SCHLAGE

Campus Lock Keycard Center

Technical / User Manual

Ingersoll Rand
Security Technologies

Ingersoll Rand Copyright Notice

CONTACT INFORMATION

Schlage
Electronic Security
575 Birch Street
Forestville, CT 06010
Phone: 860-584-9158
Fax: 860-584-2136
www.schlage.com

To contact a local Ingersoll Rand Security Technologies Consultant in your area go to:
http://securitytechnologies.ingersollrand.com/ssc.asp

Contents

Ingersoll Rand Copyright Notice 2

Typographical Conventions 1

Preface 2

Introduction 2
Overview 2

Hardware Specifications 3

Physical Specifications 3
Electrical Requirements 3
Operating Temperature 3
Operating Humidity 3

Web Server Installation 4

Introduction 4
System Requirements 4
Installation 4
Database Configuration 6
Customized Logo 7

Kiosk Set Up 8

Introduction 8
Getting the IP Address of each kiosk 8
Kioware Set Up 9
Exiting Kioware 10
Touchscreen Set Up 10
Filling the Temporary Card Dispenser 12

Configuring the Database Communication to Kiosks 13

Introduction 13
Kiosk Database Configuration 13
Kiosk Definition 18

User's Guide 20

Introduction 20
Update ID 20
Change PIN 20
Get Temporary Card 21
Staff Revalidation 21

Desktop Kiosk 22

Introduction 22
System Requirements 22
Installation 22

Typographical Conventions

Before you start using this guide, it is important to understand the terms and typographical conventions used in the documentation.

The following kinds of formatting in the text identify special information.

Formatting convention	Type of Information
Numbered (1, 2, 3 ..)	Step-by-step procedures. Users can follow these instructions to complete a specific task.
Bold	Brand names, window names, application name when used for the first time in a chapter or section, items you must select, such as menu options, command buttons, or items in a list.
Notes and warnings	Information that requires special attention of the user.
CAPITALS	Names of keys on the keyboard. for example, SHIFT, CTRL, or ALT.
KEY+KEY	Key combinations for which the user must press and hold down one key and then press another, for example, CTRL+P, or ALT+F4.
Emphasis	Use to emphasize the importance of a point or for variable expressions such as parameters

Preface

Introduction

The Campus Lock Keycard Center, used in conjunction with Schlage CL Locks, is designed to simplify keycard and credential management on school campuses. This user-friendly kiosk enables students and staff to play a role in managing their own access credentials. It provides around-the-clock replacement of lost cards, but also allows the user to change their PIN, create a temporary card or automatically update access privileges. The kiosk also manages staff card revalidation at predefined time intervals.

Overview

This manual covers the following:

- Installation
- Database Configuration
- User Guide

Setting up your Campus Lock Keycard Center is a multi-step process, as described in this manual. First, you will be installing the web server and configuring the host database. Next, the manual describes the steps that need to be taken at each individual kiosk. Finally, you will be configuring your database to communicate with each kiosk. Please follow the manual carefully as some of the steps are kiosk-specific, while other steps are universal and apply to all kiosks.

Hardware Specifications

CHAPTER 1

Physical Specifications

- Height 69.0" / 1753 mm
- Width 24.0" / 610 mm
- Depth 19.8" / 503 mm
- Weight 260 lbs / 118.8 Kg

Electrical Requirements

- 100 - 127 VAC ~ 50/60 Hz, 5.0A
- 200 - 240 VAC ~ 50/60 Hz, 2.5A

Operating Temperature

- 32° F - 115° F Degrees
- 0° C - 45° C Degrees

Operating Humidity

- 20% - 95% Relative Humidity (non-condensing)

Web Server Installation

CHAPTER 2

Introduction

The kiosk interface is a website that is accessed from an installed IIS web server. First, the web server is installed on a central computer, usually the database server, and configured to interact with the dedicated Kiosks and any other computers running the Campus Lock Keycard Center interface. This step of the configuration is completed via an installation program as described below.

Note: IIS comes standard with the Windows installation disk. The disk must be installed for the kiosk Installation program to work. Install if necessary and continue to the instructions below.

System Requirements

Operating System:

- Windows XP with IIS 5.1 or
- Windows 2003 with IIS 6.0

Hardware:

- As recommended by MS to run Server 2003 (1 GB of RAM recommended)

Note: if SMS is installed on the same machine as the IIS Server, then hardware requirements should be revised to match IR recommendations for SMS plus an additional 1 GB of RAM for IIS operation. Please see the System Requirements for SMS for more details.

Installation

1. Run the Web Server Installation program. The WISE installer will start.
2. When the message "IIS Version x.x found" comes up, click **OK**. The Welcome window will open.
3. Click **Next**. The Destination Location window will open.
4. Choose the destination folder. The default is c:\inetpub\kiosk. This can be changed either by clicking the **Browse** button and choosing a different folder, or by manually typing in the file path and folder name into the field provided. When the correct folder has been specified click **Next**. The Ready to Install window will open.
5. Click **Next**.
6. The program will now install .Net 2.0 Framework.

a) If your computer already has .Net 2.0, the Maintenance Mode window will open. You will have the option to Repair, Uninstall or Cancel. If Repair is selected, uncheck Reboot Computer.

b) Click **Cancel**. A window will open asking "Are you sure you want to cancel set up".

c) Click **Yes**. A window saying "You have chosen to cancel setup" will open.

d) Click **Finish**.

