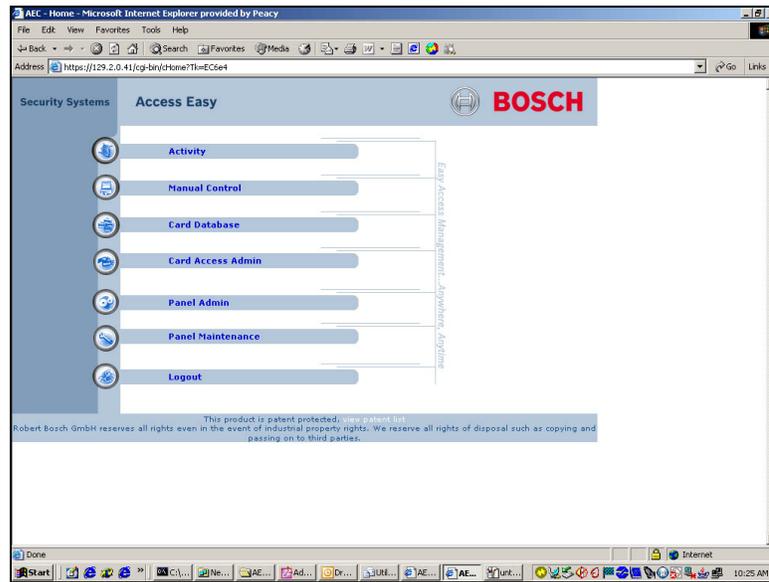


AEC



EN | Quick User Guide
Controller



BOSCH

Trademarks

Access Easy Controller™ is a trademark of Bosch Security Systems.

Netscape Navigator® is a registered trademark of Netscape Communications Corporation.

Microsoft®, Windows® 95, 98, ME, 2000, XP, and Windows NT® are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Other product and company names mentioned herein may be the trademarks of their respective owner.

Notices

All rights reserved. No part of this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise without the prior written permission of Bosch Security Systems.

This document is provided pursuant to a license agreement containing restrictions on their use. It contains valuable trade secrets and proprietary information of Bosch Security Systems and is protected by international copyright law. It may not be copied or distributed to third parties, or used in any manner not provided for in the said license agreement.

All software is provided "as is." The sole obligation of Bosch Security Systems shall be to make available all published modifications that correct program problems are published within one (1) year from the date of shipment.

The software is intended for use only with the hardware specified in this manual and in the absence of other software. Concurrent use with other software or with hardware not specified may cause the program to function improperly or not at all. Bosch Security Systems may not provide support for systems operating under such conditions.

All efforts have been made to ensure the accuracy of the contents of this manual.

The above notwithstanding, Bosch Security Systems assumes no responsibility for any errors in this manual or their consequences.

The information on this document is subject to change without notice.

End-User License Agreement for Access Easy Controller™ Software

Bosch Security Systems Software Products

- Server Software: Access Easy Controller (AEC) Software
- Number of Client Access Licenses: 8

Bosch Security Systems Hardware Products

- AEC and all input and output modules.



This End User License Agreement (EULA) is a legal agreement between you (either an individual or a single entity) and Bosch Security Systems for the Bosch Security Systems Software Product that you acquired and any hardware product previously identified.

The Software Product includes computer software, associated media, printed materials, and any online or electronic documentation. By installing, copying, or otherwise using the Software Product, you agree to be bound by the terms of this EULA. If you do not agree to the terms of this EULA, Bosch Security Systems or its resellers are unwilling to license the Software Product to you. In such event, you may not use or copy the Software Product, and you should promptly contact Bosch Security Systems or its distributors for instructions on returning the unused product for a refund.

Software Product License

The Software Product is protected by copyright laws and international copyright treaties, as well as intellectual property laws and treaties.

The Software Product is licensed, not sold.

Grant of License

The Software Product refers to the AEC software that runs on the AEC to enable a computer or workstation running a web browser software (Third-Party Software) to access or utilize the services provided by the AEC access control. This EULA grants you the following rights to the Software Product:

- **Use of the Server Software:** You may use one copy of the Server Software running on one Server that may be connected at any point in time an unlimited number of workstations or computers operating on one or more networks. You must acquire a separate Client Application Software License to access or otherwise utilize the services of the Server by using the Third-Party Software.

Other Rights and Limitations

- **Client Access Licenses:** This EULA grants you the number of Client Access Licenses for the Software Product indicated at the top of this EULA. Each license permits one additional computer or workstation the right to access or utilize the services of the Server. The services of the Server are considered to have accessed or utilized when there is a direct or indirect connection between a computer or workstation and a Server.
- **Restriction:** You are restricted from copying or modifying the Software Product. The Software Product is copyrighted by Bosch Security Systems or third parties. Except as expressly permitted in this agreement, you may not copy or otherwise reproduce the Software Product. In no event does the limited copying or reproduction permitted under this agreement include the right to de-compile, reverse engineering, disassemble, modify or electronically transfer the Software Product, or to translate the Software Product into another computer language.
- **Separation of Components:** The Software Product is licensed as a single product. Its component parts may not be separated for use on more than one Server.
- **Rental:** You may not rent or lease the Software Product.
- **Termination:** Without prejudice to any other rights, Bosch Security Systems may terminate this EULA if you fail to comply with the terms and conditions of this EULA. In such event, you must destroy all copies of the Software Product and all of its component parts.

Copyright

All title and copyrights in and to the Software Product (including but not limited to any images, photographs, animations, video, audio, music, text, and applets incorporated into the Software Product), the accompanying printed materials, and any copies of the Software Product, are owned Bosch Security Systems or its suppliers. The Software Product is protected by the copyright laws and international treaty provisions. You may not copy printed materials accompanying the Software Product.

Limited Warranty

Bosch Security Systems warrants that (a) AEC Software and (b) AEC access control panels and all input/output modules manufactured only by Bosch Security Systems will perform adequately in accordance with the accompanying User's Manual; and will be free from defects in materials and workmanship under its intended normal use and service for a period of 1 year from date of purchase.

Customer Remedies

Bosch Security Systems's entire liability and your exclusive remedy shall be, at Bosch Security Systems option, either (a) return of the price paid or (b) repair or replacement of the hardware or software that does not meet Bosch Security Systems's limited warranty and which is returned to Bosch Security Systems with a copy of your purchase receipt. This limited warranty becomes void if failure of the hardware or software has resulted from abuse, accident or misapplication.

No Liability or Consequential Damages

Under no circumstances shall Bosch Security Systems or its suppliers be liable for any other damages whatsoever (including, without limitation, damages for business interruption, loss of business profits or other pecuniary loss) arising out of the use of or inability to use this Bosch Security Systems product. Bosch Security Systems total liability under any provision of this agreement shall be limited to the amount actually paid by you for the product.

Contents

1.0	AEC and Computer Setup	5	10.1	Controlling Doors	20
1.1	AEC Setup.....	5	11.0	Manual Control (Input)	21
1.2	Installing TCP/IP and Setting Computer IP Address	5	11.1	Controlling Alarm Zone Input Points.....	21
1.2.1	Configuring Network on Windows (Windows XP)	5	11.2	Controlling Individual Input Points.....	21
1.2.2	Configuring Network on Macintosh.....	7	12.0	Manual Control (Output)	21
1.3	Configuring Web Browser for AEC	7	12.1	Controlling Output Points.....	21
1.3.1	Setting Web Browser for Windows	7	13.0	Reset APB	22
1.3.2	Setting Web Browser for Macintosh	9	13.1	Resetting APB Based on Card Number Regarding Reader/All Readers	22
1.4	Setting Initial AEC Configuration	10	13.2	Resetting APB Based on Name Regarding Reader/All Readers	22
1.4.1	Reconfiguring Web Browser for New IP Address	10	13.3	Resetting APB by All Card Numbers Regarding Reader/All Readers	22
2.0	Access Control Systems	12	14.0	Printing a Report	23
3.0	Log On/Log Off.....	13	15.0	Utilities Programs	24
3.1	Logging On	13	15.1	Running IP Setup.....	24
3.2	Logging Off	13	15.2	Viewing TypeMenu Items	24
4.0	Screen Navigation.....	14	15.2.1	Start.....	25
4.1	View Activity	14	15.2.2	Export.....	25
4.2	Manual Control	14	15.2.3	About.....	25
4.3	Card Database.....	14	15.2.4	Exit.....	25
4.4	Card Access Admin.....	14	15.3	Scanning and Changing Controller IP Address Data	25
4.5	Panel Administration.....	15	15.4	Scanning and Changing Specific Controller IP Address Data	26
4.6	Panel Maintenance	15	15.5	Scanning and Changing Controller IP Address Database on Search Criteria.....	26
4.7	Logout.....	15	15.6	Changing the Password	27
5.0	Schedules.....	15			
5.1	Defining a New Schedule	15	Figures		
6.0	Holidays.....	16	Figure 1:	AEC Server and Notebook Connection ..	5
6.1	Defining Holiday Date.....	16	Figure 2:	AEC Quick Start Stages	13
7.0	Access Groups.....	16	Figure 3:	Schedule.....	15
7.1	Defining Access Group	16			
8.0	Card Assignment.....	17	Tables		
8.1	Adding Range of Card Number	17	Table 1:	Web Page Icons	19
8.2	Adding Range of Card Numbers with Same Data Entries	17	Table 2:	View Activity Screen Columns.....	19
8.3	Adding Card Number to Database	18	Table 3:	Reports.....	23
8.4	Enrolling Card with an Unknown Wiegand Format	18			
8.4.1	Enrolling Card Using Web Page	18			
9.0	View Activity	19			
10.0	Manual Control (Door)	20			

1.0 AEC and Computer Setup

This document supplements the user manual and is not intended to be used as a stand-alone document.

