

Power LogOn™ Features List

Identity Theft Protection

- Every computer logon, internet site, and data file can be assigned its own unique, complex password.
- User does not have to remember of type in their passwords.
- No passwords ever stored on the computer for others to access or find.

Issuance options

- End-users self-enroll with their cards, using Power LogOn Password Manager software at end-user computers.
- Or, Administrator loads Power LogOn configuration data to enduser card using Power LogOn CardMaker software.

Security policy management

- Define PIN and password policies, including change reminders and repetition control.
- Define behavior when card is removed from reader: lock, logoff, shutdown computer, or no action.
- Define additional control settings, such as if end-user is allowed to self enroll, PIN verification timeout, if end-user is allowed to change default settings, and more.

And Much More...

System Requirements:

- **Windows based computers**
- **Internet Explorer 5.5+**
- **Pentium 233 MHz or higher**



Power LogOn™ Password Manager

Power LogOn Password Manager is an out-of-the box, smartcard based solution designed to protect users from online identity theft, while also offering easy-to-use password-based account access. Perfect for the small to medium size businesses, as well as the home user who want each individual to be the administrator of their own card.

Power LogOn™ Password Administrator

Power LogOn Administrator has all the features of Password Manager but with the added Power LogOn CardMaker software. Perfect for those businesses and organizations that want a central department for card administration. With CardMaker the administrator can determine user privileges and default settings. Plus the administrator can also issue, replace or revoke cards from the system though CardMaker's database.

Power LogOn™ CardMaker

The Power LogOn CardMaker software enables administrators to easily manage the logon security policies and logon entries of their Power LogOn password manager installation.

Access Smart, LLC
27762 Antonio Pkwy L1-461
Ladera Ranch, CA 92694

Phone: 949-218-8754 • Fax: 949-218-8678 • E-mail: support@access-smart.com

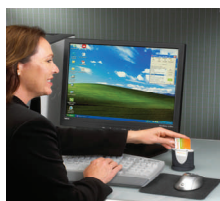


Powered by
Smartcard
Technology™

Power LogOn™ Features List

Website and Application Logon Features

Features	Description	Power LogOn Password Manager	Power LogOn Password Admin.
GINA-based logon to Windows	<p>End-user presents card to card reader and enters card PIN to logon to Windows. Power LogOn transfers logon data to Windows logon process transparently so that keystrokes cannot be observed or recorded.</p> <p>Power LogOn installations use Microsoft GINA-based logon to Windows. Power LogOn software reads user name, password, domain from card (or card server for proximity cards) and passes this data to the Windows logon process on the end-user's computer, via the Microsoft GINA API. Does not replace or change Microsoft GINA; only interacts with relevant functions.</p>	Yes	Yes
End-user managed Windows logon data	<p>Upon first use, cardholder uses Power LogOn Quick Start guide to easily enter their existing Windows logon data into Power LogOn program. With next system reboot, cardholder is prompted to present card and enter PIN to logon to Windows.</p> <p>Note: logon data which end-user saves with Power LogOn cannot be accessed by Administrator.</p>	Yes	Yes
Administrator managed Windows logon data	<p>Administrator may choose to preset Windows logon entry data for individuals or groups of cards. Administrator can also continue to manage Windows logon data for cardholders if desired, by updating Windows logon data in cardholder account.</p> <p>For entries created by Administrator, Administrator can specify if end-user will be allowed to view or</p>		Yes
Storage of multiple Windows logons	<p>For end-users with multiple Windows logon identities or domains, Power LogOn allows entry and selection of multiple logons.</p>	Yes	Yes



Access Smart, LLC
27762 Antonio Pkwy L1-461
Ladera Ranch, CA 92694

Phone: 949-218-8754 • Fax: 949-218-8678 • E-mail: support@access-smart.com

All logos and trademarks are the property of the originating company or individual.