7 The program will ask if you want to install Hotfix. Click **Ok**. A terms of agreement screen will open.

8 Click **I accept**. Hotfix will install. This may take a few moments.

9 When it is done installing, a window will open with the message "Hotfix successfully installed".

10 Click **Ok**. The installation will continue until finished. The Finished window will open.

11 Click **Finish**.

12 The program will now install MS ASP.NET 2.0 AJAX Extensions 1.0.

13 Click Next and accept the License Agreement.

14 Click Next and Install. Installation will begin.

15 Once ASP.NET 2.0 AJAX Extension Complete, please click the Finish button.

16 Click **Finish** to exit installation.

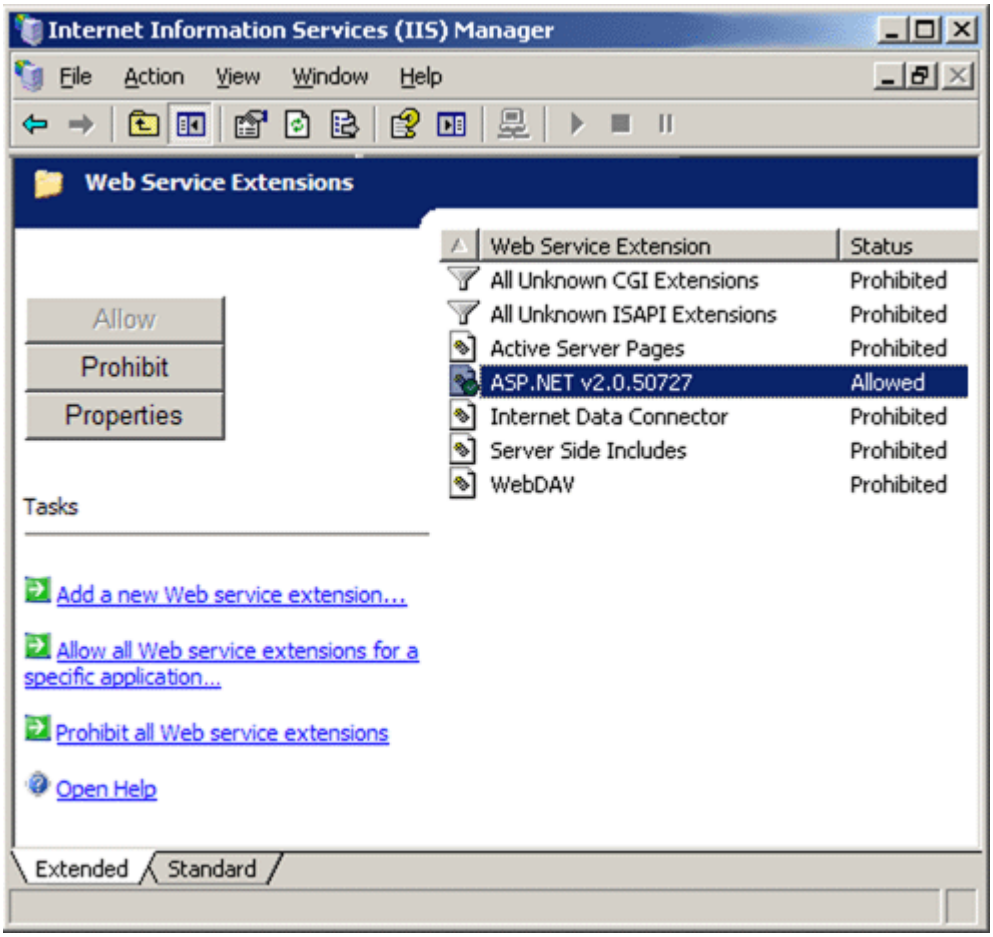
Note: The following steps are for servers running Windows Server 2003 ONLY.

17 From the Windows Start menu, click **Run**.

18 In the Run dialog box, enter **inetmgr**.

19 Click **OK**. The **IIS Manager** will open.

20 In IIS Manager, expand the local computer and then click **Web Service Extensions**.



21 In the details pane, right-click **ASP.NET** and select **Allow** from the list. The status of ASP.NET changes to Allowed.

22 Close the IIS Manager.

Database Configuration

Information regarding the Security Management System database that is used by the kiosk application is stored in the file **web.config** which is installed in a directory selected during kiosk Web Server installation. Default location suggested by installation program is: **c: \inetpub\kiosk**. If you changed this destination during installation then the file will be located in whichever directory you specified. This text file can be edited using any text editor such as Notepad or Wordpad. Follow the steps below to configure your database.

1 Right click web.config and choose **Open With...**

2 Click on **Notepad** (or **Wordpad**). The file will open.

3 Go to line 18. It will look like this:
connectionString= "Data Source= localhost; Initial Catalog= SchlageSQL; Persist Security Info= True; User ID= SMSAdmin; Password= SECAdmin1" providerName= "System.Data.SqlClient" />

The Default values are:

a) Data Source (Host Name of machine where SMS database is installed) = localhost

b) Initial Catalog (Database name) = SchlageSQL

c) User ID (SQL login) = SMSAdmin

d) Password (SQL password) = SECAdmin1 (default installation password)

4 If necessary, modify these values to reflect your database settings.

5 Go to **File>Save** to save the file.

6 Go to **File>Exit** to close the file.

Customized Logo

Optional: The kiosk user interface can be customized with your school's logo in the upper left corner of the screen. This will replace the default Schlage logo.

1 Create logo with the following requirements:

- Image Type: .gif
- Image Size: Recomended 220 x 45 pixels. Maximum: 300 x 50 pixels.

2 Save the image as **Logo.gif**.

3 Open the **images** folder in the kiosk directory. The default location is c:inetpub\kiosk\images. If the location of the files was changed during installation, the image folder will be located at \\images.

4 Re-name the current Logo.gif file. Example: OldLogo.gif

5 Copy the logo file you created into the images folder.

When you start the kiosk you will see your logo in the upper left corner.

Kiosk Set Up

CHAPTER 3

Introduction

The following steps need to be taken at each kiosk in order to ensure proper functionality as well as integration with the database. These steps will remove the sound and disable the cursor arrow, making navigation to the database more difficult. Because of this, it is recommended that you get the IP address of each kiosk before you follow the set up procedures.

Note: A keyboard will need to be connected to the kiosk in order to follow these steps. This can be done by opening the bottom cabinet of the kiosk.

Getting the IP Address of each kiosk

1. Click the Start button in the lower right corner.
2. Click on Run. The Run pop-up window will open.
3. Enter **cmd** into the field provided.
4. Click OK. The command line window will open.
5. Enter **ipconfig**.
6. Press Enter on the keyboard.
7. The IP Address is listed after **IP Address.....**.
8. Make a note of the IP Address. This will be needed later in the set up.
9. Repeat for every kiosk on campus.

This is the information you'll need later when using the Kiosk Configuration program.

Kioware Set Up

The Kioware software enables the kiosk to function in a secure manner. It provides an added level of security to the dedicated kiosks by denying users access to Windows, the web browser, or any other functionality outside of the kiosk interface. It needs to be configured correctly to interact with the IIS server that has been installed and to display the kiosk interface. These steps need to be carried out for each Campus Lock Keycard Center.

Accessing the Program

Open the Kioware Configuration program by double clicking the Kioware Configuration Icon on the desktop or go to Start>Programs>Kioware>Kioware Config Tool.

1 Setting Host URL

This tells Kioware where to look for the kiosk interface.

a) Select the **General** tab.

b) Enter the URL of the kiosk server in the provided window.

Example: http://host_computer_name/kiosk

2 Setting Start Options

Kioware allows the system to boot directly into the Campus Lock Keycard Center interface, bypassing the Windows start screen, whenever the kiosk is turned on. If the system restarts for any reason, students and users will continue to have access to the kiosk functions. Follow the instruction below to enable this feature (you'll need the Windows user name and password).

a) Select the **General** tab.

b) Click the **Start on Boot** box. This puts a check in this box.

c) Click the **Auto Logon at Boot** box. This puts a check in this box.

d) Enter Windows User Name.

e) Enter Windows Password.

f) Confirm Windows Password.