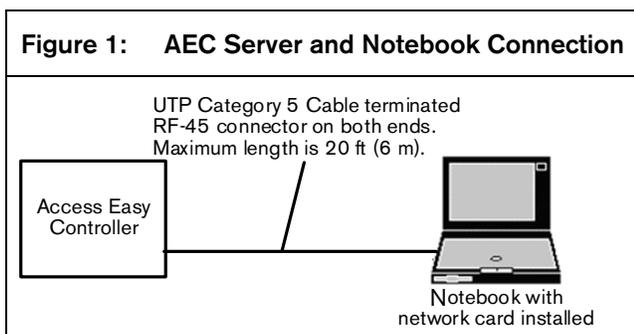
Before an AEC can be operational, you must perform basic set-up procedures. This section describes the configuration procedures required to prepare the AEC for connection to the customer's network. It also summarizes the configuration needed on a computer for the computer to connect to the AEC.

1.1 AEC Setup

AECs are shipped from the factory configured with the default IP address of 129.2.0.41. Before connecting the controller to the customer's network, change its IP address to correspond to the customer's network configuration. In instances where the AEC is directly connected to a stand-alone computer on its private network, you might not need to change the AEC's default address. Only configure the computer's network settings so it has an address on the same network as the AEC.

Use a Notebook or Desktop computer for the initial setup. The computer must have a 10/100Base-T Ethernet card installed and run any version of the Window or Macintosh operating system. The computer must also have a functional web browser program, such as Microsoft Internet Explorer (version 4.0 and later) or Netscape Navigator (version 4.0 and later).

1. Configure the computer to set the AEC's IP address to have an IP address on the same 129.2.0 network as the AEC. Set the computer's IP address to 129.2.0.40 and the subnet mask to 255.255.0.0. If you do not know how to change a computer's network settings, refer to *Section 1.2 Installing TCP/IP and Setting Computer IP Address* on page 5.
2. Connect the AEC to the computer using a standard Category-5 crossover cable (beige Category-5 cable) as shown in *Figure 1*.



Only use LAN 1 Port. Do not plug the crossover cable into LAN 2.

3. Follow the procedure in *Section 1.4 Setting Initial AEC Configuration* on page 10.

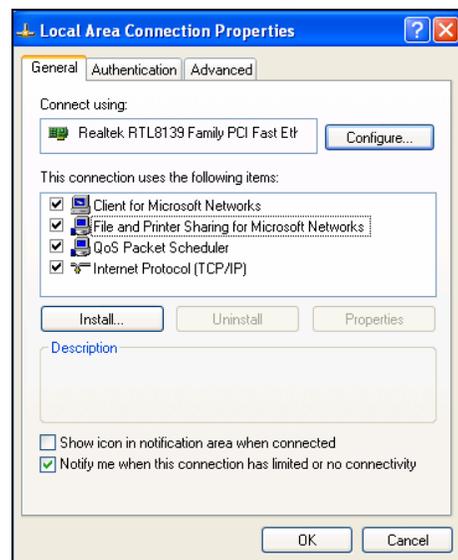
1.2 Installing TCP/IP and Setting Computer IP Address

This section describes how to install the TCP/IP communication protocol on a computer and assign an IP address to a computer. The first example describes a computer running Windows XP; the second describes the Apple Macintosh.

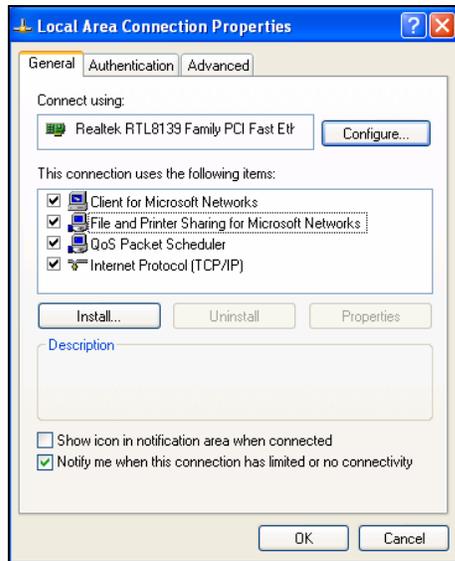
1.2.1 Configuring Network on Windows (Windows XP)

The following example is based on Window XP. Although differences might appear in some dialogs, screens, and descriptions when using another version or a different operating system, the configuration principles are the same.

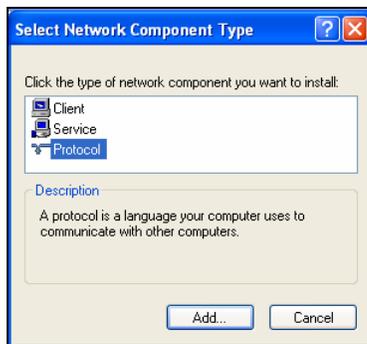
1. Click  and select **Control Panel**→**Network Connections**.
2. Double-click  and select **Properties** to open Local Area Connection Properties.



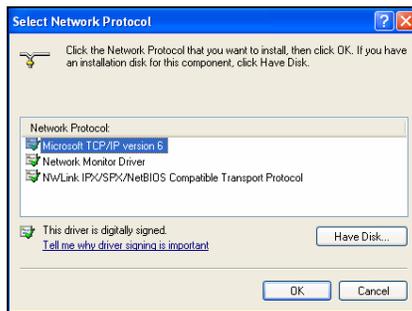
3. At **This connection uses the following items**, use the scroll bar to locate **Internet Protocol (TCP/IP)**.



4. If **Internet Protocol (TCP/IP)** is found, select it and go to *Step 10*. If **Internet Protocol (TCP/IP)** is not found, follow *Steps 5* through *8* to install it.
5. To add TCP/IP, click **Install...** to open the Select Network Component Type dialog.



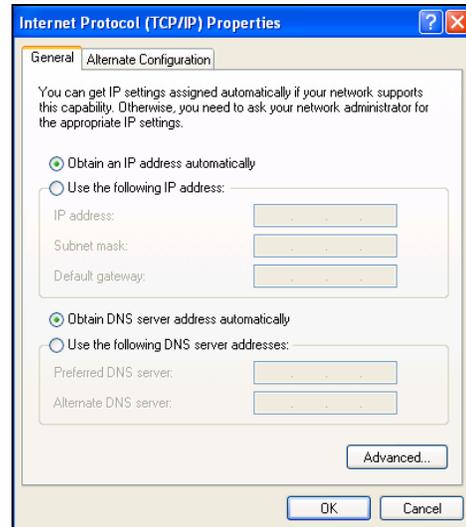
6. Highlight **Protocol** and click **Add...** to open the Select Network Protocol screen.



7. At **Network Protocol**, select **Microsoft TCP/IP version 6**.
8. Click **OK** and follow the instructions that appear on the screen.
9. If prompted, insert the Windows installation disk in the CD ROM drive. When finished, return to *Step 4* and select **TCP/IP Protocol – network**

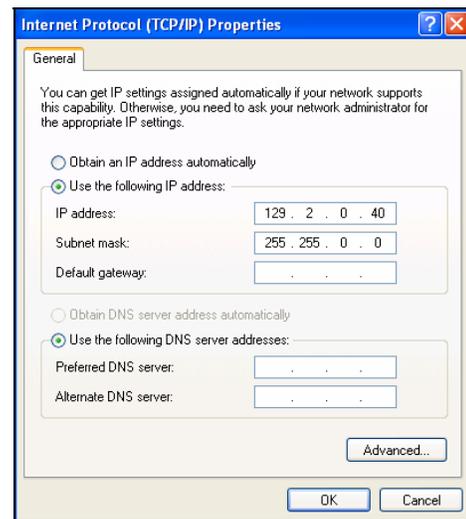
adapter line from the list of installed network components. Then go to *Step 10*.

10. With **TCP/IP – adapter component** highlighted, click **Properties** to open the Internet Protocol (TCP/IP) Properties dialog.



11. Select **Use the following IP address:** to enable the **IP address:** and **Subnet mask:** fields.
12. Type the IP address and subnet mask in their corresponding fields.

The following screen shows the recommended address and subnet mask assigned to the computer to communicate with a new AEC as received from the factory. Leave the DNS related fields blank.

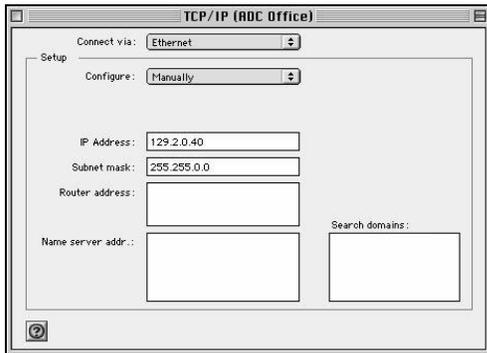
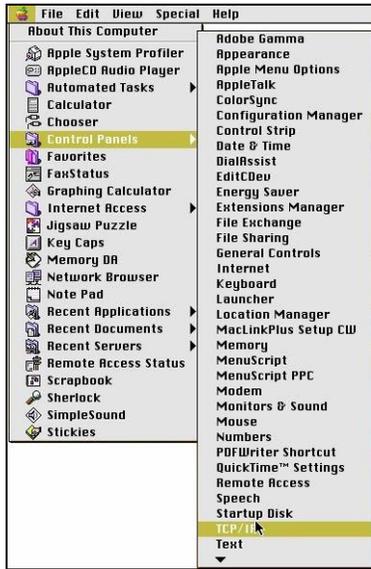


13. Verify the IP address and subnet mask are correctly entered. Then click **OK**.
14. The computer configures the TCP/IP settings, and when finished prompts you to reboot the computer for the new settings to take effect.