Powered by Smartcard Technology™

Power LogOn™ Features List

Features	Description	Power LogOn Password Manager	Power LogOn Password Admin.
Pull card to lock, logoff, or shutdown computer	<p>End-user can remove card from reader to lock, logoff, or shutdown workstation. Removal of card invokes the appropriate Windows process.</p> <p>Setting can be established by end-user in Power LogOn Password Management software or by Administrator in CardMaker software, as required. Administrator can specify if end-user will be allowed to change this setting.</p> <p>In addition to card-removal behavior, workstation can also be locked using an optional sonar device that detects when end user steps away from workstation. Power LogOn is also compatible with this device.</p>	Yes	Yes
Control Windows "secure screen saver" and "lock workstation" functions from Power LogOn	<p>End-user can "lock" Windows session before stepping away from their desk using Power LogOn short-cut button.</p> <p>End-user can "unlock" a Windows session that has been locked by Windows "secure screen saver" or "lock computer" functions by re-inserting card and entering card PIN.</p>	Yes	Yes
Windows password change synchronization	<p>When end-user changes Windows password in the Power LogOn program, password change will be synchronized with Windows so that end-user does not need to enter the change twice.</p> <p>Likewise, if Windows prompts end-user to change Windows password, and Power LogOn program is currently active, password change will be synchronized with Power LogOn program.</p>	Yes	Yes
Windows password policy control	<p>Administrator can specify required Windows password length and character type (numeric, upper case, lower case...) in the CardMaker software, and end-user must conform to these requirements when entering or changing Windows password.</p>		Yes
Generate random Windows password	<p>When end-user changes Windows password, he/she can generate a random password that conforms to the installation's Windows Password Policy, if applicable. If installation has no Windows Password Policy, end-user can specify password length and character type (numeric, upper case, lower case...) for random password.</p>	Yes	Yes



Access Smart, LLC
27762 Antonio Pkwy L1-461
Ladera Ranch, CA 92694

Phone: 949-218-8754 • Fax: 949-218-8678 • E-mail: support@access-smart.com

All logos and trademarks are the property of the originating company or individual.



Powered by Smartcard Technology™

Power LogOn™ Features List

Features	Description	Power LogOn Password Manager	Power LogOn Password Admin.
Password change reminder	<p>Power LogOn can prompt cardholder to change Windows password every specified number of days.</p> <p>Setting can be established by end-user in Password Manager software or by Administrator in CardMaker software, as required. Administrator can specify if end-user will be allowed to change this setting.</p>	Yes	Yes
Password repetition control	<p>Power LogOn can prohibit the entry of up to four previously used Windows passwords, when cardholder changes Windows password.</p> <p>Administrator can establish setting in CardMaker software.</p>		Yes
Logon to websites and applications	<p>End-user presents card to card reader and enters card PIN to logon to websites and applications. Power LogOn transfers logon data to logon process transparently so that keystrokes cannot be observed or recorded.</p>	Yes	Yes
End-user managed logon entries	<p>Cardholder can use Power LogOn's Quick Start guide to easily auto-record their logon data for websites and applications and save it to their Power LogOn smartcard.</p> <p>The next time cardholder goes to a website or application that Power LogOn knows, cardholder is prompted to present card and enter PIN to logon to website or application.</p> <p>Note: logon data which end-user saves with Power LogOn cannot be accessed by Administrator.</p>	Yes	Yes
Administrator managed logon entries	<p>Administrator may choose to preset logon entry data and load it to end-user Power LogOn accounts. Administrator can also continue to manage logon data for cardholders if desired, by updating logon data in cardholder account. For entries created by Administrator, Administrator can specify if end-user will be allowed to view or change the logon data.</p> <p>See also Managed Entry Features.</p>		Yes
Initiate recording of logon data	<p>End-users who don't want to use the auto-record feature can switch off this default setting, and click on the Power LogOn "Record" button to initiate the recording of logon data.</p>	Yes	Yes



Access Smart, LLC
 27762 Antonio Pkwy L1-461
 Ladera Ranch, CA 92694

Phone: 949-218-8754 • Fax: 949-218-8678 • E-mail: support@access-smart.com

All logos and trademarks are the property of the originating company or individual.



