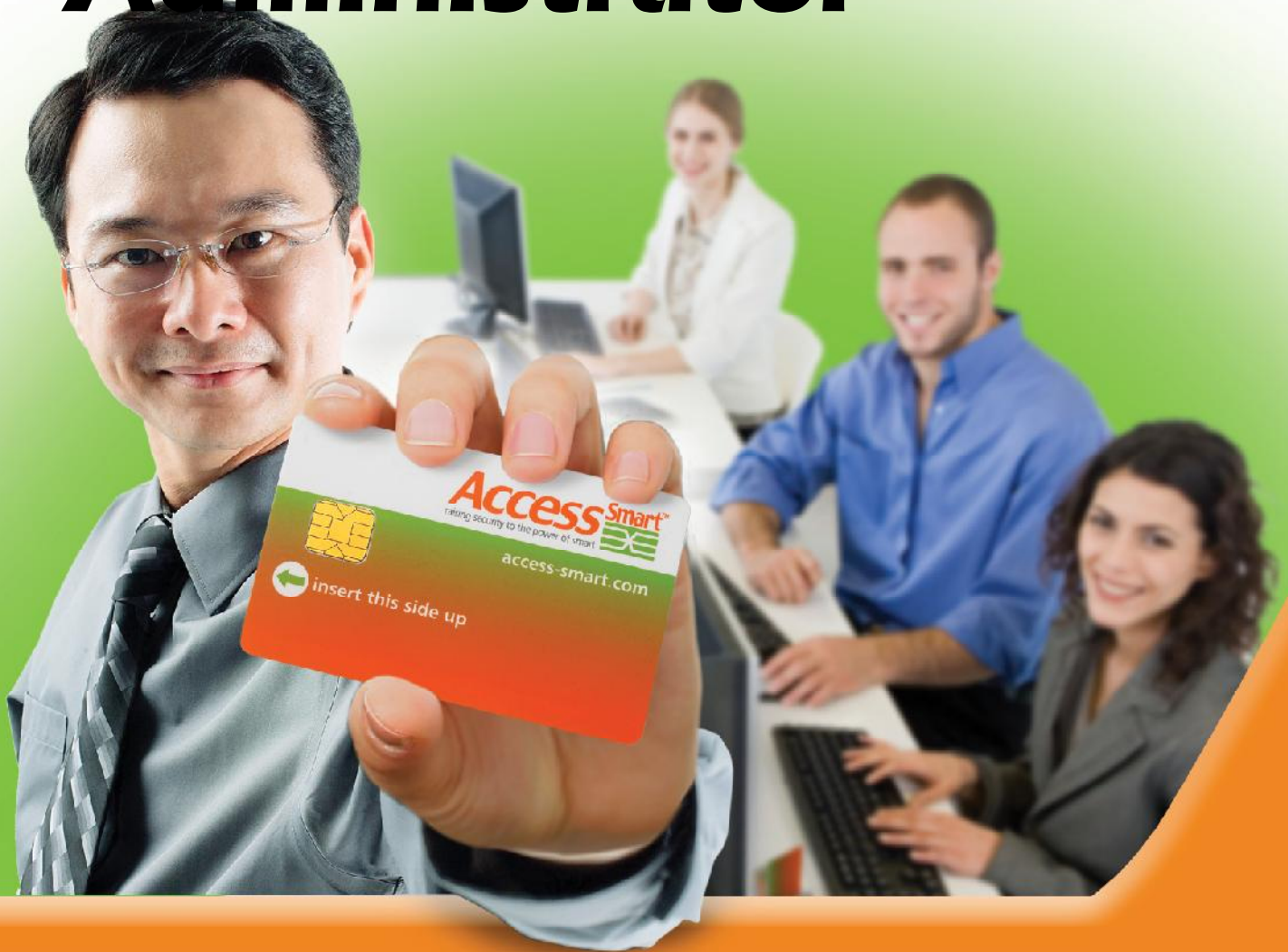


Power LogOn Administrator



Access Smart[®]
raising security to the power of smart



www.access-smart.com



Powered by
Smartcard
Technology[®]

Contents

Contents	1
Defining Strong Passwords	1
Recommendations	2
Disclaimers	2
Administrator Pre-Installation Checklist	6
Installing Software	8
Administrator Post-Installation Checklist	11
Installing Smartcard Readers	18
Customizing Card Configuration	23
Issuing Cards Using Evaluation Licenses	24
Issuing Cards Using Full Licenses	25
Additional Helpful Hints	26
Power LogOn Manager Post Installation Checklist	27
For More Information	28
Copyright and Trademark Information	28

Defining Strong Passwords

The protection of an Internet site or confidential document depends upon its passwords. Strong passwords are created using 1) Length – the total number of characters that make up a password; 2) Character Types - upper and lower case letters, numbers and symbols; and 3) Randomness – the sequence of characters

Examples:

Weak password: john2006
Strong password: D%4@*bHx\$jw#g

Power LogOn includes a random character password generator to assist you in creating strong, complex passwords. Click the “Create” tool button to launch the password generator application. Determine the parameters required for the password and then click the “Generate” button.

Recommendations

Access Smart® recommends that you keep a written backup copy of your computer/network logon User Name, Password and Domain, and the Power LogOn® back-up data file and password in a secure location like a safe or locked file cabinet. This information will assist you in regaining access to your computer in case of an emergency or if your card is ever lost, stolen or damaged. Power LogOn allows authorized users access to the Print Backup feature.