1.2.2 Configuring Network on Macintosh

The following example is based on an iMac. Although the screens might appear different when configuring other Apple models, the configuration principles are the same.

1. Click the **Apple** icon and select **Control Panels**→**TCP/IP** as shown.



2. When the TCP/IP dialog opens, type the IP address and subnet mask in the corresponding IP Address: and Subnet mask: fields.

This example shows the recommended address and subnet mask assigned to the computer to communicate with a new AEC as received from the factory.

3. When prompted, click **Save** to open the following message.



4. Click **Save** to confirm the action.

1.3 Configuring Web Browser for AEC

Use the following procedures to configure a web browser to operate with the AEC. In most cases, you are not required to make changes to a web browser setup to connect to an AEC. These procedures are for first-time browser users and as technical reference if there is difficulty in connecting to an AEC.

1.3.1 Setting Web Browser for Windows

Use this procedure to configure Microsoft's Internet Explorer, version 6.0. Other web browsers are similar.

1. From the Windows **Control Panel**, click  to open the Internet Options dialog.



2. To show the AEC Login page every time you activate your web browser software, change **Home page Address:** to the AEC assigned IP address.
3. At **Temporary Internet files**, click **Settings...** to open the Settings dialog.

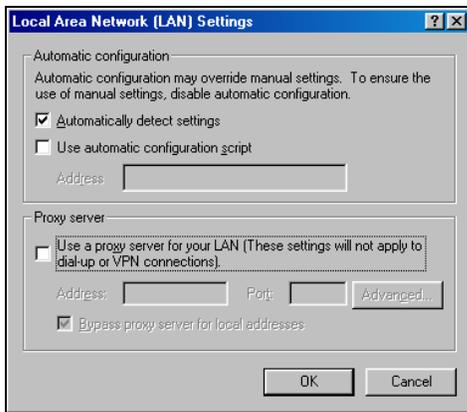


4. Verify **Check for newer versions of stored pages** is set to **Automatically**. If it is not, select it. This step is necessary for View Activity screens to refresh periodically.

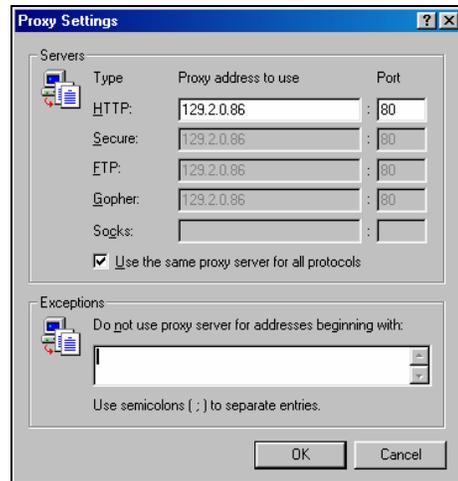
- Click **OK** to save your settings, close the dialog, and return to the Internet Option dialog.
- Select the **Connections** tab to open the Connections dialog.



- Click **LAN Settings...** to open the LAN Settings dialog.



- If your network does not use a proxy server, go to *Step 13*.
- If your network uses a proxy server, select **Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections)**, to open the Proxy Settings dialog.



- At **Exceptions**, type the default IP address of the AEC.
- If the permanent AEC IP address is different from the default address, also enter the controller's permanent address in **Exceptions**, separating each address with a semicolon (;).
- If there are addresses already listed in this field, add the AEC address and separate each address with a semicolon.

The following screen shows the default AEC IP address and three additional IP addresses (129.3.0.202, 129.3.0.203, and 129.0.204).



- Click **OK** repeatedly to exit the Internet Options Proxy Settings dialog. Then close the Control Controller.
- Ensure you have a crossover type network cable connected between the computer and the AEC. Run the web browser program from Windows.



You might receive a warning message (below) indicating the page you are trying to reach is not available. Do not be concerned with this message at this time.



- At **Address**, type the AEC IP address.

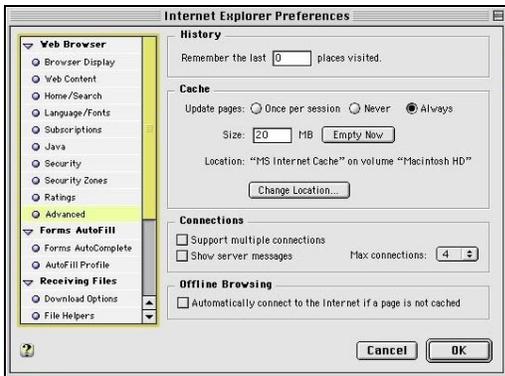
16. Press the [Enter] key or click  to open the AEC Login page.
17. Log in using the default user ID (USER1) and password (8088) to open the AEC Home page.
18. At the Home page, select **Panel Admin**→**Panel Setup** to open the Network Settings dialog.
19. Make the required changes to configure the AEC for operation on the customer's network. Then click  to store the changes.
20. When the database is saved, reboot the AEC to start up using the new IP address.
The controller is ready to connect to the customer's network.

 For detailed information on database configuration, refer to *the AEC Software User Manual (P/N: F01U027398)*.

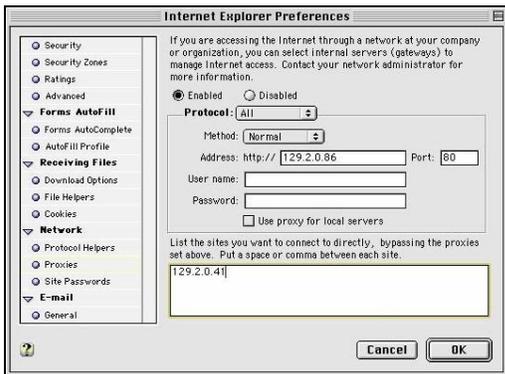
1.3.2 Setting Web Browser for Macintosh

Use this procedure to configure the Microsoft Internet Explorer (version 5.0) for Macintosh. Other web browsers are similar.

1. Launch Internet Explorer for Macintosh and select **Preferences** from the toolbar to open the Internet Explorer Preferences dialog.

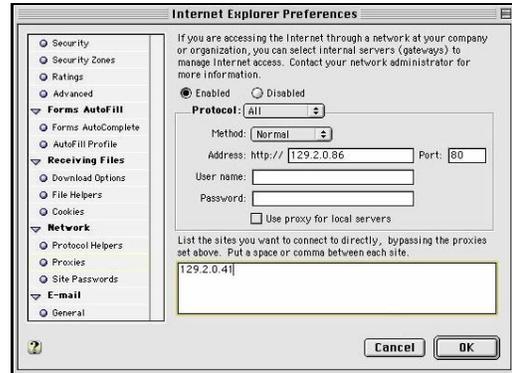


2. From the Web Browser menu, select **Advanced** to open the Advanced Settings screen.



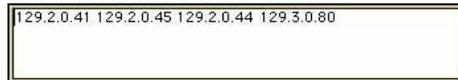
3. At the **Cache** area, set **Update pages:** to **Always**.

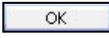
4. If your network does not use a proxy server, go to *Step 8*.
5. If your network uses a proxy server, use the menu Preferences scroll bar to locate **Network**. Then select **Proxies** to open the following screen.



6. At **List the sites you want to connect to directly, bypassing the proxies set above. Put a space or comma between each site.**, type the default AEC IP address.
7. If the permanent AEC IP address is different from the default address, add it and separate each address with a space or comma.
8. If there are addresses already listed in this field, add the AEC address and separate each address with a space or comma.

The following screen shows the default AEC IP address and three additional IP addresses (129.2.0.45, 129.2.0.44, and 129.3.0.80).



9. Click  to close the dialog.
10. Ensure you have a crossover type network cable connected between the computer and the AEC. If the web browser is not running start it at this time.

 You might receive a warning message (below) indicating the page you are trying to reach is not available. Do not be concerned with this message at this time.



11. At **Address**, type the AEC IP address.

12. Press the [Enter] key or click  to open the AEC Login page.
13. Log in using the default user ID (USER1) and password (8088) to open the AEC Home page.



For detailed information on database configuration, refer to *the AEC Software User Manual* (P/N: F01U027398).

1.4 Setting Initial AEC Configuration



Set the AEC IP address, subnet mask, and gateway address before installing the controller on a customer's network.

1. Connect a computer running the Windows operating system directly to the AEC using the crossover network cable.
2. The computer used must be configured for the 129.2.0 network:
 - IP address - 129.2.0.40
 - Subnet mask - 255.255.0.0
 - Gateway - 0.0.0.0
3. Use the crossover cable to connect the computer to the controller.
4. Power up the AEC if not already done.
5. The CPU card performs a power-up self-test that takes approximately 90 sec to complete. When the test is finished, LEDs 1, 2, and 3 alternately flash in the lower corner of the Secure/Communication Card.



During the power-up self test, there is no communication with the AEC. Wait until the self-test is complete before proceeding.