Powered by Smartcard Technology™

Power LogOn™ Features List

Features	Description	Power LogOn Password Manager	Power LogOn Password Admin.
Auto-record and auto-fill of logon data	Whenever cardholder enters logon information into a website or application that Power LogOn recognizes as being recordable, Power LogOn asks the cardholder if he/she wants to record the logon data. Then, whenever cardholder goes to a website or application logon location which Power LogOn has stored, it automatically enters logon data and cardholder is logged on.	Yes	Yes
Manual entry and button-click fill of logon data	For website or application logon locations that don't have a unique address, it's simple for cardholders to manually enter logon data into Power LogOn, and then click on the "Logon Now" button to transfer logon data to location.	Yes	Yes
Pop-up	Whenever cardholder goes to a website or application logon location that Power LogOn has stored but which is not designated as auto-fill, Power LogOn automatically pops-up with the logon data so that cardholder can complete logon.	Yes	Yes
Browse to logon location from Power LogOn	End-user can double-click on a website or application entry in Power LogOn to browse to that location or start application, and auto fill or transfer logon data.	Yes	Yes
Submit control	Cardholder can choose to submit logon data to logon processes automatically, or can choose to manually control the submission of logon data. With the latter option, cardholder must click on the website or application "Submit" or "Enter" button, to submit logon data. Manually controlled submission of logon data is the default for auto-filled entries. See also Managed Entry Features.	Yes	Yes
Password change reminder	Power LogOn can prompt cardholder to change website or application password every specified number of days. Setting can be established by end-user in Power LogOn Password Management software or Administrator in CardMaker software, as required. Administrator can specify if end-user will be allowed to change this setting.	Yes	Yes



Access Smart, LLC
27762 Antonio Pkwy L1-461
Ladera Ranch, CA 92694

Phone: 949-218-8754 • Fax: 949-218-8678 • E-mail: support@access-smart.com

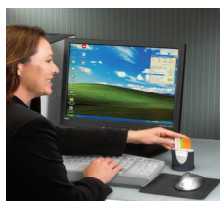
All logos and trademarks are the property of the originating company or individual.



Powered by Smartcard Technology™

Power LogOn™ Features List

Features	Description	Power LogOn Password Manager	Power LogOn Password Admin.
"Drag and drop" transferal of logon data	Logon data fields can be "dragged and dropped" into logon entry fields as desired.	Yes	Yes
Password policy control	Administrator can specify required password length and character type (numeric, upper case, lower case...) for websites/applications in CardMaker software, and end user must conform to these requirements when entering or changing passwords.		Yes
Generate random password	When end-user changes website or application password, he/she can generate a random password which conforms to the installation's Password Policy, if applicable. If installation has no Password Policy, end-user can specify password length and character type (numeric, upper case, lower case...) for random password.	Yes	Yes
Password change verification	Power LogOn can prompt cardholder to verify that password has been changed in website or application. This ensures that passwords remain synchronized (since it would not be possible for Power LogOn to automatically change a password in a third party website/application logon location that is not linked to Power LogOn via an API). Until cardholder verifies that password has been changed in website/application, Power LogOn will not accept password change. Setting can be established by end-user in Password Manager software or Administrator in CardMaker software, as required. Administrator can specify if end-user will be allowed to change this setting.	Yes	Yes
Password repetition control	Power LogOn can prohibit the entry of up to four previously used passwords, when cardholder changes a website or application password. Administrator can establish setting in CardMaker software.		Yes



Access Smart, LLC
 27762 Antonio Pkwy L1-461
 Ladera Ranch, CA 92694

Phone: 949-218-8754 • Fax: 949-218-8678 • E-mail: support@access-smart.com

All logos and trademarks are the property of the originating company or individual.

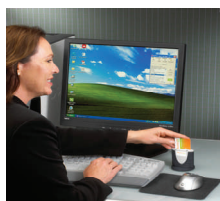


Powered by Smartcard Technology™

Power LogOn™ Features List

Other End-user Features

Features	Description	Power LogOn Password Manager	Power LogOn Password Admin.
Storage of address and payment information	End-user stores address and payment information in Power LogOn, for use in website and application entry fields. The labels of all address and payment entry fields can be customized by the end-user.	Yes	Yes
"Drag and drop" transfer of address and payment information	Cardholder can "drag" address and payment information and "drop" it into website and application entry fields, so that this basic information does not have to be continually re-typed.	Yes	Yes
Backup and restore data	<p>Cardholder can back up all of his/her Power LogOn smartcard data to his/her computer's hard drive, the network, or a removable data carrier such as a memory stick or floppy disk. Power LogOn prompts cardholder to enter a backup password. Then, if he/she loses his/her contact smartcard or forgets the authentication data for his smartcard, he/she can restore his/her Power LogOn data to a new card as long as he/she knows his/her backup password.</p> <p>Setting of backup location can be established by end-user in Password Management software or Administrator in CardMaker software, as required. Administrator can specify if end-user will be allowed to change this setting.</p>	Yes	Yes
Auto-backup reminder	<p>Power LogOn can prompt cardholder to backup his/her smartcard data every specified number of days at a certain time of day, or after data has been saved to Power LogOn a specified number of times.</p> <p>Setting can be established by end-user in Password Manager software or Administrator in CardMaker software, as required. Administrator can specify if end-user will be allowed to change this setting.</p>	Yes	Yes



