurde noch nicht von Windows registriert
	Gelb (**an**)	Gerät ist korrekt installiert, keine Karte liegt auf
	Gelb (**blinkend**)	Signalisiert gültige Karte im Bereich
	Rot (**an**)	WinLock nicht aktiv
	Grün (**blinkend**) (1 x pro 2 Sekunden)	Im Ruhezustand ist das Gerät aktiv und weckt den Computer auf, wenn eine Karte aufgelegt wird.

2.3. Einrichten der Transponderkarten

Im GiS WinLock System können unterschiedliche Transpondertypen verwendet werden. Zunächst wird das System für den verwendeten Transpondertyp eingerichtet.

Bei **Transpondertyp** wird der Typ des verwendeten Transponders eingestellt.

Bei **Benutzerrechte** wird angegeben, ob der Transponderschlüssel für einen Benutzer oder für einen Administrator mit Administratorrechten ist.
Dies wirkt sich dann aus, wenn eine Arbeitsstation gesperrt ist. Dann kann sie nur von dem angemeldeten Benutzer oder einen Administrator entsperrt werden.

In **Benutzername**, **Domäne** und **Kennwort** werden der Benutzername die Domäne und das Kennwort eingetragen, wie es auch im Windows Anmeldebildschirm eingetragen werden muss.
Die Domäne kann auch weggelassen werden, wenn keine Domäne verwendet wird.
Das Kennwort wird aus Sicherheitsgründen nicht im Klartext angezeigt.

Mit „**Karte lesen**“ kann ein bestehender Transponderschlüssel ausgelesen werden.
Hierbei wird nur der Benutzername angezeigt.
Das Kennwort wird aus Sicherheitsgründen nicht angezeigt.

Mit „**Karte eintragen**“ wird zunächst geprüft ob ein Transponder aufgelegt ist und bei **Kennwort** und **Kennwort bestätigen** derselbe Eintrag vorhanden ist. Dann werden die gewählten Einstellungen in den GiS WinLock Leser geschrieben und mit dem aufgelegten Transponderschlüssel verknüpft.

Mit „**Karten verwalten**“ wird die Liste der bereits verknüpften Transponder mit den zugehörigen Benutzernamen angezeigt. Dort können einzelne oder auch alle Einträge gelöscht werden oder bearbeitet also für eine UID ein neuer Name oder neues Passwort vergeben werden.
Außerdem kann dort die Kartenliste **exportiert** und **importiert** werden. Damit können die Anmeldeinformationen einfach zwischen WinLock Geräten ausgetauscht werden.

Durch Aktivieren von „**Kartenprotokoll**“ kann ein Protokoll aller Kartenverwaltungsvorgänge angelegt werden. Der Speicherort für die Datei wird im Eingabefeld festgelegt.
Das Kartenprotokoll hat folgenden Aufbau:

Datum und Uhrzeit	*Gerätename*	*Transponder ID*	*Transpondertyp*	*Rechte*	*Domäne*	*Benutzername*	*Aktion*
17.04.2012 15:04:48	1616-9999	0000000000000101	Unique	B		Max Mustermann	erstellt
17.04.2012 15:04:49	1616-9999	0000000000000102	Unique	A	Domain	Erika Mustermann	erstellt
17.04.2012 15:07:23	1616-9999	0000000000000101			Domain	Max Mustermann	gelöscht
17.04.2012 16:16:05	1616-9999	----------	-	-	---	--------	alle gelöscht

Die Spalten im Protokoll sind mit TAB getrennt.
Folgende Aktionen können auftreten:

erstellt	Der Eintrag für den Benutzer wurde erstellt
gelöscht	Der Eintrag des Benutzers wurde gelöscht
alle gelöscht	Alle Einträge im Gerät wurden gelöscht

2.4. Sprachauswahl und Infobox

Über das Systemmenü (Erreichbar durch Rechtsklick auf die Titelzeile) oder durch Anwahl der entsprechenden Sprache kann die Sprache der Applikation ausgewählt werden.

Durch Auswahl von
„Info über GiS WinLock Administrator…“ wird die Info-Box der Applikation angezeigt.