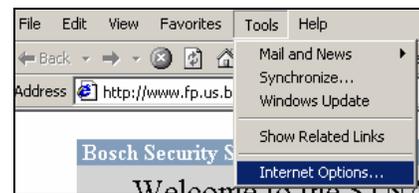
6. On the computer, open a web browser application (Microsoft Internet Explorer or Netscape Navigator) and type the AEC IP address (129.2.0.41) in the browser's address or location bar.
7. Click **GO** or press [Enter] to connect to the AEC and open the AEC Login screen.
8. Log in to AEC using the master user name (user1) and password (8088).
9. Press **Login** to open the AEC Home page. Then select **Panel Admin** to open the Users list screen.
10. Select **Panel Setup** from the menu on the left-side menu to open the Network Settings page.
11. Set the AEC **IP Address**, **Netmask**, and **Gateway** fields to the values provided by the customer.

The values for these fields must be set correctly for the controller to operate over the customer's network. Contact the customer or a representative from the customer's IT department.

12. Click **Save** at the bottom of the screen.
13. Select **Reboot controller** from the left-side menu. This causes the controller to reboot and load the new IP address information entered and saved in the previous steps. After rebooting, the controller begins responding to its new address, no longer responding to the default address 129.2.0.41.

1.4.1 Reconfiguring Web Browser for New IP Address

Reconfigure the web browser for the new IP address. Use the following procedure to configure Internet Explorer. For Macintosh, refer to *Section 1.3 Configuring Web Browser for AEC* beginning on page 7.



1. Open your browser and select **Tools**→**Internet Options...** to open the Internet Options dialog.

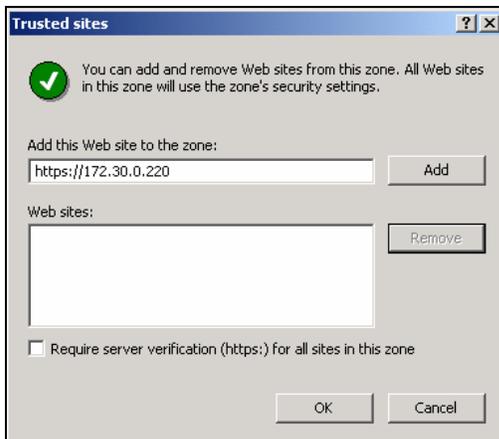


The example used here is Internet Explorer (version 6.0). The actual screen might be different depending upon the browser used.

- Click the **Security** tab to open the Security dialog.



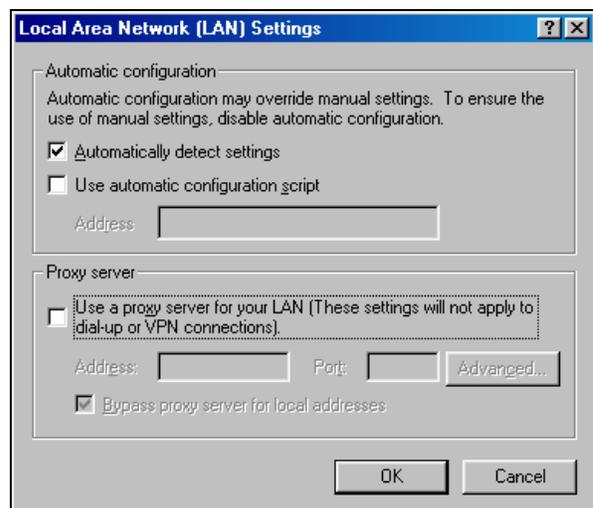
- Click the **Trusted Sites** icon and **Sites...** to open the Trusted sites screen.



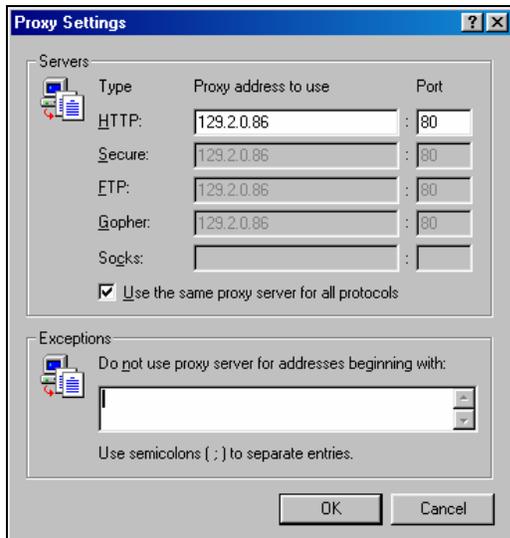
- At **Add this Web site to the zone:**, type the AEC IP address as **https://XXX.XXX.XXX.XXX** (where X is your AEC IP Address). The IP address used here is an example. Your IP address is most likely different.
- Click **Add...** to show the IP address in **Web sites:**.
- Click **OK** and return to the Internet Option screen.
- Select the **Connections** tab to open the Connections dialog box.



- Click **LAN Settings...** to open the Local Area Network (LAN) Settings dialog.

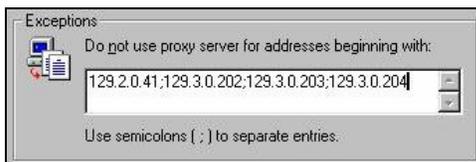


- If your network does not use a proxy server, go to *Step 10*.
- If your network uses a proxy server, select **Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections)**, to open the Proxy Settings dialog.



11. At **Exceptions**, type the default IP address of the AEC.
12. If there are addresses already listed in this field, add the AEC address and separate each address with a semicolon.

The following screen shows the default AEC IP address and three additional IP addresses (129.3.0.202, 129.3.0.203, and 129.0.204).



13. Click **OK** repeatedly to exit the Internet Options screen. Then close the Control Controller.
14. Ensure you have a crossover type network cable connected between the computer and the AEC. Run the web browser program from Windows to open the browser.
15. Before connecting the AEC to the customer's network, test it using the new settings to confirm proper setup.
16. Change the network configuration of your computer to an address on the same network as the AEC. Refer to *Section 1.2 Installing TCP/IP and Setting Computer IP Address* beginning on page 5 for details on this configuration.

For example, you set the AEC IP address to 172.30.0.220 and the Netmask to 255.255.0.0. To test the AEC using your computer, change the computer's network setup to a similar address on the same network. If you set the computer to 172.30.0.222, you must set the Netmask on the computer to the same value as the AEC.

17. After changing computer's network setup, reboot the computer.
18. Connect the AEC by typing its new address in the location or address bar of the browser, opening the Login screen.
19. When the proper operation is confirmed, log out of the AEC and close your browser.
20. Disconnect the crossover cable from both the AEC and the computer.

The AEC is ready to connect to the customer's network. Generally, this connection is made to a wall jack or hub using a straight-through network cable.

2.0 Access Control Systems

An Access Control System (AEC) is a computerized entry controller of any area that can be secured with a lock and key and monitored with alarm points. The controller locks and unlocks doors and tracks persons in certain areas during specific times. An alarm point can be anything from a door to a motion detector that changes state. For example, a door alarm point can change from normal to an alarm state if it is opened from the previously closed or normal state.

An access control system grants and denies access to areas such as entire buildings, individual offices, designated areas, parking lots and/or outside-gated areas. Corporate management defines access by configuring the AEC with pertinent information, such as who, what, when, or where.

- A card assigned to an individual acts as a key to unlock secured areas and allow access. Each card has an internal encoded number, identified by the Access Control System. When the reader reads a card, the encoded number locates the person's information in the AEC database. The database is configured with information about the person along with access rights.
- Access rights grant or deny access based on a criterion, such as management, department, or any scheme fitting your environment. Access rights assigned to individuals enable when and where access is granted. Schedules can be set up to control when certain access rights are valid and when to lock or unlock areas based on a time criterion.

3.0 Log On/Log Off

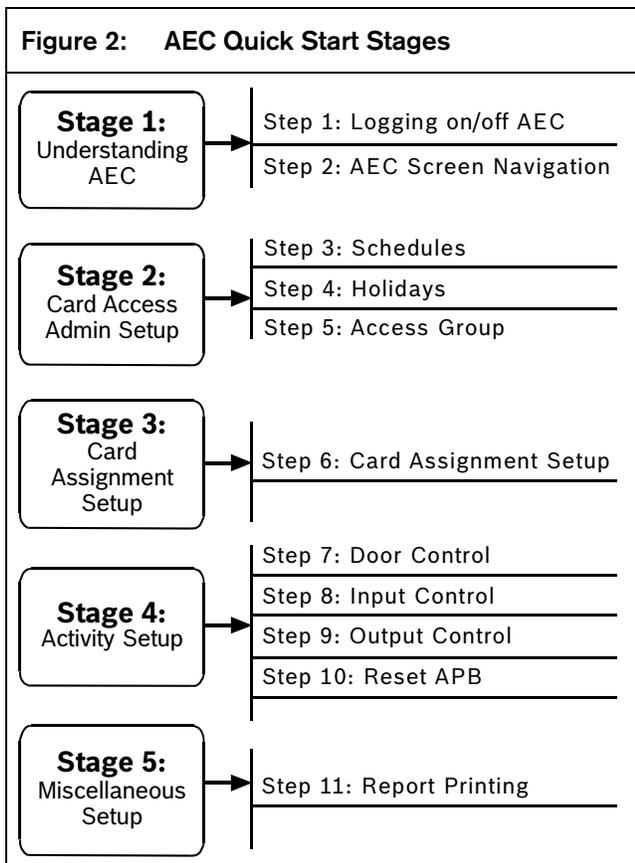
The AEC uses the web to change an access control system's implementation.

The conventional implementation installs PC based application programs to remotely control and monitor a controller in the system. In addition, application programs designed for a specific operating system must be re-developed before it can run on another operating system (such as Windows 98® to Windows NT/2000®).