Access Smart, LLC
27762 Antonio Pkwy L1-461
Ladera Ranch, CA 92694

Phone: 949-218-8754 • Fax: 949-218-8678 • E-mail: support@access-smart.com

All logos and trademarks are the property of the originating company or individual.



Powered by Smartcard Technology™

Power LogOn™ Features List

Features	Description	Power LogOn Password Manager	Power LogOn Password Admin.
<p>Save Power LogOn data to laptop</p>	<p>For card installations that use the CardMaker server to store Power LogOn entries, cardholders have the option to save their smartcard data to Laptop Mode, so that they can use Power LogOn to access this data without a card, card reader or network connection while they travel with their laptop.</p> <p>Administrator also has the option to disable Laptop Mode, or require that a card and card reader is also required in Laptop Mode, and can specify this setting in the CardMaker software.</p>	<p style="background-color: #cccccc;"></p>	<p style="text-align: center;">Yes</p>
<p>Access Power Logon data on CardMaker server remotely</p>	<p>For card installations that use the CardMaker server to store Power LogOn data, this feature enables user to access Power LogOn data on server without a card or card reader, when traveling.</p> <p>For security reasons, this option is typically only made available upon user request - for example, if user forgot to load Power LogOn data to laptop before leaving headquarters.</p> <p>Administrator can activate this capability on an individual basis for a defined period of time in the CardMaker software.</p>	<p style="background-color: #cccccc;"></p>	<p style="text-align: center;">Yes</p>
<p>No training required</p>	<p>End-user interface is intuitive and easy to use. Software prompts guide end-user through program.</p>	<p style="text-align: center;">Yes</p>	<p style="text-align: center;">Yes</p>
<p>Auto-start and minimize</p>	<p>Power LogOn Password Management software automatically starts at system startup, so that it is available for logons throughout the session. After auto-start, Power LogOn automatically minimizes to the system tray. Thereafter, Power LogOn auto-fills logon data or end-user double-clicks on Power LogOn icon to access software, as required. These default setting can also be switched off according to user preference.</p>	<p style="text-align: center;">Yes</p>	<p style="text-align: center;">Yes</p>



Access Smart, LLC
 27762 Antonio Pkwy L1-461
 Ladera Ranch, CA 92694

Phone: 949-218-8754 • Fax: 949-218-8678 • E-mail: support@access-smart.com

All logos and trademarks are the property of the originating company or individual.



Powered by Smartcard Technology™

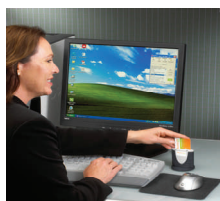
Power LogOn™ Features List

Auto-enrollment Features

Features	Description	Power LogOn Password Manager	Power LogOn Password Admin.
No configuration required	Software is pre-configured with standard default settings and ready for end-user self-enrollment immediately after installation.	Yes	Yes
End-user self-enrollment	Upon first use, cardholder presents card to card reader and is prompted to enter name and employee ID# to register with Power LogOn. Cardholders with Power LogOn Password Manager will also be prompted to enter their Power LogOn license key. Power LogOn software is then ready for immediate use.	Yes	Yes
End-user self re-enrollment	If end-user loses his/her card and is given a new card, he/she can self re-enroll with Power LogOn and access his/her previous Power LogOn data if he knows his/her personal security code. Note: Password Manager users must have a backup of their previous Power LogOn data and know their backup code, if they want to use previous data with their new card.	Yes	Yes