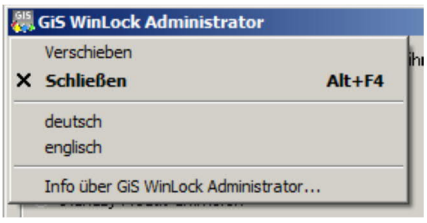


Table of contents

1. Preface

The GiS WinLock System is used for user authentication at Microsoft Windows™ computers. The operating systems Windows 7™, Windows 8™, Windows 8.1™ and Windows 10™ are supported.

The user authentication can be done with different 125 kHz or 13.56 MHz tags, dependent on the used device.

1.1. Transponder format

To prepare the transponders the "GiS WinLock Administrator" software is used.
When using a WinLock LF device the following transponder types are supported:
Unique, Hitag1, Hitag2, HitagS, Hitagμ, ATA5577, Q5, Titan, EM4305 and EM4569.

When using a WinLock HF device the following transponder types are supported:
ISO15693 (ICode SLI, Tag-it, …) and ISO14443 (MIFARE®, MIFARE DESFire®, …).

Also this software is used to write the user entry for the transponder id to the GiS WinLock device.

In one GiS WinLock up to 30 Entries (Users with corresponding Transponder ID Number) can be stored.

1.2. Operating systems

The GiS WinLock protection is available for Windows 7™, Windows 8™, Windows 8.1™ and Windows 10™.

1.3. Integration to the operating system

At the user authentication the transponder reader is integrated.
This is done by installation of a corresponding module.

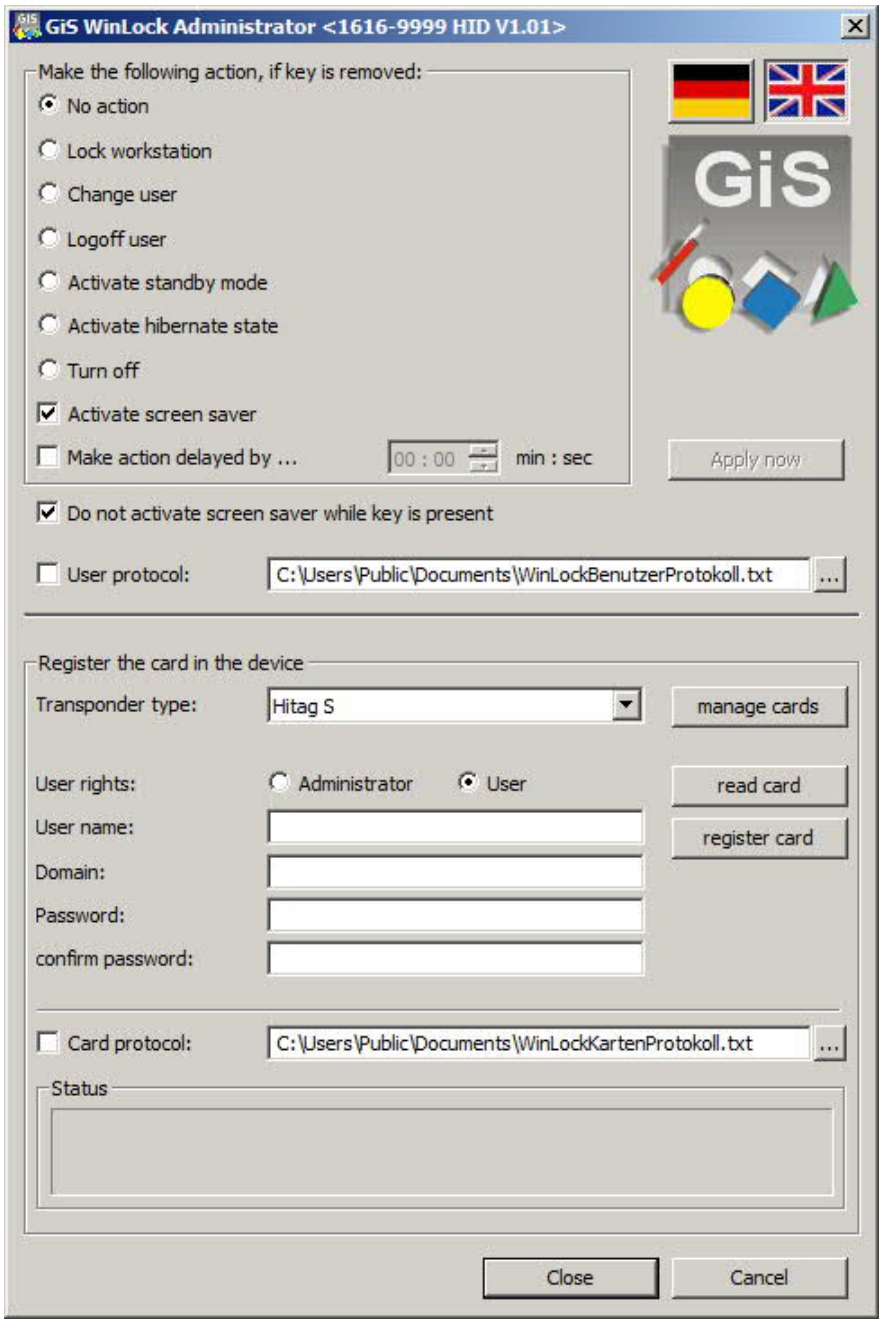
The user logon is done automatically by the given transponder key, the logon data of the user are stored encrypted in the reader device.