3 Change the Kioware Password

This is the password that allows you to exit the Kioware system and access Windows.

a) Select the **General** tab.

b) Enter Current Password. Default is: 3523

c) Enter New Password.

d) Confirm New Password.

Note: Keeping this password as the default will leave the system unsecured. It is very important to change this password.

Exiting Kioware

Once Kioware is set up it will no longer be possible to access Windows without a password. To exit Kioware the user must follow these steps.

1. Touch the kiosk in the upper left hand corner of the touchscreen.
2. Touch the kiosk in the upper right hand corner of the touchscreen.
3. Touch the kiosk in the lower right hand corner of the touchscreen.
4. Touch the kiosk in the lower left hand corner of the touchscreen.
5. The Password Keypad will open in the center of the screen.
6. Enter the password (default is 3523).

Kioware will shut down and the user will have access to Windows.

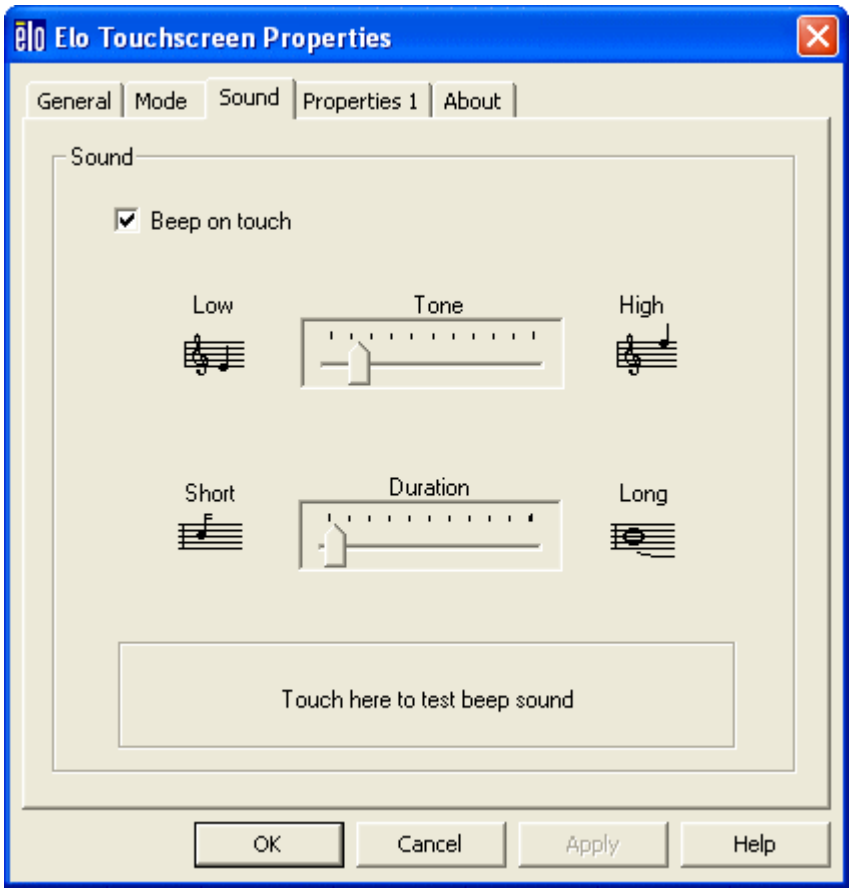
Touchscreen Set Up

The Elo Touchscreen runs the touchscreen interface of the kiosk. The sound and mouse pointer settings need to be disabled before the kiosk is ready.

1. Access the Elo touchscreen settings by finding the icon in the system tray to the lower right of the screen. Click on the Elo icon. The Elo Touchscreen Properties window will open.
2. **Disabling Sound**

   The kiosk interface has a dedicated sound function to ensure that a user only hears a beep when a button on the touchscreen is engaged. To avoid confusion, disable the non-dedicated sound functions of the touchscreen.

a) Open the **Sound** tab.

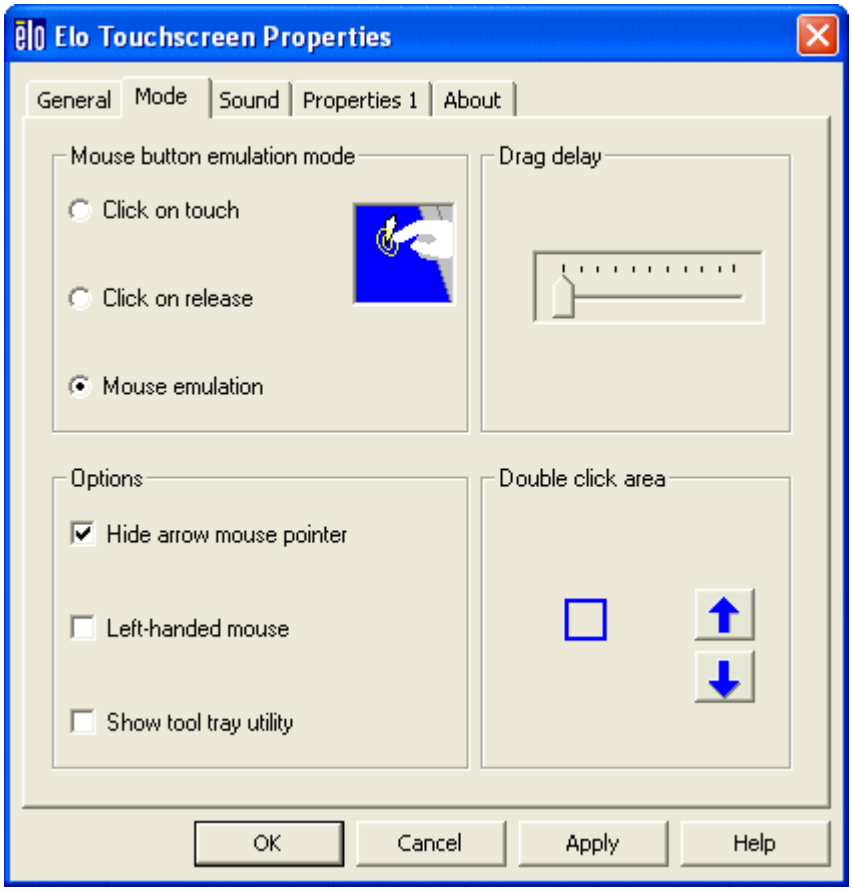


b) Click on the **Beep on Touch** box. This removes the check from this box, leaving it empty.

c) Non-dedicated sound is now disabled.

3 Disabling Pointer

a) Open the **Mode** tab.



b) Click on the **Hide Arrow Mouse Pointer** box in the Options section. This puts a check in this box.

c) Arrow Mouse Pointer is now disabled

Note: The Hide Arrow Mouse Pointer option will remove the cursor from the screen, making it much harder to navigate during set up. This should be completed as the final step in setting up the kiosk.