WHEN USING POWER LOGON, YOU HAVE SOLE RESPONSIBILITY FOR YOUR PIN AND PUK AND YOU MUST BE VERY CAREFUL NOT TO LOSE OR DISCLOSE YOUR PIN OR PUK. BECAUSE OF THE SENSITIVE NATURE OF THE INFORMATION WHICH IS STORED ON YOUR CARD, IT WOULD BE A BREACH OF SECURITY FOR ACCESS SMART TO RESET YOUR CARD PIN SO THAT YOU COULD CHOOSE A NEW PIN. IF YOU ENTER THE PIN WRONG 6 TIMES, IT WILL DISABLE THE CARD. HOWEVER, YOU CAN RESET THE CARD USING YOUR PUK. IF YOU ENTER YOUR PUK WRONG 6 TIMES, YOU WILL PERMANENTLY DESTROY THE CARD.

Frequently backup your card's data so you can easily recreate your card if it is ever lost, stolen or damaged. Contact Access Smart at **Support@access-smart.com** if you need a replacement card.

Disclaimers

SECURITY DISCLAIMER

Power LogOn conveniently manages the security of your passwords. The security of your files, documents and web sites are dependent upon how you manage your passwords, the strength of your passwords and who has access to your passwords. Therefore, Access Smart will not be responsible for any losses or damages that may result from the use of the Power LogOn product.

This Guide was written using a computer running Windows 10. If you are running a different operating system then you will need to check their documentation to find the corresponding commands and functions.

WARNING!

POWER LOGON IS NOT INTENDED FOR AND SHOULD NOT BE USED WITH ANY MACHINE OR DEVICE WHICH IS ESSENTIAL TO HUMAN LIFE OR HEALTH. ACCESS SMART WILL NOT BE RESPONSIBLE FOR ANY DEATH, INJURY, LOSS, OR DAMAGE RESULTING FROM THE USE OF THE POWER LOGON PRODUCT OR THE FAILURE OF THE POWER LOGON PRODUCT TO OPERATE. USE OF THIS PRODUCT WITH ANY SUCH MACHINE OR DEVICE IS SOLELY AT USER'S RISK AND THE USER ASSUMES THE RISK OF ANY DEATH, INJURY, LOSS, OR DAMAGE THAT MAY RESULT, DIRECTLY OR INDIRECTLY, FROM SUCH USE.

To protect against risk of fire, bodily injury, electric shock or damage to the equipment::

- Do not immerse any part of this product in water or other liquid.
- Do not spray liquid on this product or allow excess liquid to drip inside.
- Do not use this product with any equipment that has sustained damage, such as a damaged cord or plug.
- Disconnect this product before cleaning.

ABOUT YOUR RIGHTS AND OBLIGATIONS

The software with this product is licensed, not sold. You must either agree to the license contract in the Software Setup screen or promptly return the Power LogOn reader, software and cards for a refund, excluding the return costs. After you install the software, you may consult the License Agreement and the Limited Warranty for the product at any time by looking in the "Legal Information" section of the on-screen Help file installed with the software. You may also print a copy for your records.

The software license resides on the card and not in the Power LogOn Manager Application. Copies of the Power LogOn Manager can be loaded on a number of computers. Only licensed cards will work with the Power LogOn Manager Application.

REGULATORY INFORMATION

Tested to comply with FCC Standards for office or home use. Not intended for use in machinery, medical or industrial applications that are essential to human life or health. Any changes or modifications not expressly approved by Access Smart could void the user's authority to operate this device.

This product is for use with NRTL Listed (UL, CSA, ETL, etc.), and/or IEC/EN 60950 compliant (CE marked) Information Technology equipment. No serviceable parts are included.

This device is rated as a commercial product for operation at a temperature of +41°F (+5°C) to +95°F (+35°C).

This Class B digital apparatus complies with Part 15 of the U.S. Federal Communications Commission (FCC) rules, Canadian ICES-003 and RSS-210. Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

The term "IC:" before the certification/registration number only signifies that the Industry Canada technical specifications were met.

This product has been evaluated to comply with International Standard IEC 60825-1:1993/A2:2001.

This product uses LEDs that are inherently Class 1.

Product Disposal Information

Dispose of this product in accordance with Local and National Disposal Regulations.

Product Information and Software Updates

For general product information or to purchase additional products and software updates, go to the Access Smart Web site at: **www.access-smart.com** .

Power LogOn Administrator

The Power LogOn Administrator software is only installed on the computer / server used by the administrator who determines password policy parameters and issues the smartcards. Power LogOn Manager is the end user interface to ensure compliance with password policies and securely manage all computer, network, application and web access. This manual describes the functionality of Power LogOn Administrator and how to configure Power LogOn smartcards to meet a

company's network security policies with Power LogOn Manager. To learn more about Power LogOn Manager please reference the **Power LogOn Manager User's Manual** included on the CD-ROM in the Documentation > Manuals folder.

Power LogOn Manager

With Power LogOn Manager, the user will never need to type or remember a password again. Capable of storing up to 100 different accounts on a single smartcard, Manager is the most convenient, secure and portable way to guard all of their user names, passwords – and even credit card information for safe eCommerce transactions. With two clicks of a mouse, it can assign, store and enter complex passwords, immediately logging the user in to any computer network, Internet site or data file. It is simple to set up and intuitive to use. Since it is designed to work on both laptop and desktop computers, Power LogOn Manager is ideal for individuals, large corporations, and everything in between.

Administrator Pre-Installation Checklist

Before installing the Power LogOn Administrator software, complete all of the following steps that are applicable to your installation.