Set-Up Features

Features	Description	Power LogOn Password Management	Power LogOn Password Admin.
Easy installation of end-user software	Pre-configured Power LogOn Password Management software self-installs at end-user computers and is ready for immediate use, with no additional configuration required. Power LogOn setup is based on Microsoft Installer, which is compatible with numerous network installation tools.	Yes	Yes
Easy installation of administrator software	Pre-configured CardMaker software self-installs at administrator server computer. Administrator specifies only three server settings and software is ready for immediate use, with no additional configuration required.		Yes



Access Smart, LLC
 27762 Antonio Pkwy L1-461
 Ladera Ranch, CA 92694

Phone: 949-218-8754 • Fax: 949-218-8678 • E-mail: support@access-smart.com

All logos and trademarks are the property of the originating company or individual.



Powered by Smartcard Technology™

Power LogOn™ Features List

Features	Description	Power LogOn Password Manager	Power LogOn Password Admin.
No change to network or Windows setup	<p>Requires no change to existing network setup or user accounts on domain server. Requires no change to existing Windows setup.</p> <p>Logon to Windows performs according to standard Windows protocols for Standalone as well as networked computers (NT Domain Servers, Active Directory).</p>	Yes	Yes

Managed Enrollment Features

Features	Description	Power LogOn Password Management	Power LogOn Password Admin.
Customizable settings	Installation can use manufacturer's software default settings. Or, Administrator can change software settings in CardMaker software before issuing cards, to reflect corporate security policies and control how the end-user uses Power LogOn.		Yes
Database importing	Employee data can be imported from HR database into CardMaker software before card issuance, if required. Built-in data import functions support ODBC and LDAP compatible databases. CardMaker can also be linked with facility access control card management system if desired.		Yes
User groups	Administrator can specify different default card settings and managed entries for different user groups, for example, "Sales Department" or "Management".		Yes
One step issuance	Administrator clicks "Issue Card" in CardMaker software and chooses end-user from database, or enters end user data, to issue card.		Yes
Lost or stolen card "hotlist"	When a card is lost or stolen, it can be reported to the CardMaker software so that it will no longer be accepted within the Power LogOn system.		Yes



Access Smart, LLC
 27762 Antonio Pkwy L1-461
 Ladera Ranch, CA 92694

Phone: 949-218-8754 • Fax: 949-218-8678 • E-mail: support@access-smart.com

All logos and trademarks are the property of the originating company or individual.



Powered by Smartcard Technology™

Power LogOn™ Features List

Features	Description	Power LogOn Password Manager	Power LogOn Password Admin.
One step card re-issuance	After a card has been hot listed, a new card can be re-issued to the cardholder by selecting the cardholder's name from the cardholder list.		Yes
Recycle card	All Power LogOn smartcard data can be erased using the CardMaker software, so that the card can be re-used and issued to another user.		Yes
Reports	Complete cardholder reports and transaction logs are available in the CardMaker software.		Yes

Managed Entries Features

Features	Description	Power LogOn Password Management	Power LogOn Password Admin.
Easy creation of managed entries	Administrator simply creates a logon entry using the Power LogOn Password Management software and saves it. When the administrator "auto-records" the logon entry, Power LogOn "learns" the logon location of the entry, and the formats for user name, password and other entry fields.		Yes
Easy assignment of managed entries to user groups or individuals	Administrator assigns managed entries to user groups or individuals, and edits user name and password information as required for the group or individual.		Yes
Simple managed entry screen	Managed entries are easy to edit using the Managed Entries screen in the CardMaker software, where Administrator has an overview of all managed entries and can easily select, edit, and assign managed entries.		Yes
End-user edit control	Administrator can specify if user group or individual end-user will be allowed to view, edit all, edit password, or delete the managed entry.		Yes



Access Smart, LLC
27762 Antonio Pkwy L1-461
Ladera Ranch, CA 92694

Phone: 949-218-8754 • Fax: 949-218-8678 • E-mail: support@access-smart.com

All logos and trademarks are the property of the originating company or individual.