Filling the Temporary Card Dispenser

Follow the instructions below to fill the temporary card dispenser.

1. Unlock the screen housing with the keys provided with the kiosk. The locks are located on the sides of the kiosk in the upper left and the upper right sides of the screen housing.
2. Tilt the screen housing down towards you. Inside are the temporary card dispenser and the card encoder. The temporary card dispenser is on the left.
3. Orient the temporary cards so that the magnetic stripe is facing down and on the right side.
4. Insert a stack of cards into the dispenser through the top bracket.
5. Insert more cards until they reach the top of the dispenser.
6. Close and re-lock the screen housing.

Configuring the Database Communication to Kiosks

CHAPTER 4

Introduction

Once all kiosks on campus have been set-up, the user will need to configure them using the Kiosk Configuration program.

Kiosk Database Configuration

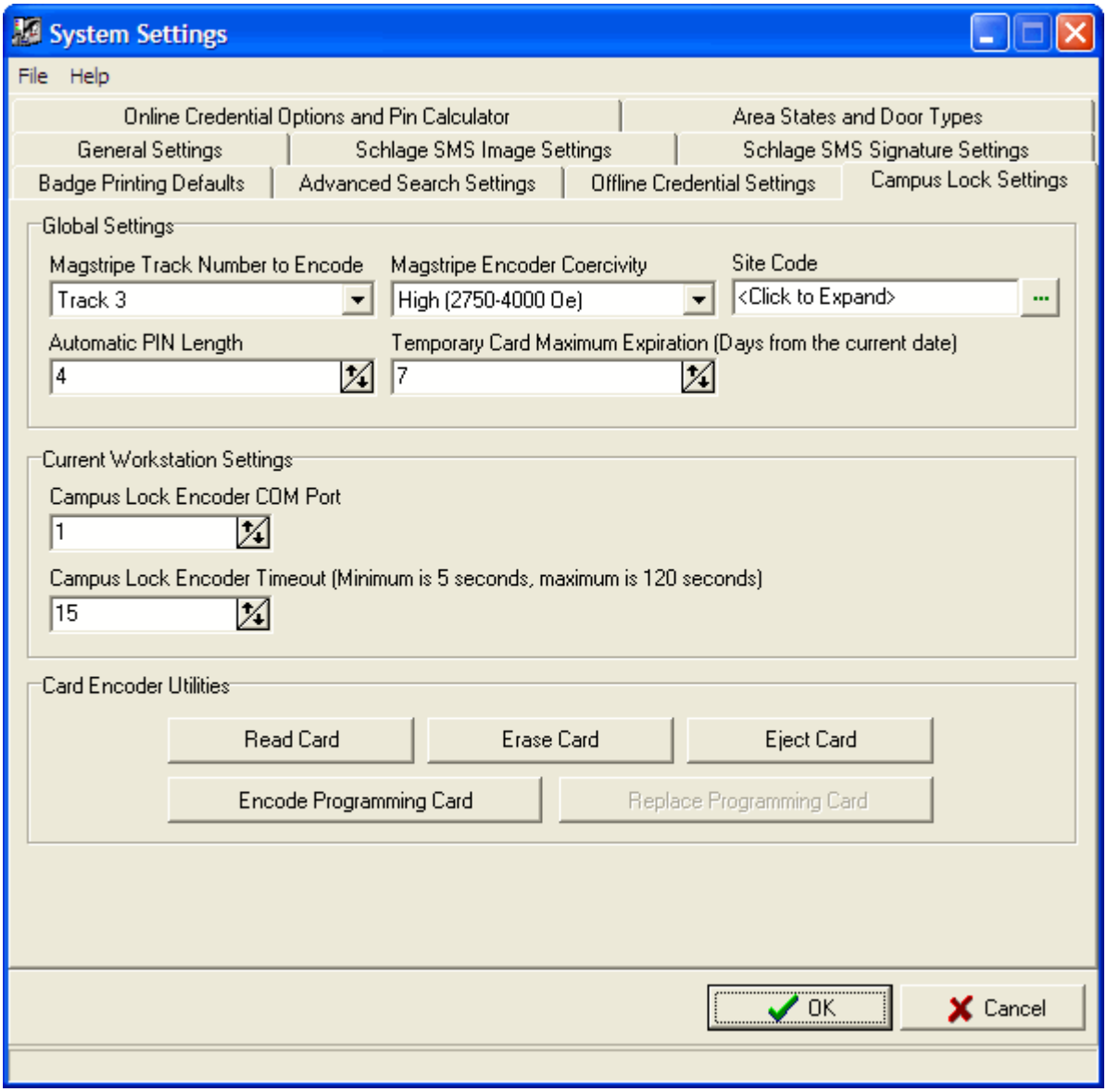
The CL Kiosk is designed around the concept that a college or university's "One Card" system is typically the master for credentials in the higher education market. These systems use track 2 on a magstripe card to identify the student. This track cannot be modified by the SMS systems. SMS can interact with track 1 or 3. The kiosk solution uses both the data from the One Card system and data on track 1or 3 for the CL locks. The kiosk uses both tracks for the management of the CL data on the credentials. The data the kiosk uses for matching credentials will be stored in two User Defined Fields that will be setup in the Cardholder Definition. These fields will be further defined in the section that follows.

Setting PIN Length

Before running the Kiosk Configuration application it is necessary to configure the PIN length in System Settings.

1. Go to **Start>Programs>Schlage SMS>Schlage SMS** or double click on the **Schlage SMS** icon from the desktop.
2. Double click on **System Settings**. The System Settings application will open.

3 Click on the **Campus Lock Settings** tab.



4 Using the **Automatic PIN Length** drop down in the **Global Settings** section of the tab, specify the length of the PIN. Minimum is 3 and maximum is 8.

5 Click **OK**. System Settings will close.

Note: PINs can not start with 0.