All Installations

Turn Off the Anti-Virus and Anti-Malware Programs

Because Power LogOn will make modifications to the Windows GINA and Registration Files most anti-virus programs and anti-malware programs will block files from being properly loaded. That is why we strongly suggest that you always temporarily turn off these programs before installation. As soon as installation is finished these programs can be re-activated.

Different anti-virus and anti-malware programs have different ways to temporarily turn them off. Check your anti-virus manual or contact the company

Confirm Internet Information Services (IIS) Installation

Before installing the Administrator software, you must confirm that Internet Information Services (IIS) is installed and that the features listed below are activated.

Confirm/install from Start > Control Panel > Programs and Features > Turn Windows Features On or Off.

For IIS 7, 7.5, 8, 8.5 (Windows 7 and Higher)

Internet Information Services

- Web Management Tools
 - IIS Management Console
- World Wide Web Services
 - Application Development Features
 - ASP
 - ISAPI Extensions
 - Common HTTP Features
 - Default Document
 - Directory Browsing
 - HTTP Errors
 - Static Content

- Health and Diagnostic
 - HTTP Logging
 - Request Monitor
- Security
 - Request Filtering
 - Windows Authentication

Windows 7, 8.x, or 10 Installation

De-activate User Account Control (UAC) setting

If you are installing Administrator or Manager on a Windows Vista machine, you must ensure that User Account Control (UAC) under Control Panel > User Accounts is unchecked in order to install or uninstall the software.

To Deactivate UAC (not required but suggested):

- Click **"Start"**
- Click **"Control Panel"**
- Click **"User Accounts"**
- Click **"Change User Account Control setting"**
- Slide lever to **"Never notify"**.
- Click **"OK"**
- Reboot computer for these changes to take effect

After installing Power LogOn Manager you can keep the UAC turned off. However if you want to re-activate the UAC, simply repeat the above process. Click **"OK"** and reboot.

Installing Software

Power LogOn Administrator requires both Administrator and Manager to be installed on the administrator's computer. Follow the instructions below based upon your computer's configuration.

UNINSTALLING AN EARLIER VERSION OF POWER LOGON ADMINISTRATOR

If this is your first time installing Administrator, you can skip this section.

If you don't use Terminal Services or IIS functions, skip steps 1 and 3.

If installation is on a Terminal Server (TS), logon in console mode, and make sure that there are no other TS sessions open.

1. Close down all Administrator, and/or Power LogOn Manager applications that are running. Also check icons in the system tray for any of these applications that may be running in the background.
2. Make a backup copy of all configuration and server-based card data
 - a. For Stand-Alone systems:
 - i) Backup data files located in 'c:\ProgramData\Administrator\Data\
 - (1) **'Cardlog.mdb'**
 - (2) **'Cardholder.mdb'**
 - (3) **'TxLog.mdb'**
 - ii) Backup configuration files
 - (1) **'c:\ProgramData\Administrator\CardMaker.ini'**
 - (2) **'c:\ProgramData\Administrator\rfip.ini'**
 - (3) **'c:\ProgramData\Administrator\CardSettings*.*'**
 - b. For Server based systems
 - i) Backup server-based card data
 - (1) **'c:\ProgramData\Administrator\data*.*'**
 - ii) If you are using Administrator with MS SQL database, you must also backup the SQL files located in the MS SQL data directory - i.e. "C:\Program Files\Microsoft SQL Server\MSSQL\Data\
 - (1) **'sphinx_cardholder.mdf'**
 - (2) **'sphinx_txlog.mdf'**
3. Restart IIS
4. From Desktop select **"Start - Control Panel - Programs and Features"**

5. Select "**Power LogOn Administrator**" and click on the "**Uninstall**" button. Follow on screen instructions to completely uninstall.
6. Delete the directory tree "**c:\program files\Power LogOn Administrator**"
7. Skip down to Installing Power LogOn Administrator.

UNINSTALLING AN EARLIER VERSION OF POWER LOGON MANAGER

If this is your first time installing Power LogOn Manager, you can skip this section.

Because Manager has some major changes, any older versions of Power LogOn Manager must first be removed from your computer. Manager saves all your passwords on the smartcard and not on your computer. So removing the Manager application does not affect any of your stored smartcard data.

1. Open Power LogOn Manager.
2. Select "**Settings**" from the menu and click "**Logon to Windows**"
3. You may need to click onto the "**Change**" button to remind yourself of your computer's User Name, Password and Domain Name since these will be required during the re-boot process.
4. Un-check the "**Use card to logon to Windows**" box.
5. Click on **OK** button.
6. Exit Power LogOn Manager.
7. Reboot computer.
8. Start the un-install process by clicking "**Start - Control Panel - Program and Features**" options.
9. Select **Power LogOn** and click "**Uninstall**".
10. Reboot your computer as needed.

INSTALLING POWER LOGON ADMINISTRATOR

It is strongly recommended that you temporarily turn off any antivirus and antimalware software before installing. Win7 users must turn off the UAC as defined in the "Windows 7, 8.x, or 10 Installation" section above.

Three different software applications will be installed: Power LogOn Administrator, Card reader drivers, and Power LogOn Manager.

1. Before installing the Power LogOn Administrator software, you must confirm that Internet Information Services (IIS) is installed. For more details go to the **Power LogOn Administrator User's Manual**; Section 2.1 Power LogOn Administrator Pre-Installation Checklist.
2. Insert the CD into your drive and the installation will start up automatically. If not, click on CD drive (usually D:) and double-click on "**InstallationOptions.exe**".