The behavior of the system after the key is removed can be adjusted using the "GiS WinLock Administrator" software. This application can be started by any user. But only administrators can change the settings.

2. WinLock Administrator

The “GiS WinLock Administrator” program is used to set up the actions which depend on the transponder key and also to register the user cards.

Application hint: “GiS WinLock Administrator” needs administrator rights to run. If the user account control is active, or the active user is no administrator, the “GiS WinLock Administrator” can be run in administrator mode by clicking with right mouse key to the symbol and select “run as administrator” A valid administrator account has to be given.



2.1. Action selection

There is always one action out of the first six actions active.
The two settings for the screen saver are to be separately chosen.

No action
The workstation is not locked. You can continue work at the computer also if the key is removed. The key is only used for user logon, but not for security reasons after logon.

Lock workstation
If the key is removed, the workstation is ***locked***. With this the computer is protected from access through unauthorized persons. The user is still logged on, so all applications are kept open. As soon as the key is available again, the computer is reactivated. Benefit of the variant is that all applications stay open; disadvantage is that only this user can unlock the computer, no user change is possible.

Change user
If the key is removed, the workstation is ***locked*** and the change user dialog is opened. The computer is securely protected. The user is still logged on, so all applications are kept open. As soon as the key is available again, the computer is reactivated. Also by giving another valid key another user can log on. Benefit of the variant is that all applications stay open and also another user can log on.

Logoff user
If the key is removed, the user is ***logged off***. The computer is securely protected. If a valid key is attached, this user is logged on. Advantage of this variant is that any user can log on. Disadvantage is that all open applications are closed at logoff. Not saved information might be lost.

Activate standby mode
If the key is removed the computer is set to ***Standby mode***. To turn on the computer the power button has to be pressed. After turning on the last active user is logged on and the workstation is locked. If the key is given, the computer is automatically unlocked. To have this option active, the standby mode support has to be enabled. Activation through key is only possible, if the activation of the computer from hibernate or standby mode is activated in the device manager for the WinLock device.

Activate hibernate state

If the key is removed the computer is set to ***Hibernate mode***. To turn on the computer the power button has to be pressed. After turning on the last active user is logged on and the workstation is locked. If the key is given, the computer is automatically unlocked. To have this option active, the hibernate mode support has to be enabled. Activation through key is only possible, if the activation of the computer from hibernate or standby mode is activated in the device manager for the WinLock device.

Turn off

If the key is removed the computer ***turned off***. To turn on the computer the power button has to be pressed.

Activate screen saver

Using this option the given screen saver is activated immediately after removing the key. If the key is given, the screen saver is removed. Using only this option gives no security for access to the computer. Of course this option only takes effect if a screen saver is activated for the user logged on.