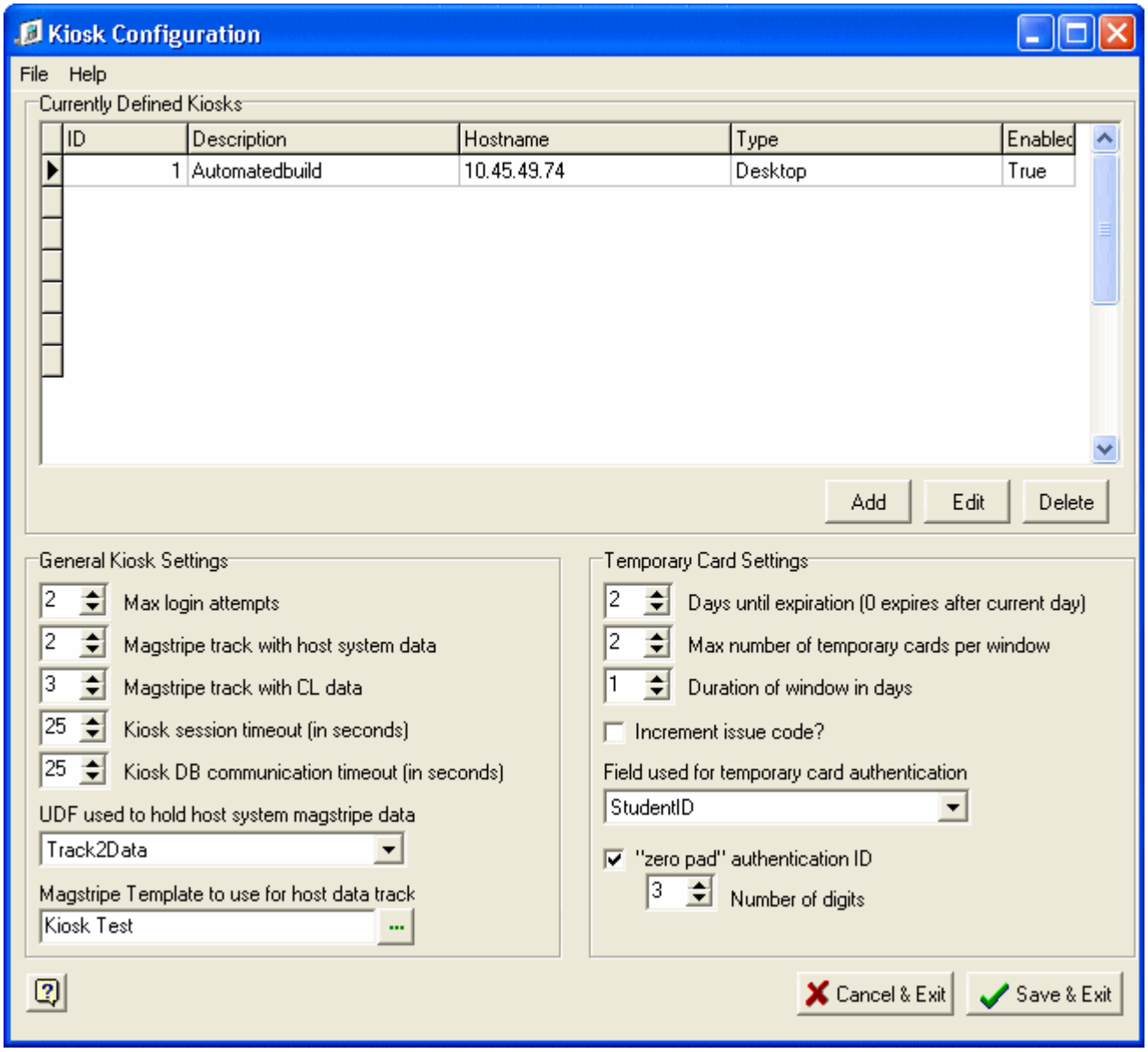
Accessing the Application

After the PIN length has been specified, the Kiosk Configuration application can be run.

1 Go to **Start>Programs>Schlage SMS>Schlage SMS** or double click on the **Schlage SMS** icon from the desktop.

2 Add Kiosk Configuration to the SMS Launcher. See the **System Security** Chapter of the SMS software manual for details on adding a program to the Launcher.

3 In the **System Launcher**, double click on the **Kiosk Configuration** icon. This opens the Kiosk Configuration program.



Currently Defined Kiosks

This section shows any kiosks (both dedicated kiosks and desktop kiosks) that have been added to the system. You can **Add** a new kiosk, **Edit** an existing kiosk or **Delete** a kiosk by clicking the appropriate button. For more details on adding a kiosk see the kiosk Definition section of this chapter.

General kiosk Settings.

These settings need to be defined for kiosks to interact with the database correctly. These are global settings that effect all the kiosks the user has defined.

- **Maximum Login Attempts** - Selects the number of logins a user can attempt before the session is terminated. Can be set from 1 - 5.
- **Magstripe track with host system data** - Defines which track number the system will use to find student or employee information. Track 2 is the standard track number to encode.
- **Magstripe track with CL data** - This is the track number that the kiosk will use while encoding a card. Track 3 is the standard track number to encode.
- **Kiosk session timeout** - Determines how many seconds can elapse after the user's last input before the kiosk resets to the start page.
- **Kiosk DB communication timeout** - Determines how long the system will wait to receive information from the Database. If the allotted time passes without a response from the database the system will cancel the user session.
- **UDF used to hold host system magstripe data** - This User Defined Field must contain all of the data encoded on track 2 of the credential being used for the CL locks. When a student uses their card at a kiosk this data will be used, and will be interpreted based upon the magstripe template you choose (see below), to verify that the student has the rights for the action they wish to perform. The information contained in this database field must match the track 2 data contained on the cardholder credential. For more information please see the User Defined Fields chapter and the Cardholder Definition chapter in the SMS Manual. This data will be used for all kiosk functions with the exception of the Temporary Card feature.
- **Magstripe Template to use for host data track** - Click on the browse button to select a magstripe template. All templates defined in the System Manager will be available here. This template will apply a mask to the data from Track 2 before it is compared with the information in the User Defined Field. For more information on defining a magstripe template please see the Defining Magstripe Template section of the System Manager chapter in the SMS manual.

Temporary Card Settings.

The use of both track 2 and the track the CL locks are configured for on the students's credential is critical for the temporary card function. The temporary card is issued based upon the validation of the track 2 data (Field used for temporary card authentication) input by the student (Student ID Number) and a PIN code which is configured for the credential for each cardholder using CL locks. Settings below are universal and affect all the kiosks the user has defined.

- **Days until expiration** - Determines how many days a temporary card is valid for. After this time expires the card will no longer be active. 30 days is the maximum. 0 denotes current day only.
- **Max number of temporary cards per window** - Determines how many temporary cards a user can receive in the given window of time.

- **Duration of window** - Determines how many days are in a temporary card allowance window. The window begins when the student receives their first temp card and ends after the number of days specified.