The AEC combines the features of a web server and access control functionality into one complete unit. This combination provides a highly cost-effective solution that offers you the simplicity and ease-of-use associated with the web browser. All these, plus sophisticated security features essential for small to medium-sized businesses completes the package.

The AEC adopts a design common to all web based applications for consistency and ease of use. The same look-and-feel such as buttons and check boxes you experienced in other web-based applications are in the AEC.

Refer to *Figure 2* for the stages for an AEC quick start. For additional details, refer to the *AEC Software User Manual* (P/N: F01U027398).



3.1 Logging On

A working knowledge of Windows® or Macintosh® and the standard web browser, either Internet Explorer®, version 4.0 or higher, or Netscape Navigator®, version 4.0 or higher, and the ability to maneuver with a mouse is required to complete the screens.

When the AEC is initially installed, there is only one assigned user ID and password. This default user ID (super user) is assigned to the system administrator. The access rights cannot be disabled, but the user ID and password can be changed. The default user ID is "user1" and the password is "8088".



Once the system is commissioned, immediately change the default user ID and password to prevent unauthorized access.

1. Launch your web browser and type the AEC URL address to open the User Login page.
2. Type your user ID and password to begin operations.

If you do not know your user ID and password, contact your system administrator. User IDs and passwords are configured by the system administrator.

3.2 Logging Off

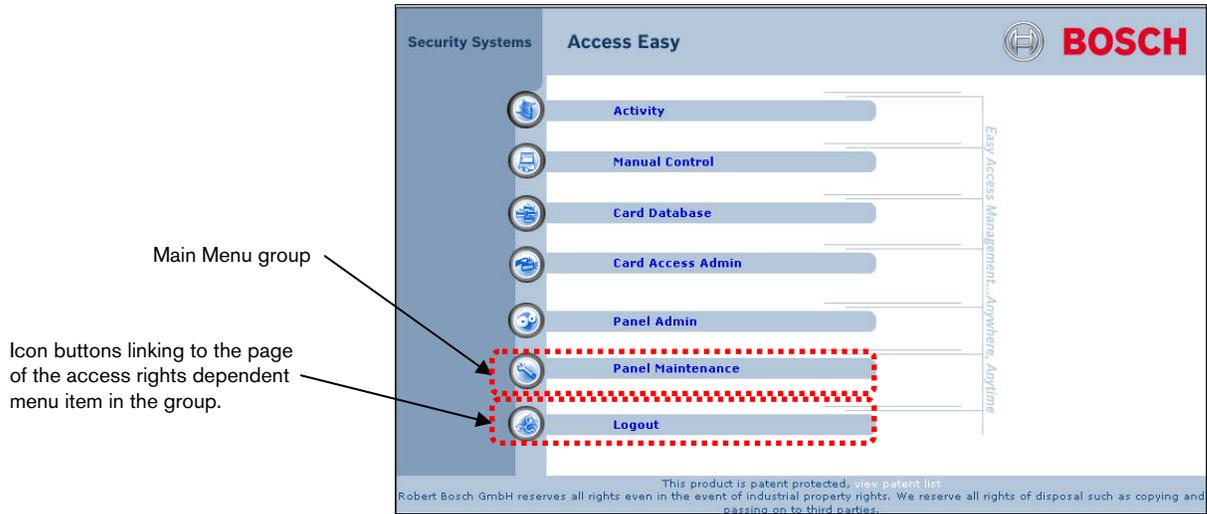
1. Click the **Logout** link.
A message box prompts you to back up the database.
2. Click the appropriate button to proceed.



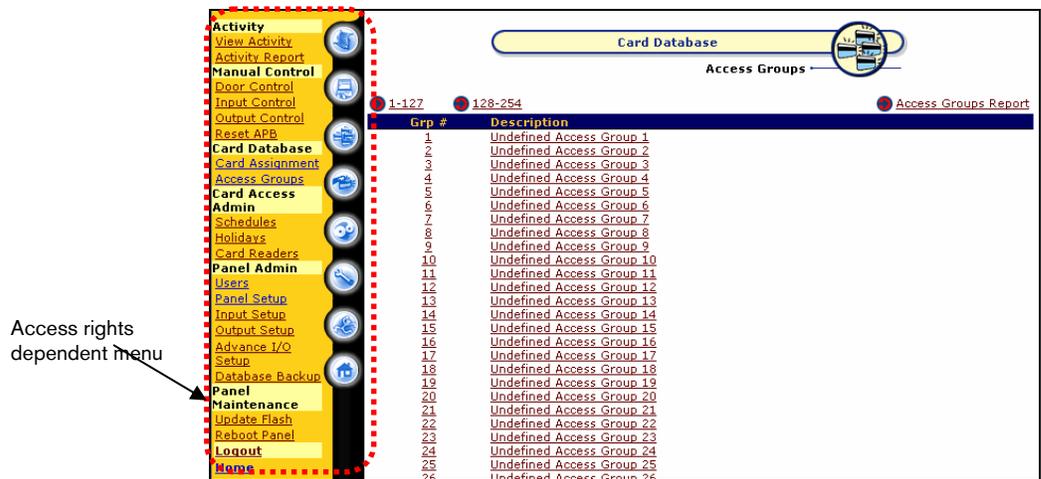
Always log off before leaving the computer.

4.0 Screen Navigation

After you log on, the Home page with icon buttons and menu item groups opens.



If you have access rights to one or more menu items of a group, click on the group link or icon button to view the menu item web page. Click the menu items links on the left pane to maneuver around the various web pages.



4.1 View Activity

Select transactions for access control, system control, and alarm conditions from the View Activity menu. The transactions categories are **Alarm**, **Valid**, **Restore**, and **Time Attendance**. Select **All Transactions** to view all categories.

4.2 Manual Control

This group represents user intervention or manual control of system hardware. It includes **Door Control**, **Input Control**, **Output Control**, and **Reset APB**.

4.3 Card Database

Access Groups: Categorizes the card readers into different access groups for the cardholder’s access rights during a specific schedule.

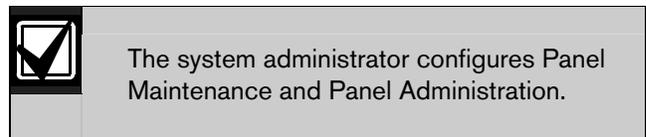
Card Assignment: Identifies rights and parameters by entering the cardholder’s name, number, right to arm or disarm an alarm zone, and so on.

4.4 Card Access Admin

Schedules: Sets up time intervals for use in access, system and hardware control.

Holidays: Defines and assigns programmable holiday dates.

Card Readers: Defines the function of the reader and its parameters, such as **Door Settings**, **Hardware Setup**, and so on.



4.5 Panel Administration

Users: Sets up the user ID and password including access rights to the various menu items. This is configured by the system administrator.

Input Setup: Sets up the Alarm Monitoring Point to be armed or disarmed based on Schedule or using an assigned reader. If an alarm is detected, this defines which Output Point(s) to trigger.

Output Setup: Triggers the Output Relay based on schedule, such as turning on lighting in an area after office hours.

Database Backup: Backs up all databases into the flash memory of the controller and downloads to the hard disk of a PC. The AEC performs an automatic backup to flash memory that the user defines.

Advance I/O Setup: Re-routes physical or logical information from one operation to another.

Panel Setup: Sets up the following parameters:

- Network Settings
- Input Point Configuration
- Set Date & Time
- Auto Logout Timer
- Audit Log
- Default Settings
- Card Format
- Company Profile
- Email/SMS Configuration

4.6 Panel Maintenance

Update Flash: Programs updates for firmware enhancement, new feature, and bug fixing when required. It can also recover databases.

Reboot Panel: Reboots the AEC before changes can take effect, such as an IP address change or a firmware upgrade.

4.7 Logout

Use **Logout** to log off from AEC.

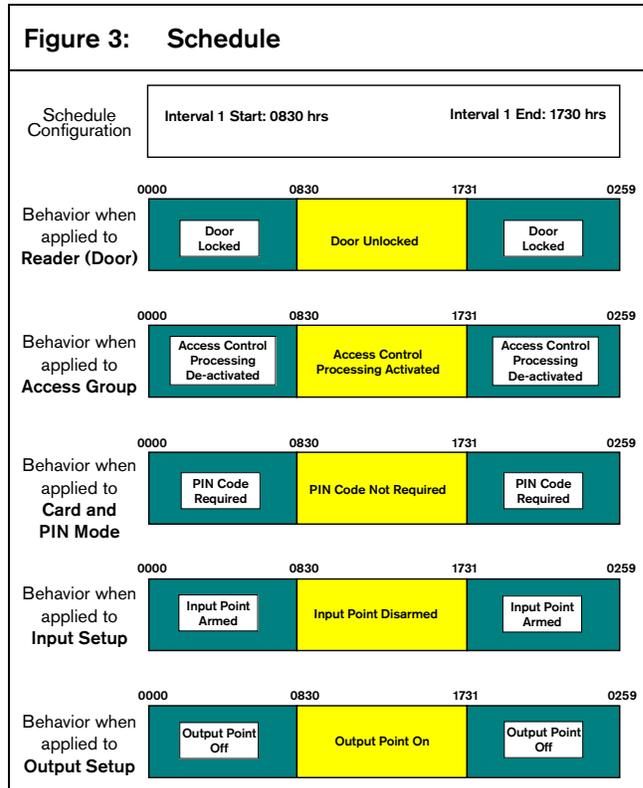
5.0 Schedules

- Allocate schedules to card readers for access groupings to specify whether cardholders can access specific readers at a specific time.
- Allocate schedules to the card readers to activate/deactivate readers or use PIN Mode at a specified time.
- Define the time interval to arm or disarm the Input Points for alarm monitoring.
- Define the time interval for triggering output points such as to trigger the lighting utility for an area.