Figure 1: Power LogOn Installation Wizard

3. Select “**Power LogOn Administrator**” for installation. **NOTE: “Show All Options”** Is for advanced users that allows individual selection of applications to install.
4. Follow the screen instructions.
5. Click the “**Close**” button after Password Administrator has been loaded. Then click “**Exit**” on the “Power LogOn Installation Options” screen.
6. If all previous data as well as card and program settings are to be kept, replace the saved backup files identified in step 3 of “Uninstalling an earlier version of Password Administrator” into their corresponding new folder locations.

Note: Make sure that the Administrator version that you are updating to supports the same configuration file and database structure of your previous version. Consult any documentation that comes with the update and/or consult with your Power LogOn distributor or Access Smart, LLC.

8. Restart your computer.

Administrator Post-Installation Checklist

After installing the Administrator software, complete all of the following steps that are applicable to your installation.

All Installations

Verify reader driver installation

Installation of a Power LogOn-compatible contact or contactless card reader driver is required for Power LogOn Administrator operation.

For server installations: The card reader can either be physically connected to the server computer directly, or to a terminal which is used to connect to the server in console mode. After installation, it is not necessary to leave the card reader at the Administrator computer, unless needed.

Server Installations

Requesting Encrypted Server Address

Note: If you are evaluating Administrator using “localhost” server mode, with the Power LogOn Manager and Power LogOn Administrator software installed on one

computer, you can disregard this step.

Note the IP address where the Administrator software is installed by going to Start > Run. Type in "cmd" and click OK to see the command prompt. Type in "ipconfig" and hit Enter. IP address for server computer will be displayed. Make a note of the IP address, note whether your Administrator server is SSL secured.

Security note: Be assured that disclosing the IP address does not pose a threat to the system. Power LogOn Administrator sensitive end-user data is encrypted and can only be accessed externally through a challenge/response handshake which requires the end-user card and PIN.

Create Virtual Directory

Note 1: If you successfully created the virtual directory as prompted during CardMaker installation, you can disregard this step.

Note 2: If you are using SSL, this step is not required. Instead, follow SSL setup instructions in the Power LogOn Administrator User's Manual Appendix: SSL-Secured Client Setup .

Go to Control Panel > Administrative Tools > IIS (Internet Information Services). In IIS, right-click on default website, then go to "New" then "Virtual Directory". At the welcome screen, click "Next". When window pops up asking for an alias, enter "rfserver". Click "Next". At website content directory, click on "Browse" and select Program Files > Power LogOn Admin > Data. Click "OK" then "Next". At access permissions windows, enable the "Read" and "Run Scripts" permissions. Click "Next" then "Finish".

Check Firewalls

Ensure that access to ports 80 and 443 are not blocked by any Firewalls.

Ensure IIS Server Supports ASP Scripts

2003/2008 Server installations should especially be aware that the default settings only support ASP.NET scripts, but by default do not support classic ASP scripts. Since Power LogOn uses classic ASP scripts, support for ASP scripts must be enabled under Internet Information Services > Web Server Extensions

Modify access permissions (Optional)

As a part of installation, Power LogOn Administrator will automatically add the user “Everyone” to the “Security” tab of the Power LogOn Administrator Data sub-directory. This user “Everyone” is given full access permissions, so that the Internet Information Services (IIS) is able to access the Power LogOn Administrator database.

After installation you can further restrict access permissions by removing the user “Everyone” from the “Security” tab and replacing it with a user account that is specifically used for authentication of the virtual directory “rfserver”, as described below.

Open Windows Explorer. Right-click on folder “... **Users\All Users\Power LogOn\Administrator\Data** “. From the menu that appears, select “**Properties**” then select “**Security**” tab.

If your “Security” tab is not displayed:

Launch Windows Explorer or My Computer. Click on **Tools** at the menu bar, then click on **Folder Options**. Click on **View** tab. In the Advanced Settings section at the bottom of the list, uncheck the “**Use simple file sharing (Recommended)**” check box. Click **OK**.

If “Internet Guest Account” is NOT listed under “Group or user names”, click on **Edit/Add** button. In the “Select Users or Groups” window, click on the “**Locations...**” button. In the “Locations” window, select the computer that you are working on and click **OK**.

Back in the “Select Users or Groups” window, click on the “**Advanced...**” button. Then click “**Find Now**” button and select the “IUSR_(computer name)” account (the Internet Guest Account for the computer you’re working on) and click **OK** twice.

Back in the “Data Properties” window, verify that the “Internet Guest Account” is listed and highlighted, and that all permissions other than “**Full Control**” are checked. Then click on the **Apply** button, and then on the **OK** button.

Note: Some installations may need to additionally ensure that IUSR... refers to a local account and that it matches the user listed under Internet Information Services.

You can check this in XP/2000/2003/2008/2012 as follows:

Go to Internet Information Services (server name)>Web Sites>Default Web Site. Right click on rfserver>Properties>Directory Security>Edit under Anonymous access... Ensure that Anonymous access is enabled and that the user name matches.

You can check this in Windows 7 and higher:

Go to Internet Information Services (server name)>Web Sites/Sites
>Default Web Site>rfserver>Authentication. Right click on **Anonymous Authentication**>**Edit** and ensure that the user name matches.

SSL Setup (Optional)

Installations that will be using SSL to protect communication between Power LogOn Manager computers and the Power LogOn Administrator server should now refer to the Appendix, which provides assistance with SSL setup for website and client. After successful SSL setup, continue server setup below.

Additional Installation Tips

Remote or rack mounted servers

If your server computer is not physically accessible or is a rack mounted system, proceed as follows: Use a local workstation to connect to server via remote desktop in "Console" mode. Install card reader driver on both server and workstation, and plug reader into local workstation. Note that you may have to connect reader to server's USB port initially, to complete driver installation.