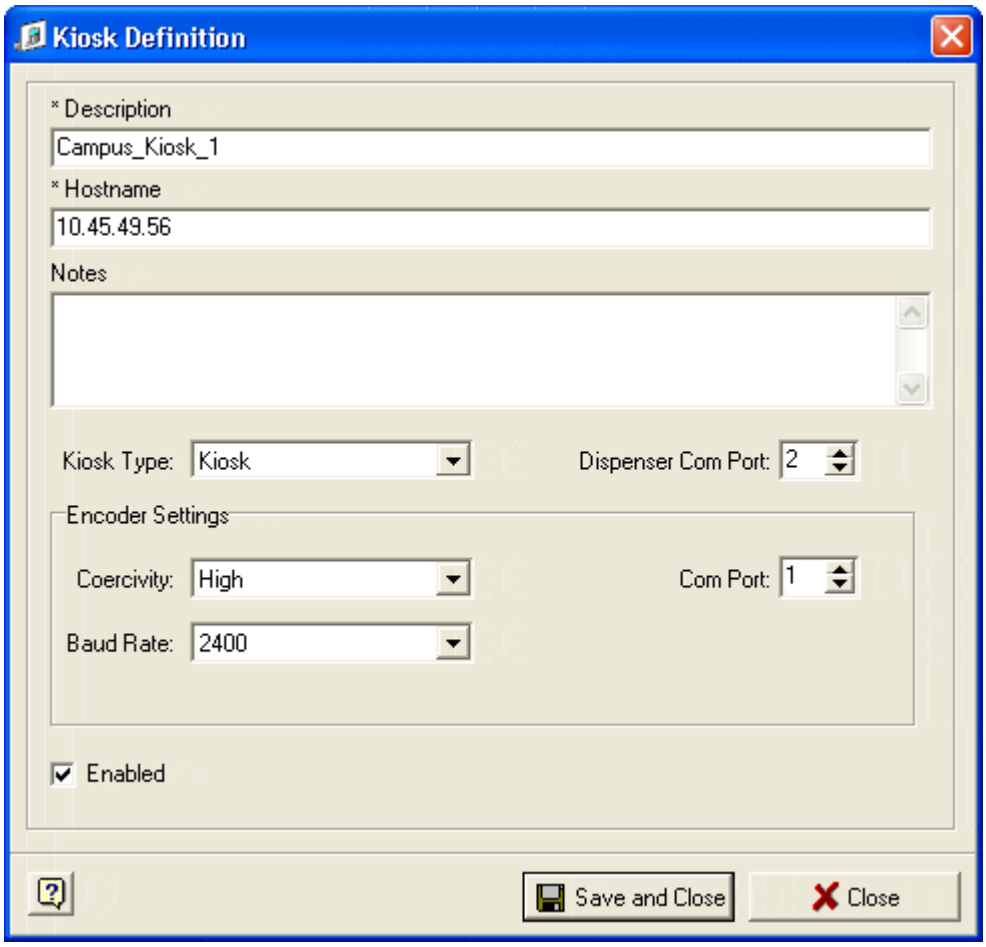
  Example 1: The Max number of temporary cards per window is set to 1 and the Duration of window is set to 7. When a student receives a temporary card they will not be able to do so again for seven days.

  Example 2: The Max number of temporary cards per window is set to 2 and the Duration of window is set to 5. When a student receives a temporary card they will only be able to get one more card in the next five days.

- **Increment Issue Code** - Putting a check in this box enables Issue Codes for temporary cards. If enabled this function will invalidate the user's permanent card at the time they get a temporary card.
- **Field used for temporary card authentication** - Specifies which User Defined Field (UDF) the system will refer to when authenticating a student's ability to receive a temporary card. This is typically a 9 digit student ID number.
- **"zero pad" authentication ID** - Check this box to enable zero pad authentication.
- **Number of digits** - Set this to the length of your Student ID number. Maximum length is 37.

Kiosk Definition

Each Campus Lock Keycard Center (kiosk or desktop) requires a system definition. Go to **Kiosk Configuration>Currently Defined kiosk>Add** to define each kiosk. Settings are specific to each kiosk.



1 **Description** - This is what appears in the Description column of the Kiosk Configuration program. Each kiosk should have a unique description.

2 **Hostname** - Enter the IP address of the kiosk being defined. (Please see the kiosk Set Up section for details on getting the IP address.)

3 **Notes** - This is an optional field. Put any additional information that you require here.

4 **Kiosk Type** - Select whether you are defining a dedicated kiosk or a Desktop/Laptop without Dispenser

5 **Dispenser Com Port** - Specify which Com Port the dispenser is using. For dedicated kiosks this should be set to 2. This value must be different than the setting for Encoder Com Port (see below for details on Encoder Com Port).

6 Define the **Encoder Settings**

a) **Coercivity** - The three options are High, Medium, and Low with High being the default. This option must match the magstripe badges the customer buys otherwise it will not encode properly and may damage the cards.

Note: High Coercivity cards are standard.

b) **COM Port** - Specify which COM Port the card encoder is connected to. For dedicated Kiosks this needs to be set to 1. For Desktop/Laptop Kiosks this can be set from 1 - 255 depending on which COM Port the encoder is connected to.

c) **Baud Rate** - Specify at what speed the kiosk communicates with the encoder. 9600 is recommended.

7 **Enabled** - Click this box to enable the kiosk after all the settings have been entered. If this box is left unchecked the kiosk will not function.

8 Click **Save and Close** to save the kiosk and return to the kiosk Configuration window.

User's Guide

CHAPTER 5

Introduction

Once the Campus Key Card Center has been set up and configured it is ready to be used by students and employees.

The kiosk has four different functions:

- Update ID
- Change Pin
- Get Temporary Card
- Staff Revalidation

Detailed below is how to use each of these functions from a kiosk or desktop version.

Update ID

This function is used to update access privilege on an ID card.

Example: A student changes rooms in the middle of the semester and the update is entered into the database. The student then goes to a kiosk to update his/her ID card with the new access privileges. The student is now granted access to the new room.

1. Touch the **Update ID** button on the left of the main screen.
2. Touch the **Press Here to Begin** button. Kiosk will beep when it is ready to read your card.
3. After the beep, insert card into right side card reader.
4. Enter your pin number. Touch **Submit**.
5. Card is updated with new access information.
6. Retrieve card from right side card reader.

Change PIN

This function is used to change the PIN for a given ID card.

1. Touch the **Change PIN** button on the left of the main screen.

2. Touch the **Press Here to Begin** button. kiosk will beep when it is ready to read your card.
3. After the beep, insert card into the right side card reader.
4. Enter current PIN number. Touch **Continue**.
5. Enter new PIN number. Touch **Continue**.
6. Re-enter new PIN number. Touch **Submit**.
7. PIN number will be updated.
8. Retrieve card from card reader.

Get Temporary Card

This function is used to generate a temporary card for lost or stolen ID cards. A student identification number and PIN is required.

1. Touch the **Get Temporary Card** button on the left of the main screen.
2. Enter PIN number. Touch **Continue**.
3. Enter your student ID number. Touch **Submit**.
4. Wait for temporary card to be dispensed from left side dispenser.
5. Kiosk will beep when it is ready to read your card. After the beep, insert temporary card into right side card reader.
6. Temporary card is encoded.
7. Retrieve temporary card from card reader.