Powered by Smartcard Technology™

Power LogOn™ Features List

Features	Description	Power LogOn Password Manager	Power LogOn Password Admin.
Storage control	Administrator can specify if the managed entry will be stored on the end-user card and on the server, or stored only on the Power LogOn server.		Yes
No additional programming required	Many other logon management systems require that the administrator program links to the applications for which logon entries will be managed. No programming is required with Power LogOn. The managed entries functionality works as easily as all of the other Power LogOn features.		Yes
API for identity management systems	All managed entries are available via an API for 3rd party identity management and provisioning systems. Interfaces are based on ODBC, LDAP and XMP-RPC standards.		Yes

Other Administrator Features

Features	Description	Power LogOn Password Manager	Power LogOn Password Admin.
Administrator program protection	Administrators logon to CardMaker using Administrator password, or based on the administrator rights granted to their card.		Yes
Administrator assignment	Primary Administrator grants or revokes CardMaker rights for other Administrators.		Yes
Activity log	When Administrators logon to CardMaker with their card, the activity log automatically records which administrator performed each activity.		Yes



Access Smart, LLC
27762 Antonio Pkwy L1-461
Ladera Ranch, CA 92694

Phone: 949-218-8754 • Fax: 949-218-8678 • E-mail: support@access-smart.com

All logos and trademarks are the property of the originating company or individual.

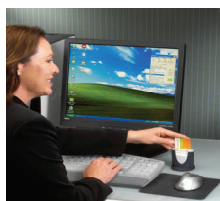


Powered by Smartcard Technology™

Power LogOn™ Features List

Security Features

Features	Description	Power LogOn Password Manager	Power LogOn Password Admin.
User designated PIN	Upon first use, cardholder is prompted to choose a unique Personal Identification Number (PIN). This PIN, along with presentation of the card, will be required for all access to the Power LogOn Password Manager software.	Yes	Yes
User designated PUK	Upon first use, cardholder is prompted to choose a unique Personal Unlock Key (PUK). The PUK is a second card PIN, which the cardholder can use to unlock their card. A card will be locked and no longer accepted within the Power LogOn system if the cardholder enters the wrong PIN multiple times. Once a card has been locked, Power LogOn will prompt the cardholder to enter the PUK to unlock the card.	Yes	Yes
Require PIN/PUK change upon first use option	All Power LogOn installations prompt end-user to change the initial PIN and PUK upon first use. Installations that require an additional level of control can select the CardMaker option which will require that the end-user change the PIN/PUK upon first use. In this case, if the PIN/PUK is not changed, the program will not continue.		Yes
Randomly generated PIN option	<p>Most Power LogOn installations use a standard default initial PIN of "12345", which the end-user is prompted to change upon first use. This is typically appropriate when the card that was issued does not yet contain any personalized data.</p> <p>Installations which want to specify a different initial PIN for each card that is issued - for example, installations that preload information to the card or card account - have the option to generate a random PIN for each card. A PIN letter can be generated in the CardMaker software that can then be delivered to the end-user. Cardholders with randomly generated PINs will also be prompted to change their PIN upon first use.</p> <p>In both of the above cases, the initial PIN and the PUK will be the same, but the cardholder will be prompted to change each individually.</p>		Yes



Access Smart, LLC
 27762 Antonio Pkwy L1-461
 Ladera Ranch, CA 92694

Phone: 949-218-8754 • Fax: 949-218-8678 • E-mail: support@access-smart.com

All logos and trademarks are the property of the originating company or individual.



Powered by Smartcard Technology™

Power LogOn™ Features List

Features	Description	Power LogOn Password Manager	Power LogOn Password Admin.
PIN policy control	Administrator can specify required PIN length and character type (numeric, upper case, lower case...) in CardMaker software, and end-user must conform to these requirements. PIN Policy established also applies to PUK.		Yes
PIN verification timeout	Specifies the length of time that a PIN will be stored in memory. After this time, end-user will be prompted to re-enter PIN. Setting can be established by end-user in Power LogOn Password Management software or Administrator in CardMaker software, as required. Administrator can specify if end-user will be allowed to change this setting.	Yes	Yes
Biometric authentication	A biometric device such as a fingerprint or iris reader can be used for end-user authentication, either in combination with a card and/or PIN or by itself. Full biometric capabilities are completely integrated into the Power LogOn software and work out-of-the-box with selected BIOAPI compatible devices, including biometric enrollment and authentication.		Yes
Encryption	Each issued Power LogOn smartcard or Power LogOn account is secured by its own unique set of TDES encryption keys. If an installation requires a specific encryption method, the modular Power LogOn encryption engine can be exchanged for special customized versions.	Yes	Yes
Secured data exchange with card	For card installations that store Power LogOn data on the card, all security sensitive Power LogOn data is first encrypted before being exchanged with the card.	Yes	Yes
Card security features	Power LogOn takes advantage of the card security features already offered by the powerful compatible card technologies to provide an additional layer of security.	Yes	Yes



Access Smart, LLC
 27762 Antonio Pkwy L1-461
 Ladera Ranch, CA 92694

Phone: 949-218-8754 • Fax: 949-218-8678 • E-mail: support@access-smart.com

All logos and trademarks are the property of the originating company or individual.