Distributed installation of client software

Ask your distributor for a Power LogOn silent installation kit. The Power LogOn Manager setup is based on Microsoft Windows Installer (MSI) and supports MSI Command-Line Options. These options can be especially useful when installing Power LogOn Manager from a central server onto distributed clients. The following link to Microsoft MSDN website contains information on MSI command line options and their usage:

<http://msdn2.microsoft.com/en-us/library/aa367988.aspx>

Terminal Services installations

If end-users will access Power LogOn Manager inside of Terminal Services sessions, then the Power LogOn Manager software must be installed on the Terminal Services (TS) server computer. This computer must be running Windows 2003 or 2008 in order to support all of the Terminal Services features and required smart card services redirection capabilities. When Power LogOn Manager is installed on the TS server, it can be configured to facilitate logon to the Windows session as well as logon to websites and applications. Services are provided based on the successful

authentication of the end-user's card, which must be presented to the card reader at the client computer/terminal. See also Appendix: Using Power LogOn with Terminal Services, for more information.

Note that any computer connecting to the server over RDP (Remote Desktop Protocol) will have its smart card services redirected from the client to the host. In this case, the type of card reader driver installed at the server computer must match the client computer card reader.

Failover server installations

For installations that require a failover server: If your installation requires a failover server, refer to Appendix: Using a Failover Server for additional information.

De-installation Note for IIS

Before you de-install Power LogOn Administrator from any computer, you must first exit Administrator and re-start IIS (Internet Information Services). This is to ensure that the web server is not currently linked to any of the Administrator components at the time of de-installation.

Encrypted Server IP Prompt

At first start of Power LogOn Administrator, a prompt will ask if you want to request an encrypted server IP.



Figure 2: Encrypted Server: IP Prompt

<p>If you are performing a test of Power LogOn functionality in localhost mode:</p> <p>(Where server software and client software are installed on the same computer.)</p>	<p>You do not need to request an encrypted server IP.</p> <ul style="list-style-type: none"> • When Power LogOn Manager and Administrator are installed on one computer, Power LogOn Manager is preset to communicate directly with Administrator server, so an encrypted IP address is already included. • You will notice that this setup functions somewhat slower than an actual networked setup, due to the fact that Internet Information Services (IIS) is slowed down when it runs on the same machine as the client.
<p>If you are running a standard networked server installation:</p> <p>(Where server computer and the client computers communicate over a network.)</p>	<p>You will need to request an encrypted IP address.</p> <ul style="list-style-type: none"> • The encrypted IP address secures the communication between the Power LogOn Manager client computers and the Administrator server. • Continue to the next screen to request an encrypted IP address.

Follow the instructions on the right side of the screen to get the IP address for your server computer and to send the request email. In response to your email, you will receive an encrypted IP address, with instructions on how to copy it in to your installation.

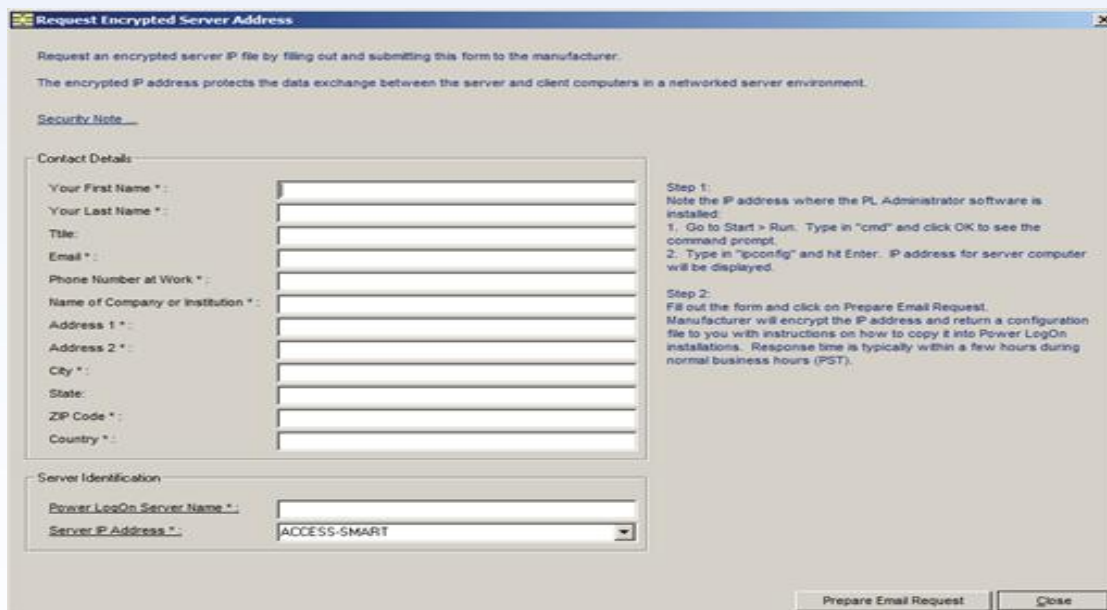


Figure 3: Encryption Server: Request Encrypted Server Address

Installation Instructions for RFIP.INI Files

- 1) After submitting your IP address or server name you will receive an RFIP.INI file. If the RFIP file is sent by email, in order to bypass anti-virus software from blocking the file, you will see the extension a file name formatted as "rfip_[Installation][IP].zip.rename" (i.e. rfip (XYZCorp Power LogOn Server)(62.54.222.103).zip.rename).
- 2) Rename the file 'rfip' by removing the ".rename" extension to make it a .zip extension. Extract file rfip.ini and copy it to the following locations (replacing the existing rfip.ini files):
 - "**C:\ProgramData\Power LogOn\Logon Manager**" (at all installations of Power LogOn on all client and server computers)
 - "**C:\ProgramData\Power LogOn\Administrator**" (on server computer(s) running Power LogOn Administrator)
- 3) Make sure that any new rfip.ini has been registered with Power LogOn Administrator program settings:
- 4) Exit and re-open Power LogOn Administrator, then open **Configuration > Local Settings > System**
- 5) Verify that the displayed settings under '**Power LogOn Server Identification**' match the settings of the currently used rfip.ini file.