Staff Revalidation

Staff Revalidation adds an extra level of security to your system by requiring staff with master access credentials to revalidate their cards on a periodic basis. Follow the instructions below to revalidate a card.

Note: For revalidation to work you need to check the **Revalidation Allowed at Kiosk** box in the User Type Definition window of the CL Lock profile in System Manager. For more details see the Defining User Type section of the Campus Locks chapter of the SMS manual.

1. Touch the **Staff Revalidation** button on the left of the main screen.
2. Touch the **Press Here to Begin** button. Kiosk will beep when it is ready to read card.
3. After the beep, insert card into the right side card reader.
4. Enter PIN. Touch **Submit**.
5. Card is revalidated.
6. Retrieve card from right side card reader.

Desktop Kiosk

CHAPTER 6

Introduction

Desktop Kiosk refers to any PC or laptop that has been configured to work as a Campus Lock Keycard Center. This allows for greater flexibility in the number of kiosks available. It is especially useful during high traffic times such as the beginning of a semester. The computer will need a JOMS UERW-301 encoder attached to it (in order to encode cards) and be web enabled so that the browser can interact with the IIS server hosting the kiosk interface.

Note: The Desktop Kiosk does not have the lock down software of a dedicated kiosk. Because of this, it is strongly recommended that a Desktop Kiosk not be used directly by students or staff but by an administrator assisting them.

System Requirements

Operating System:

- Windows XP with IE 6.x or 7.x

Hardware:

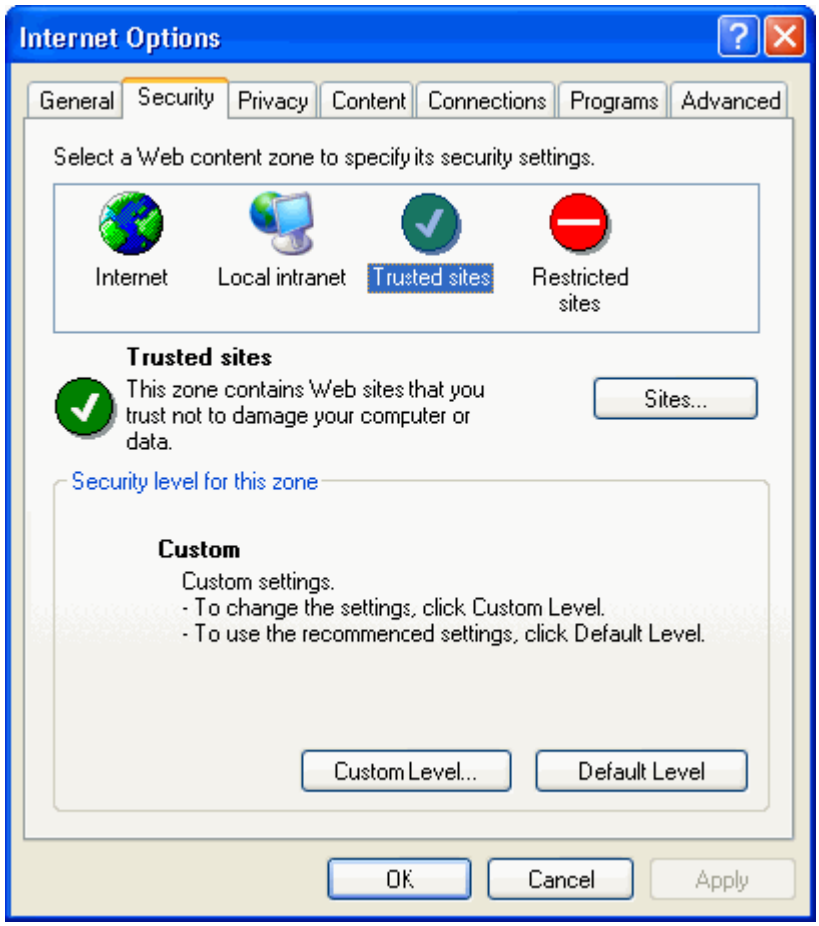
- As recommended by MS to run Windows XP (512 MB of RAM recommended)

Note: Desktop Kiosk is not supported on MS Windows Vista computers.

Installation

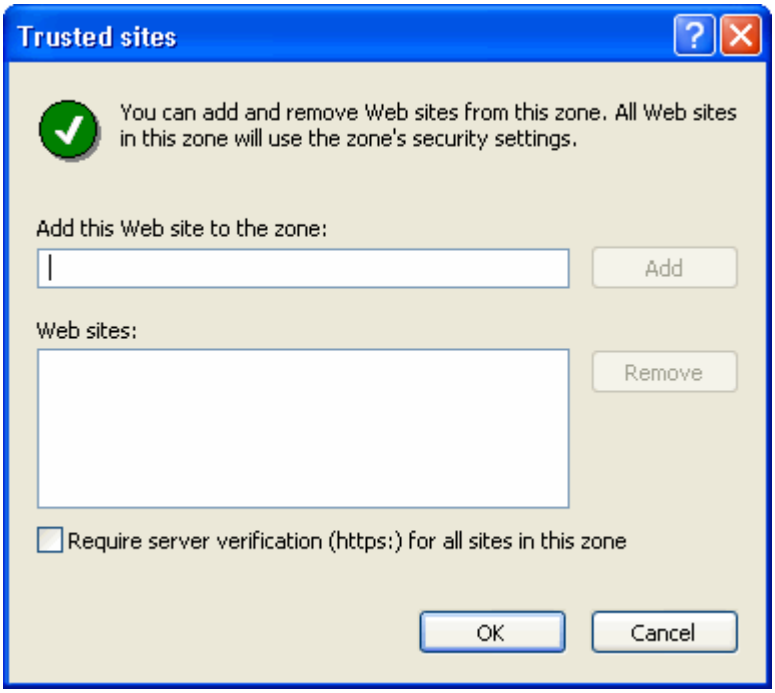
1. Attach JOMS UERW-301 encoder to serial port COM 1.
2. Run KioskClientInstall.exe installer.
3. Modify Internet Explorer Security settings. (These instructions are for IE 6.x and 7.x)
   a) Open **Tools>Internet Options.**

b) Select the **Security** tab.



c) Select the **Trusted sites** icon.

d) Click on the **Sites** button. The Trusted Sites window will open.