Request your system administrator's permission before making changes or configuring new schedules.

Refer to *Figure 3* for the system when configured to a Schedule.



5.1 Defining a New Schedule

1. Click on the **Schedule** link.
2. Click **Undefined Schedule**.
3. Highlight the default text and type the new description and click .
4. Click , the day of week (DOW), **Regular Hol**, or **Special Hol** row to enable the entire row for editing.
5. Click the required field, starting from **Interval 1 – Start**, and type the appropriate time in a 24-hour, 4-digit format.
6. Repeat *Step 5* for all applicable entries.
7. If the operation period is the same Monday to Friday, click the check boxes to duplicate the current setting to other **DOW**. De-select **DOW** by clicking on it again.
8. Click .

6.0 Holidays

Set holiday parameters only if the system's operation is required to exhibit a different behavior during the holidays. Samples of how the parameters affect system operation behavior are:

- The controller unlocks a specific door during working hours but during a holiday, the door remains locked the entire day.
- A cardholder has access to certain areas during working hours but during a holiday, the cardholder is not allowed access.



Set the Special Holiday parameters on the eve of a holiday.

Holiday menu items are categorized as Regular Holiday dates or Special Holiday dates. There is no difference in the operational behaviors of either type.

6.1 Defining Holiday Date

1. Click the **Holidays** link.
2. Select the appropriate holiday, **Regular** or **Special**.
3. Click the next **Undefined Holiday**.
4. Highlight the default text and type the new holiday description. Then select the holiday date.
5. If the holiday date is the same year after year, select **No** when prompted by Include year in processing?.
6. Click .

7.0 Access Groups

An access group defines a list of readers within certain authorized times the cardholders can access.

Cardholders within this access group can access those readers only within this Schedule.

7.1 Defining Access Group

1. Click the **Access Groups** link.
2. Select the next **Undefined Access Group** number. The system administrator predetermines the description of the readers in use.
3. Highlight the default text and type the new access group description.
4. Click the appropriate check boxes to indicate a tick (✓) mark for readers) assigned to this access group.
5. Select the appropriate schedule for each reader.
6. After completing the settings for the first eight readers, set the next e readers, if required, by clicking .
7. Repeat *Steps 4* and *5*.
8. Click .

8.0 Card Assignment

8.1 Adding Range of Card Number

1. Click  to open the Batch Cards screen.
2. At the **Card #** field, type the desired card number. The number you specify is the starting number of the batch card operation.
3. The number in **Facility code:** is configured in **Panel Setup→Default Settings**. Change the code if it is different from the default. Refer to **Default Settings** for details.
Type “0” if the card format does not support the Facility Code.
4. From the **Card Format:** list, select the appropriate card format. The card format is configured in **Panel Setup→Card Format**. Refer to **Card Format** for details.
5. At **Number of Cards:** type the card number and click .
The message “Cards added successfully” appears.
6. Click  to return to the first page of menu items.
7. Edit the new card number parameters.

8.2 Adding Range of Card Numbers with Same Data Entries

This function adds a range of card numbers with data entries copied from a reference card number. All card numbers added are copied with the data and parameters of the reference card except the Facility Code, Card Format, and Username that relate to the individual card and cardholder.

 The reference card number you enter must be the exact card number, facility code, and card format for the process to complete. The AEC prompts you with an error message if a non-existent reference card number is specified.

Save time when assigning a range of card numbers to a specified department staff by assigning cards with numbers ranging from 19001 to 19100, such as the Production Department staff.

 Card number 18020 is an ADC Proprietary Card Format with a facility code of 0. It is used as a reference to set similar parameters for new card numbers such as Access Group.

This range of card numbers uses Facility Code 0, an ADC Proprietary Card Format. To use card number 18020 from the Production Department as the reference for the new card range setting:

1. Click  to open the Batch Cards screen.
2. Click .
3. Edit the newly added card number parameters by clicking on the desired card number link. Follow *Steps 2 to 13 in Section 8.3 Adding Card Number to Database* on page 18 to edit card number parameters.

8.3 Adding Card Number to Database

1. Click the [Card Assignment](#) link.
2. Click  and type a card number at **Card #:**. This is a required field. Not placing information in this field returns an error message.
3. Leave **Facility code:** as is. Your system administrator predetermines facility codes.
4. Select a format from the pull-down menu in **Card Format:**. Your system administrator predetermines card formats.
5. At **User Name:**, type the cardholder's name.
6. At **Department:**, type cardholder's department.
7. Type the appropriate entry in the following two fields. Your system administrator predetermines the descriptions of the fields.
8. Select the appropriate Access Group from the pull-down menu. The Access Group is a combination of assigned card readers and schedules that define when and where a person has access. Up to two Access Groups are assigned to each cardholder. Your system administrator predetermines the descriptions of the access fields.
9. Click  to continue.
10. **Card Functionality** defines how and when the cardholder uses his/her card.
 - Cardholders can arm or disarm an Alarm Zone using a dedicated card reader.
 - Cardholder must abide by holiday schedules. Access to the reader is determined by holiday schedules.
 - Allow exit reader usage only according to time schedules. The cardholder can exit as determined by the time schedules.
 - The cardholder can enable card enrollment operation. This allows selected cardholders to use their card to activate a reader into the Enrollment Mode.
 - Disable card from all access permanently. When this mode is selected, the user card is immediately denied access from the system. This feature prevents illegal access to the system if you lose or misplace the card.
 - Cardholder with one time access only allows the administrator to assign the cardholder a one-time access to the system. After a one-time use, the cardholder's access is invalid. To regain access, the cardholder must request the administrator to reactivate the one-time access right.

- Ensure **Valid** is selected for Access Status. After the card is used for one-time access, Access Status is automatically updated to Expired.
 - **Card + PIN** is required on keypad readers. This is the card plus PIN Mode.
11. If required, highlight **default user PIN** (1234000) and type a new PIN code (1 to 7 digits).
 12. Use **Card Validation Dates** to define when the card is valid and/or when it expires. Check the appropriate box before selecting the date.
 13. Select **Dual Card presentation sequence** and choose whether the card is a First Card or Second Card. If no sequence is required, select **Don't Care**.
 14. Select **Dual Card Group ID** from the list.
 15. Click  to save the card parameters.

8.4 Enrolling Card with an Unknown Wiegand Format

To use any unknown proprietary Wiegand card format, the system administrator activates a reader either by pre-assigned enrollment card or through the web. He/she selects Enrollment Mode and enrolls any card in the card database with a maximum bit length of 64:

8.4.1 Enrolling Card Using Web Page

1. At the Card Database screen, select **Card Assignment** and click  at the top-right corner.
2. Click [Go to Cards Enrollment](#).
3. Select a reader for the enrollment reader and click  to activate it.
4. Present the card with the unknown Wiegand Format to the enrollment reader.

The card you presented appears in the box for the list of scanned cards.

The administrator can now assign a card number and name to the card.



Assign a number to the card of unknown Wiegand format beforehand. Place a label on the card to reference the card number during the card enrollment process.

5. Highlight the card in the list of scanned cards the card number and name is assigned to.
6. Click  to add the card with the assigned card number and name to the database.

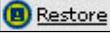
9.0 View Activity

Use the View Activity feature to view activity transactions. The transactions are shown in Real-Time Mode according to the date and time of the transaction occurred. Click the appropriate link to view the following transactions:

- Alarm Transactions
- Restore and Alarm Transactions
- Valid and Alarm Transactions,
- Time Attendance
- All Transactions

When any Alarm Activity transaction is executed, an alert tone is sent to the monitoring computer’s audio system.

Refer to *Table 1* for the web page icons.

Icon	Description
	Alarm transactions only
	Valid and alarm transactions.
	Restore and alarm transactions
	All transactions
	Only time clocking transactions.
	Acknowledges alarm transactions and silences audible tones on the CMC.
	Updates web page for the latest transactions.
	Print preview of cardholders who are in the specific APB Zones at the time of the preview.
	Print preview of the Activity Report before printing.
	Located on the left side of the status bar, this icon shows the current AEC time and date.

- All new transactions have a yellow background.
- All alarm transactions have red text; other transactions have black text.
- After a page refreshes, the yellow background becomes grey except for alarm transactions. These remain unless you active the . The following is a sample of the View Activity screen.

The following screen is a sample View Activity screen. Refer to *Table 2* for a description of the screen columns.



Column	Description
No. 6	New Clock Out - Time Attendance transaction
No. 5	New Restore transaction (black text; yellow background)
No. 4	Valid transaction
No. 3	Not acknowledge Alarm transaction (red text, yellow background).
No. 2	Valid transaction
No. 1	Restore transaction
No. 0	Acknowledged Alarm transaction (red text; grey background)

10.0 Manual Control (Door)

The screenshot shows the 'Manual Control (Door)' interface. At the top, there's a 'Manual Control' header and a 'Door Control' sub-header. Below these are four buttons: 'Input Control', 'Output Control', 'Reset APB', and 'View Activity'. The main content is a table with the following columns: 'Door #', 'Description', 'Current Status', and 'Manual Actions'.