Installing Smartcard Readers

1. Power LogOn Card and Reader Configuration.

In the Power LogOn Installation Kit there is the Components Reference Card that specifies the required setting based upon the equipment supplied. The below instructions are for example purposes, your setting may be different.

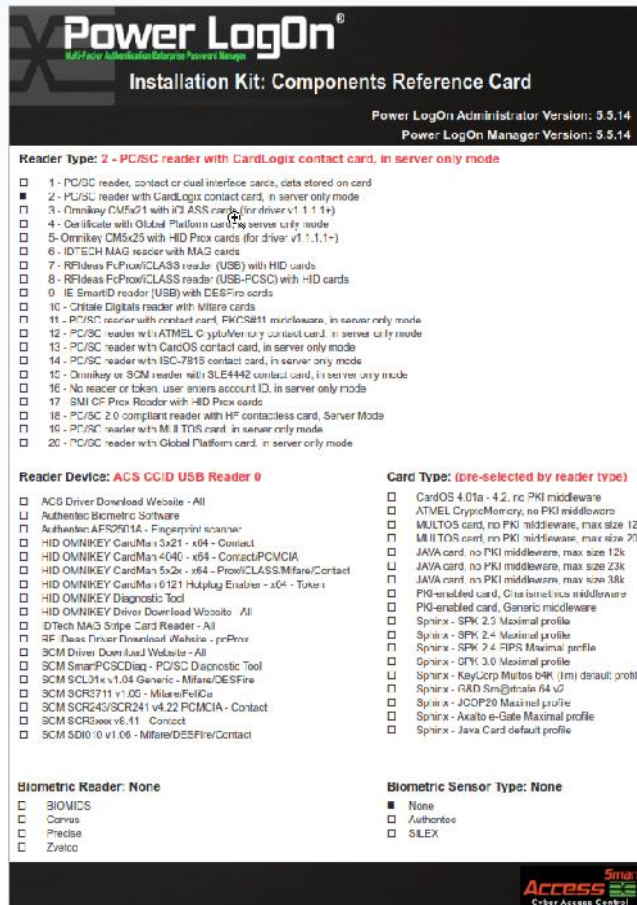


Figure 4: Installation Kit Reference Card

If you have any questions please contact your reseller or Access Smart at support@access-smart.com

a. Stand Alone Installation:

1) Select card reader type:

“1 – PC/SC reader with contact or dual interface smart cards”

2) Select card type:

“ATMEL CryptoMemory, no PKI middleware”

b. Server Installation:

1) Reader type:

“2 - PC/SC reader with CardLogix contact card, in server only mode”

2) Device:

“ACS Driver Download Website - All”

On the ACS website select:

- **Products**
- **PC-Linked Smart Card Readers**
- **ACR38U-H1**
- **Downloads** tab
- **“PC/SC Drivers”** for the Windows OS version you are using

NOTE: for contactless and other card users: select the corresponding reader and card options as required.

Click **OK**

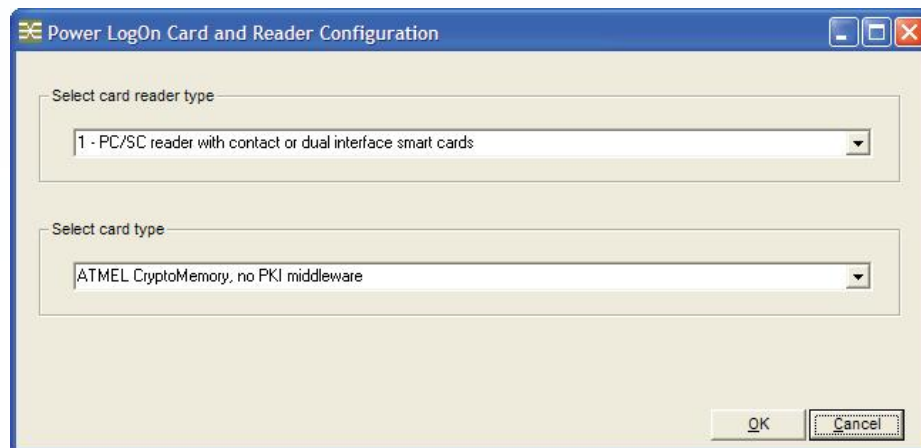


Figure 5: Card and Reader Configuration

2. Click **“File”** in the menu bar and choose **“Logon with User Name / Password”**



Figure 6: File: Logon with User Name / Password

3. Logon with the administrator password. The default password is “**admin**”.
Click **OK**. A screen will pop up reminding you that you are using the default password and a chance to change the password. It may be wise to click the Later button until you have configured Administrator to accept smartcards with a custom user name and password. (See the “**Power LogOn Administrator User Manual**” for details).
4. Set up the card readers to be used by the Administrator and for Production.
 - a. Click **Configuration > Card Reader Setup > Administrator**.
Follow the screen prompts.
 - b. Click **Configuration > Card Reader Setup > Production**.
Follow the screen prompts.