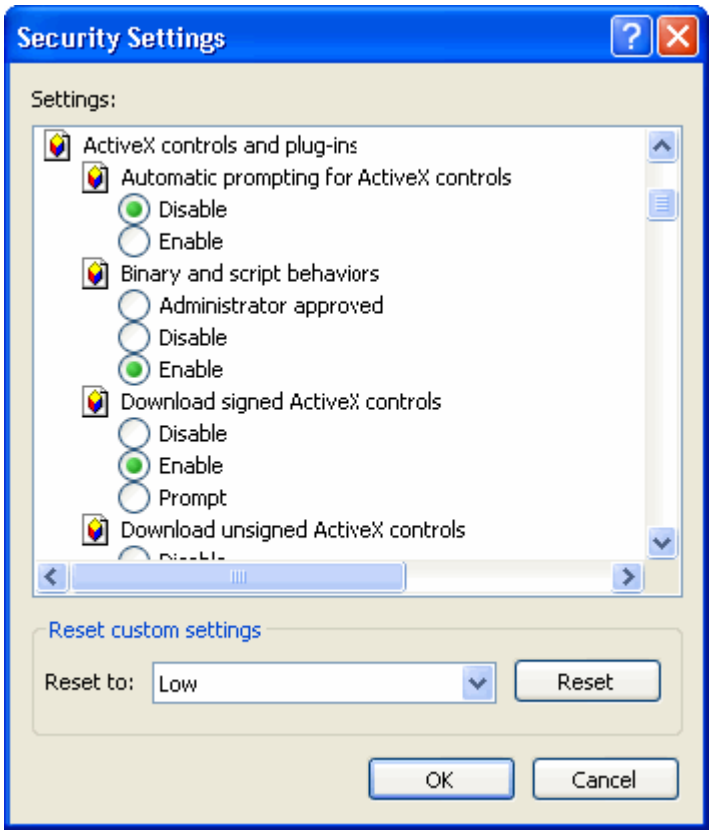
e) Type"http://IISServerAddress/kiosk/Default.aspx" in the **Add this Web site to the zone** box, where "IISServerAddress" is the address of your IIS server. Please see the Web Server Installation section for details.

f) Uncheck the **Require server verification (https:) for all sites in this zone** check box.

g) Click the **Add** button.

h) Click the **OK** button, this will save the site and return to the Security tab.

i) Click the **Custom level** button to open the Security Settings window.



j) Scroll to the **ActiveX controls and plug-ins** section.

k) Click the **Disable** button for Automatic Prompting for ActiveX Controls.

l) Click the **Enable** button for every other option in the ActiveX section.

m) Click **OK** at the bottom of the Security Settings window when you are finished.

n) A window will pop up and ask "Are you sure you want to change the security sections for this zone?" Click **Yes**.

o) Click **OK** to save these changes.

4 Modify Internet Explorer Security settings. (These instructions are for IE 7.x only)

a) Open **Tools>Internet Options.**

b) Select the **Security** tab.

c) Click the **Custom level** button to open the Security Settings window.

d) Scroll to the **Miscellaneous** section.

e) Click the **Enable** button for Access Data Sources across domain

f) Click the **Enable** button for Allow META refresh

g) Click the **Enable** button for Allow scripting of IE Web Browser control

h) Click the **Enable** button for Allow script initiated window without size

i) Click the **Disable** button for Use Phishing Filter

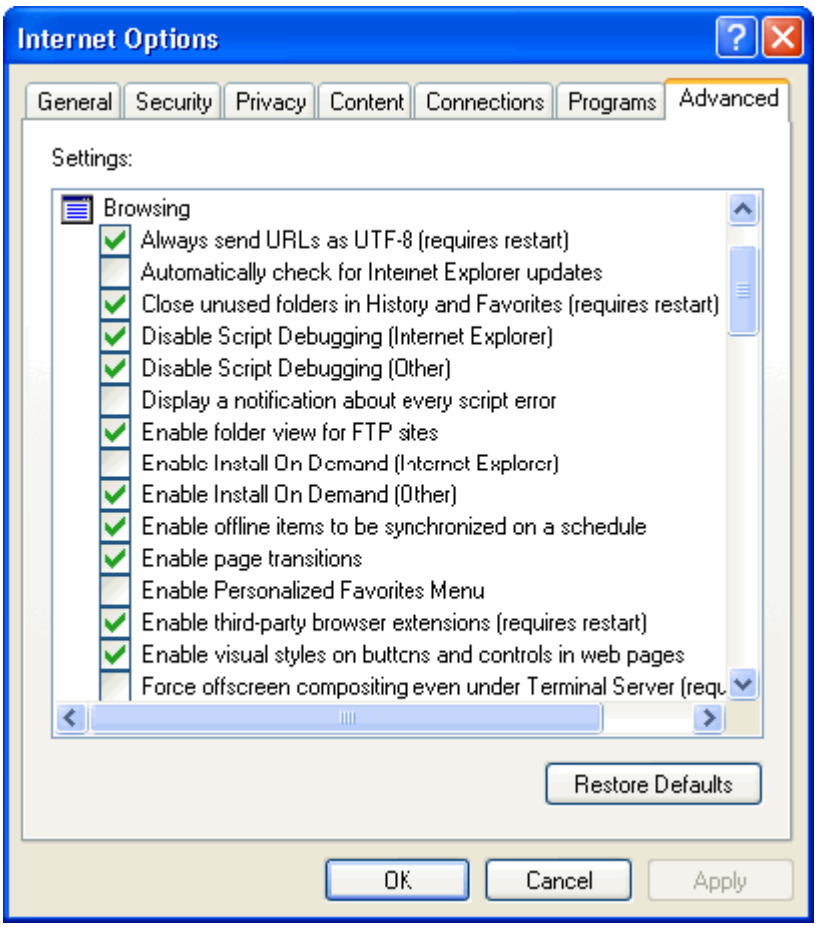
j) Click **OK** at the bottom of the Security Settings window when you are finished.

k) A window will pop up and ask "Are you sure you want to change the security sections for this zone?" Click **Yes**.

l) Click **OK** to save these changes.

5 Modify Internet Explorer Advanced settings. (These instructions are for IE 6.x and 7.x)
Open **Tools>Internet Options**

a) Select the **Advanced** tab.



b) Scroll to the **Browsing** section.

c) Put a check in the **Disable Script Debugging (Internet Explorer)** box.

d) Put a check in the **Disable Script Debugging (Other)** box.

6 Close and then re-open Internet Explorer.

7 To start using the Kiosk, point your IE browser to the appropriate address. Example: http://campusshowkiosk/kiosk

8 Go to full screen mode by either selecting **View>Full Screen** or by pressing **F11**.

Your Desktop is now ready to use. For more information on the kiosk functions please see the User's Guide chapter.

Note: For your Desktop Kiosk to work properly it needs to be defined in the Kiosk Configuration program. Please see the Configuring the Kiosk chapter for more details.

Ingersoll Rand's Security Technologies Sector is a leading global provider of products and services that make environments safe, secure and productive. The sector's market-leading products include electronic and biometric access-control systems; time-and-attendance and personnel scheduling systems; mechanical locks; portable security; door closers, exit devices, architectural hardware, and steel doors and frames; and other technologies and services for global security markets.

866-322-1237

www.schlage.com www.ingersollrand.com

 LK-5252 Rev. 011/07