Make action delayed by …

To delay the above selected action by an specified amount of time use this option. The delay time is defined in the edit box on the right side with minutes : seconds. With this you can for example activate the screen saver 20 seconds after the key is removed.

Do not activate screen saver while key is present

With this the screen saver is suppressed while the key is on hook.

User protocol

By activating "**User protocol**", a protocol of all user actions, that is every key attachment or removal, is written. The storage place for the file is set in the input field.
The user protocol has the following layout:

Date and time	*Device name*	*Transponder ID*	*User name*	*Action*
01.01.2012 07:12:48	1616-0001			startup
01.01.2012 07:12:48	1616-0001	00000101	Max Mustermann	enter
01.01.2012 17:20:48	1616-0001	00000101	Max Mustermann	leave
01.01.2012 17:23:35				shutdown

The lower 8 digits of the Transponder ID are stored here, in difference to the Card protocol where all 16 possible digits are stored.
This means no limitation in nearly all cases, because more than 8 digits are only possible at ATA5577, Unique, ISO15693 and ISO14443 transponders. And even at these transponders normally only the lower 8 digits are different.

The columns in the protocol are separated with TAB.
The following actions can occur:

Startup	The computer was started
Shutdown	The shutdown was initiated
Enter	The given key was attached
Leave	The given key was removed
Reader removed	The WinLock reader was removed
Reader attached	The WinLock reader ware attached

2.2. LED's

	Green (**on**)	Power ok
	Yellow (**off**)	Device is not registered by Windows
	Yellow (**on**)	Device is correctly installed, no card is attached
	Yellow (**blinking**)	Signals valid card
	Red (**on**)	WinLock not active
	Green (**blinking**) (1 x per 2 seconds)	Device is active in Hibernate mode, awakes the computer if card is attached.

2.3. Setup transponder cards

In the GiS WinLock System different transponder types can be used. First of all the system is set up to the used transponder type.

At **Transponder type** the type of the used transponders is given.

With **User rights** can be selected if the transponder key is for a user or an Administrator with administrator rights.
This takes effect if the workstation is locked. Only the logged on user or an administrator is able to unlock the workstation.

In **User name, Domain** and **Password** the user name, domain and the password are given exactly as they have to be given at the windows logon screen.
The domain can be left off if no domain is used.
The password is not shown as clear text because of security reasons.

Use "**read card"** to read an existing transponder key.
Only the user name is shown, the password is not shown because of security reasons.

If "**register card**" is used, it will be checked if a transponder key is available and in **Password** and **confirm Password** the same input is given. Then the given settings are written to the attached GiS WinLock Reader, and connected to the attached transponder key.

Using "**manage cards**" the list of all registered cards is shown with user name and transponder ID. There, individual or even all entries can be deleted or edited so for a UID a new name or new password can be assigned.
Also the Card list can be **exported** and **imported** there. Using this the Logon information can be easily transferred between WinLock devices.

By activating "**Card protocol**" a protocol of all card management processes can be stored.
The storage place for the file is given in the input field.
The card protocol has the following layout:

Date and Time	*Device name*	*Transponder ID*	*Transponder type*	*Rights*	*Domain*	*User name*	*Action*
17.04.2012 15:04:48	1616-9999	0000000000000101	Unique	B		Max Mustermann	created
17.04.2012 15:04:49	1616-9999	0000000000000102	Unique	A	Domain	Erika Mustermann	created
17.04.2012 15:07:23	1616-9999	0000000000000101			Domain	Max Mustermann	deleted
17.04.2012 16:16:05	1616-9999	----------	-	-	---	--------	all deleted

The columns in the protocol are separated with TAB.
The following actions can occur:

created	the entry for the user was created in the device
deleted	the entry for the user was removed from the device
all deleted	all entries in the device are removed

2.4. Language selection and info box

The language for the application can be chosen using the system menu (accessible by right clicking on the title bar) or by selecting the appropriate language.

Click to "About GiS WinLock Administrator…" to show the about box of the application.