Figure 7: Configuration: Card Reader Setup

5. Import the evaluation licenses (keys)
 - a. Click **Configuration > Keys > Import**



Figure 8: Keys: Importing

- b. The Key data file is located
"C:\ProgramData\Power LogOn\Administrator\Data"
- c. Select **Keys_Evaluation_0001x to 0006x.mdb**



Figure 9: Evaluation keys data file

- 6. Click Open button from **"Select Key to Import from"** screen
- 7. Click **OK** button from **"Import Keys"** screen. Your information may be different.

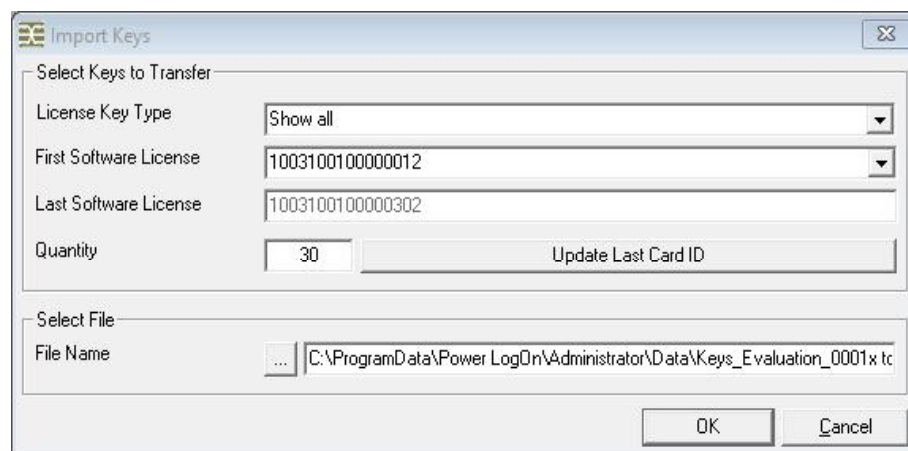


Figure 10: Import Keys

8. Click **OK** from the “Import Log” screen

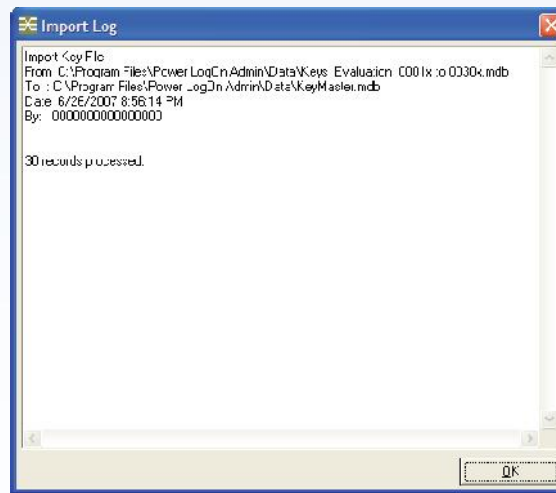


Figure 11: Import Log

Customizing Card Configuration

Before issuing cards, it's a good idea to check **Configuration > Card Settings**, to view the default card settings and make any changes required for your particular installation. Some administrators may also want to check the **Configuration > Program Settings**, but this is not as critical since the default settings specified suit most installations.

For assistance with card and program settings, refer to the "**Power LogOn Administrator User's Manual**" found on the CD-ROM in the Documentation folder or by clicking **Info > User Manual (pdf)** in the Power LogOn Administrator menu.



Figure 12: Power LogOn Administrator User's Manual cover.

If pre-configuration has not been performed by the manufacturer, the Power LogOn Administrator performs the following configuration steps before issuing cards:

- Imports the license key file into the Power LogOn Administrator program.
- Configures program settings, including installation-specific system and server settings.
- Configures card settings, by creating one or more card setting default files which will be used for card issuance.
- Selects card reader which will be used for card issuance, as required.
- Select the type of smartcards being used.

Because of the advanced features and capabilities of Power LogOn Administrator, you will need to read the "**Power LogOn Administrator User's Manual**" found on the CD-ROM or by clicking **Info > User Manual (pdf)** in the Password Administrator menu before setting up custom configurations.

Issuing Cards Using Evaluation Licenses

Refer to **Power LogOn Administrator User's Manual**, Section 3 for more detailed information. Power LogOn Administrator includes 6 blank smart cards and 6 evaluation keys. The purpose of these cards and licenses is to give the card administrator product to practice, test and determine how they want to configure their computer systems, server and cards before going to full deployment. Evaluation keys only have a life span of 90 days before they revert to demo mode.

To purchase full licenses contact your Power LogOn reseller or Access Smart at support@access-smart.com.

1. Click on "**Card**" in the menu bar, and click on the "**Issue Card**" selection.

NOTE: if cardholder names have been pre-entered, click on desired entry to highlight the entry, and click on the Select button. Refer to **Power LogOn Administrator User's Manual**, "**Tools**" Section 5.3 to import employee data from an HR database.

2. To enter a new cardholder, click on the **Add New** button.
3. Enter a new cardholder's information.

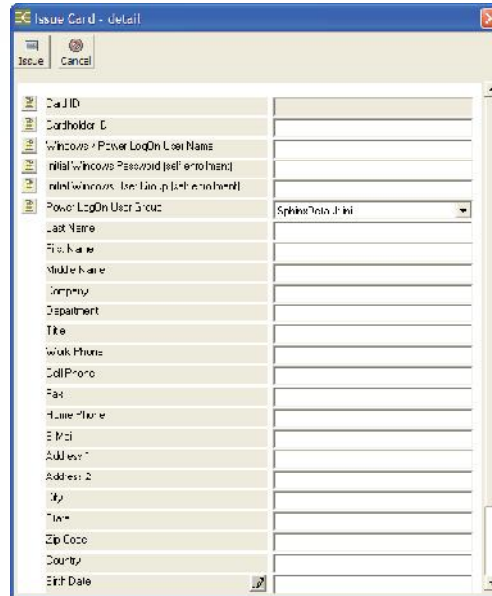



Figure 13: Issue Card - Detail.