Door #	Description	Current Status	Manual Actions
1	Reader 1	Unlocked - Closed	<input checked="" type="radio"/> No Change <input type="radio"/> Lock <input type="radio"/> Momentarily Unlock
2	Reader 2	Locked - Closed	<input checked="" type="radio"/> No Change <input type="radio"/> Unlock <input type="radio"/> Momentarily Unlock
3	Reader 3	Locked - Closed	<input checked="" type="radio"/> No Change <input type="radio"/> Unlock <input type="radio"/> Momentarily Unlock
4	Reader 4	Locked - Closed	<input checked="" type="radio"/> No Change <input type="radio"/> Lock <input type="radio"/> Momentarily Unlock
5	Reader 5	Unlocked - Closed	<input checked="" type="radio"/> No Change <input type="radio"/> Lock <input type="radio"/> Momentarily Unlock
6	Reader 6	Unlocked - Closed	<input checked="" type="radio"/> No Change <input type="radio"/> Lock <input type="radio"/> Momentarily Unlock
7	Reader 7	Unlocked - Closed	<input checked="" type="radio"/> No Change <input type="radio"/> Lock <input type="radio"/> Momentarily Unlock
8	Reader 8	Unlocked - Closed	<input checked="" type="radio"/> No Change <input type="radio"/> Lock <input type="radio"/> Momentarily Unlock
9	Reader 9	Unlocked - Closed	<input checked="" type="radio"/> No Change <input type="radio"/> Lock <input type="radio"/> Momentarily Unlock
10	Reader 10	Unlocked - Closed	<input checked="" type="radio"/> No Change <input type="radio"/> Lock <input type="radio"/> Momentarily Unlock
11	Reader 11	Unlocked - Closed	<input checked="" type="radio"/> No Change <input type="radio"/> Lock <input type="radio"/> Momentarily Unlock
12	Reader 12	Unlocked - Closed	<input checked="" type="radio"/> No Change <input type="radio"/> Lock <input type="radio"/> Momentarily Unlock
13	Reader 13	Unlocked - Closed	<input checked="" type="radio"/> No Change <input type="radio"/> Lock <input type="radio"/> Momentarily Unlock
14	Reader 14	Unlocked - Closed	<input checked="" type="radio"/> No Change <input type="radio"/> Lock <input type="radio"/> Momentarily Unlock
15	Reader 15	Unlocked - Closed	<input checked="" type="radio"/> No Change <input type="radio"/> Lock <input type="radio"/> Momentarily Unlock
16	Reader 16	Unlocked - Closed	<input checked="" type="radio"/> No Change <input type="radio"/> Lock <input type="radio"/> Momentarily Unlock

At the bottom of the table, there are two icons: a document with a hand cursor and a blue 'X' icon. Below the table, there is a disclaimer: 'This product is patent protected, view patent list. Robert Bosch GmbH reserves all rights even in the event of industrial property rights. We reserve all rights of disposal such as copying and passing on to third parties.'

Manual Control (Door) checks the status of all the doors and sends a command to either momentarily or permanently unlock the door without being at the door location.

When you manually control this operation, you supersede control of the system. When the system encounters a valid schedule interval, it takes over and resumes normal operation

10.1 Controlling Doors

1. Select the desired action radio button(s). Your system administrator predetermines the reader's description.

2. Click  or  to send the command. (Only select the door you want to send commands to.)

The screen refreshes to reflect the new status. The current status of the door for a Momentary Unlocked command does not show the true status after the Door Strike Timer elapsed, unless you refresh the screen by

clicking .

11.0 Manual Control (Input)

Manual Control (Input) checks the status of all the input points in a predetermined alarm zone and sends a command to arm or disarm the zone manually.

When you manually control this operation, you supersede control over the system. When it encounters a valid schedule interval, the system takes over and resumes normal operation.

11.1 Controlling Alarm Zone Input Points

1. Click  or  to view the desired alarm zone.

Your system administrator predetermines and groups the input points with their respective alarm zones. The status of the selected zone and either



or  appears.

2. Click  or  to toggle the status.
The web page refreshes to reflect the new status.

11.2 Controlling Individual Input Points

1. Click on the input control link to view input status.
2. Observe the status of all inputs not grouped to an alarm zones.
3. Select Arm Now or Disarm Now and click  to arm or disarm.

12.0 Manual Control (Output)

Manual Control (Output) checks the status of all the output points and sends a command to turn them on or off. If the output point is linked to an input point as an alarm output, the status will not be indicated.

When you manually control this operation, you supersede control over the system. When the system encounters a valid schedule interval, it takes over and resumes normal operation.

12.1 Controlling Output Points

1. Click  or  to view the range of output points.
2. Select the desired radio button(s). Your system administrator predetermines the output point's description.
3. Click  or  to send the command.
Only select the output point(s) you want to send commands to.

The screen refreshes to reflect the new status.

The current status of the output point for a Duration On or Duration Off command does not show the true status after the duration elapses unless you refresh the screen.

13.0 Reset APB

Reset APB resets the anti-passback (APB) feature once it is violated. This feature is only applicable to **Full APB** and **Soft APB**.

Use **Full APB** to reset the violation and allow violators to access or exit the controlled door.

Use **Soft APB** to stop logging Activity transactions such as Access Granted, Soft APB and Exit Granted, Soft APB for a violator's subsequent access or exit respectively.

Reset the APB violation by:

- card number regarding Reader/All Readers
- name with regarding Reader/All Readers
- all card numbers regarding Reader/All Readers

13.1 Resetting APB Based on Card Number Regarding Reader/All Readers

Reset APB based on card number by using the card number, its facility code, and its card format.

1. Click the **Reset APB** link.
2. Type the card number of the APB violator.
3. Leave **Facility Code** as is. This field is predetermined by your system administrator.
4. Select **Card Format** from the pull-down list.
5. Select the appropriate Reader or All Readers.
6. Click .
7. If the command is executed successfully, a message indicating APB reset by card number and zones with respect to reader/all readers will be displayed.

8. Click on the  button to return.

13.2 Resetting APB Based on Name Regarding Reader/All Readers

1. At **Name:**, type a character, portion, or full name and click .

If a match is found, a window with the names appears. For example, entering John and clicking  opens the following screen.

By Name	
Search:	<input type="text" value="John"/> 
Names found:	<div style="border: 1px solid gray; padding: 2px;"> John d'Baptist John </div>
Option:	<input type="text" value="Name"/> 

2. Select the appropriate name from **Names found:**. The selected name appears.
 3. Select the appropriate **Reader** or **All Readers**.
 4. Click .
- A message appears indicating the APB is reset by name and zone regarding Reader/All Readers.
5. Click .

13.3 Resetting APB by All Card Numbers Regarding Reader/All Readers

1. Select the appropriate **Reader** or **All Readers**.
 2. Click .
- A message appears indicating the APB is reset by all cards and zones regarding Reader/All Readers.
3. Click  to return.

14.0 Printing a Report

Refer to *Table 3* for the AEC reports.

Table 3: Reports	
Report	Description
View Activity	Shows the activities and events that occurred during system operation. Includes the following type: <ul style="list-style-type: none"> • Alarm • Valid • Restore • All • Time Attendance
APB Report	Lists cardholders who are in the specific APB Zone at the time of report preview.
Card Assignment	Shows details of all cards in the database.
Access Groups	Shows the access groups available to cardholders with access to specified readers during specified schedules.
Schedules	Shows the intervals definition for a different DOW for each Schedule.
Holidays (Regular or Special)	Lists holiday description and dates.
Card Readers	Gives details of all card readers in use.

1. Open the first page of menu items and click the **Report** link.
A **Selection Criteria** page opens.
2. Make your selection and click  for a report preview.
3. Select **File→Print**.

15.0 Utilities Programs

15.1 Running IP Setup

1. Start Windows and place the CD containing the Access Easy Utilities Disk in your CD ROM drive.
2. Run the Windows Explorer and click on the CD ROM drive to view the **AEMC Utility**, **IPSetup**, and **SQL Desktop Engine (MSDE2000)** folders.