Powered by Smartcard Technology™

Power LogOn™ Features List

Features	Description	Power LogOn Password Manager	Power LogOn Password Admin.
Secure web server	CardMaker software, installed on a Windows 2000 Server or Windows 2003 Server machine, utilizes the Windows information server functionality and Secure Socket Layer (SSL) encryption to provide secure server functionality.		Yes
Connection to secure server protected by SSL	All security sensitive Power LogOn data is first encrypted before being exchanged via SSL protected connection with the secure server.		Yes

Other Administrator Features

Features	Description	Power LogOn Password Manager	Power LogOn Password Admin.
Wide compatibility	The Power LogOn software can be used out-of-the-box with a broad diversity of RFID and contact chip cards, cards readers, and PKI applications. See www.access-smart.com for Products list and out-of-the-box Solution Packages.	Yes	Yes
Power LogOn API for OEMs features	OEMs who want to bundle Power LogOn with other client applications have the option to use the built-in API to integrate further.	Yes	Yes
Multi-language	Power LogOn multi-language tool enables convenient translation and maintenance of the Power LogOn program text files, including Asian languages with double-byte characters. Also enables easy branding of software for OEMs.	Yes	Yes



Access Smart, LLC
 27762 Antonio Pkwy L1-461
 Ladera Ranch, CA 92694

Phone: 949-218-8754 • Fax: 949-218-8678 • E-mail: support@access-smart.com

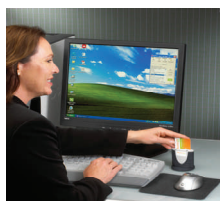
All logos and trademarks are the property of the originating company or individual.



Powered by Smartcard Technology™

Power LogOn™ Features List

Features	Description	Power LogOn Password Manager	Power LogOn Password Admin.
<p>Built for interoperability</p>	<p>The Power LogOn software is built around open API standards to provide interoperability between platforms, card readers, cards, and third-party software solutions. Power LogOn is either out-of-the-box compatible or can easily be integrated with many third-party software and hardware products. By leveraging interoperability standards, Power LogOn reduces the total cost of ownership for the end customer.</p> <p>PC/SC: can be used with all PC/SC conforming smart card readers.</p> <p>ISO 7816: has built-in interfaces for a number of ISO 7816 compatible cards. ISO 7816 compatible cards that are currently not supported can easily be integrated with Power LogOn.</p> <p>ISO 14443 A/B: supports ISO 14443 compatible RF cards through a number of contactless readers.</p> <p>ODBC: compatible with major database systems such as MS Access, MS SQL, Oracle, MySQL.</p> <p>LDAP: interfaces with LDAP-based directories such as Active Directory.</p> <p>COM: includes COM API for server and client-based software.</p> <p>XML: includes API based on XML-RPC function calls over IP.</p>	<p>Yes</p>	<p>Yes</p>
<p>CardMaker API for third party applications on server computer</p>	<p>Data elements of the CardMaker database are accessible through standard ODBC API.</p> <p>CardMaker features a flexible, built-in import function for LDAP and ODBC based data sources. This means that, for example, cardholder identification data can be imported from an HR or access control database without requiring any programming.</p> <p>All managed entries are available via an API for third party identity management and provisioning systems. Interfaces are based on ODBC, LDAP and XMP-RPC standards.</p>	<p></p>	<p>Yes</p>



Access Smart, LLC
 27762 Antonio Pkwy L1-461
 Ladera Ranch, CA 92694

Phone: 949-218-8754 • Fax: 949-218-8678 • E-mail: support@access-smart.com

All logos and trademarks are the property of the originating company or individual.



Powered by Smartcard Technology™