Click on the  icon found along the left side for information about that specific field.

4. Click **Issue** button when finished entering data.

5. The Power LogOn Administrator will prompt you to insert a Power LogOn smartcard into the card reader. Card will be processed, and a window will alert you when you may remove the card and deliver it to cardholder.
6. The card is now ready to be issued and used with Power LogOn Manager.

NOTE: Evaluation keys provide full Power LogOn functionality for 90 days after installation. After expiration, installation will revert to demo mode, which stores only a few entries. To convert your evaluation version into a fully licensed version, contact your Power LogOn reseller or Access Smart at support@access-smart.com to purchase full licenses. To continue to use Power LogOn entry data that you save in this evaluation version: be sure to create a Power LogOn backup before your 90-day evaluation period expires. This backup can then be restored onto a fully licensed Power LogOn version.

Issuing Cards Using Full Licenses

1. Contact your Power LogOn reseller or Access Smart at support@access-smart.com to purchase the quantity of full licenses needed. The licenses will be sent you electronically in a .zip format.
2. Unzip the file and store the keys in:
“**C:\ProgramData\Power LogOn\Administrator\Data**”
3. Import the demonstration keys
 - a. Click **Configuration > Keys > Import**

NOTE: for full license keys: installations that are installing full license keys can follow instructions as described, but select instead the license key file received from distributor

- b. The Key data file is located:
“**C:\ProgramData\Power LogOn\Administrator\Data**”
 - c. Select the new key file.
4. Follow all the same procedures as describe in the above section “Issuing cards using evaluation licenses”.

Additional helpful tips

Remote or rack mounted servers

If your server computer is not physically accessible or is a rack mounted system, proceed as follows: Use a local workstation to connect to server via remote desktop in "Console" mode. Install card reader driver on both server and workstation, and plug reader into local workstation. Note that you may have to connect reader to server's USB port initially, to complete driver installation.

Distributed installation of client software

Ask your distributor for a Power LogOn silent installation kit. The Power LogOn Manager setup is based on Microsoft Windows Installer (MSI) and supports MSI Command-Line Options. These options can be especially useful when installing Manager from a central server onto distributed clients. The following link to Microsoft MSDN website contains information on MSI command line options and their usage:

<http://msdn2.microsoft.com/en-us/library/aa367988.aspx>

Terminal Services installations

If end-users will access Power LogOn Manager inside of Terminal Services sessions, then the Manager software must be installed on the Terminal Services (TS) server computer. This computer must be running Windows 2003 in order to support all of the Terminal Services features and required smart card services redirection capabilities. When Manager is installed on the TS server, it can be configured to facilitate logon to the Windows session as well as logon to websites and applications. Services are provided based on the successful authentication of the end-user's card, which must

be presented to the card reader at the client computer/terminal. See also Power LogOn Administrator's Manual Appendix: "Using Password Manager with Terminal Services", for more information.

Note that any computer connecting to the server over RDP (Remote Desktop Protocol) will have its smart card services redirected from the client to the host. In this case, the type of card reader driver installed at the server computer must match the client computer card reader.

De-installation Note for IIS

Before you de-install Administrator from any computer, you must first exit Administrator and re-start IIS (Internet Information Services). This is to ensure that the web server is not currently linked to any of the Administrator components at the time of de-installation.

Power LogOn Manager Post-Installation Checklist

After installing Power LogOn Manager at end-user computers, complete all of the following steps that are applicable to your installation.

Server Installations

- Enter Encrypted IP Address

Note: If you are evaluating Power LogOn using "localhost" server mode, with the Manager and Administrator software installed on one computer, you can disregard this step.

Enter encrypted IP address received from distributor into each end-user computer where Power LogOn Manager software has been installed (see also Encrypt IP Address instruction in previous section).

Windows 2003/2008 Server Installations

- Configure Security Settings

You must deactivate the "Internet Explorer Enhanced Security Configuration" preset if you want end-users to be able to Auto-record and Auto-fill web logon entries.

Windows Win 7, 8.x, 10 Installations

- Verify User Account Control setting

If you will be using a card to logon to Windows machines: in order for Power LogOn to be able to redirect the logon to the card, logon as administrator and uncheck the “**User Account Control**” setting, under **Control Panel > User Accounts**. Next, open Manager and set the Settings > Logon to Windows > Use card to logon... setting to active.

For More Information

Please read the **Power LogOn Administrator User’s Manual** available under the Info menu to learn more about these and other features and options.

Copyright and Trademark Information

Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Access Smart. Access Smart may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Access Smart, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

© 2005- 2017 Access Smart, LLC. All rights reserved.

Access Smart, Access Smart Logo, Power LogOn, Powered by Smartcard Technology and design are registered trademarks licensed to Access Smart, LLC in the United States and/or other countries.

Other parties’ trademarks or service marks are the products of their respective owners.

NOTES:



The new look of Power LogOn

NOTES:

Access Smart, LLC

27762 Antonio Parkway, L1-461

Ladera Ranch, CA 92694

Phone: (877) 795-6466

Web: www.access-smart.com

E-mail: info@access-smart.com