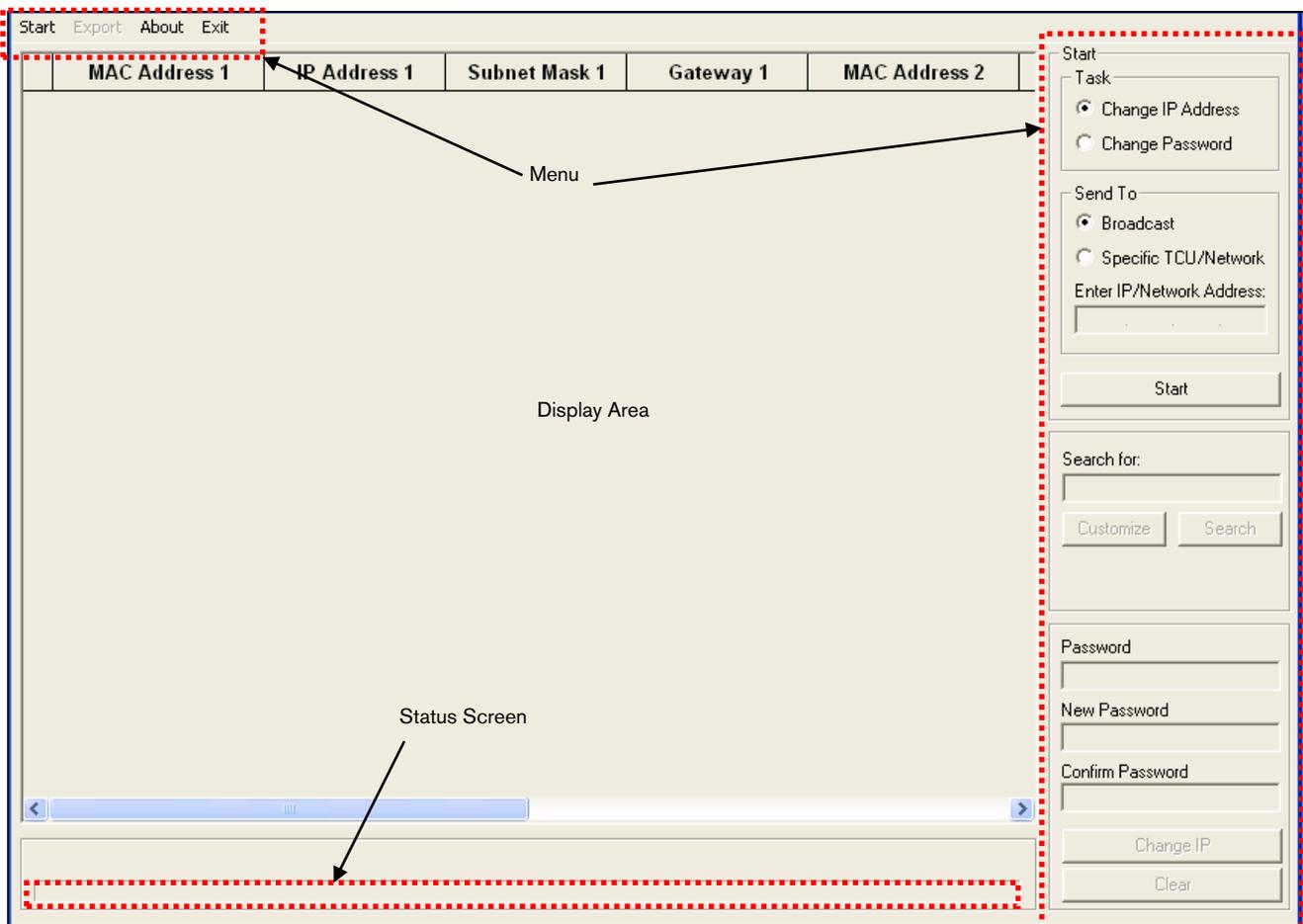
3. Double-click **IPSetup** and look for the Setup.exe file.

Alternatively, you can copy the entire **IPSetup** folder to your PC and launch the IP Setup program.



4. Double-click  to launch IP Setup.

15.2 Viewing TypeMenu Items



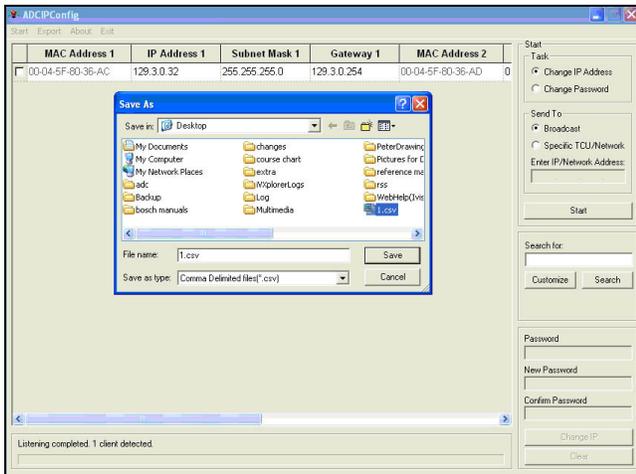
15.2.1 Start

Start allows you to begin scanning the existing controller's IP address that is available within the network.

15.2.2 Export

Export allows you to export the available controller's IP address data to a CSV file format. You can also use this option to housekeep and track controller data.

1. After scanning and editing the controllers' IP address data, select **Export** on the Main menu to open the Save As screen.



2. Click **Save** to export the selected data.

15.2.3 About

About shows the current FingerprintIP Setup software version. From the Main menu, select **About** to open the About IP Setup screen and view the current software version.

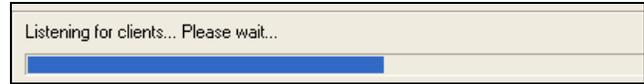


15.2.4 Exit

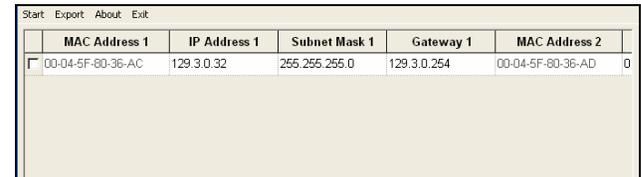
Exit logs out of the FingerprintIP Setup software.

15.3 Scanning and Changing Controller IP Address Data

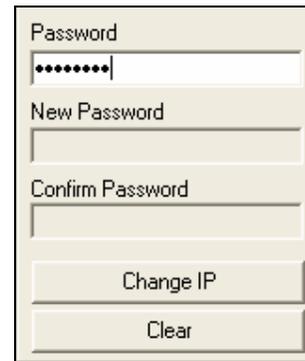
1. Select **Start** on either menu to begin scanning. The IP Setup begins scanning for controllers within the network and the following message appears.



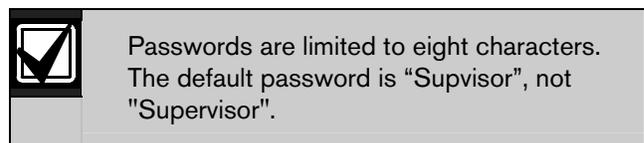
The results appear in the display area.



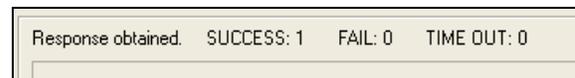
2. Check the controller's box and click **IP Address 1** or **IP Address 2**, **Subnet Mask 1** or **Subnet Mask 2**, **Gateway 1** or **Gateway 2** to change the data. In the following example, IP Address 1 was changed to 129.3.0.33.



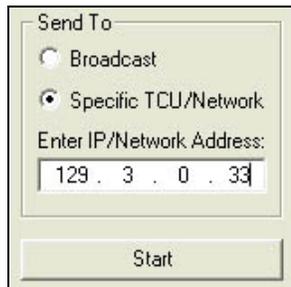
3. Type the password and click **Change IP**.

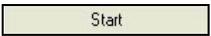


The results are reflected in the Status screen (below) to indicate success or failure.



15.4 Scanning and Changing Specific Controller IP Address Data



1. From **Send To**, select **Specific TCU/Network**.
2. Type the IP address you want to search for in **Enter IP/Network Address**. This example shows IP address 129.3.0.33.
3. Click .

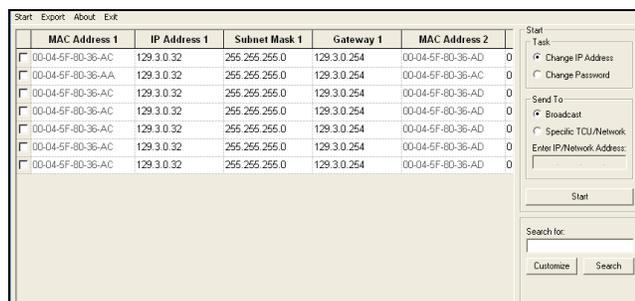
The results appear in the following display.

MAC Address 1	IP Address 1	Subnet Mask 1	Gateway 1	MAC Address 2
<input type="checkbox"/> 00-04-5F-80-36-AC	129.3.0.33	255.255.255.0	129.3.0.254	00-04-5F-80-36-AD 0

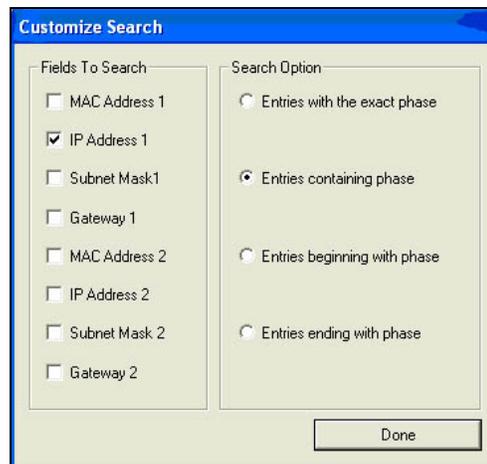
4. Follow *Steps 2 and 3 in Section 15.3 Scanning and Changing Controller IP Address Data* on page 25 to change the desired data.

15.5 Scanning and Changing Controller IP Address Database on Search Criteria

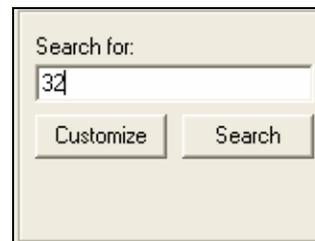
Several controllers can be detected within the network. Use the search function to narrow the range or look for a specific controller and edit the necessary data.



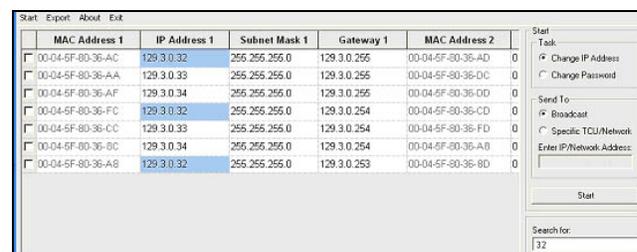
1. At **Search for**, click  to open the Customize Search dialog.



2. Select the desired parameters. In this example, **IP Address 1** in **Fields to Search** and **Entries containing phase** in **Search Option** are the search parameters.
3. Click  to open the Search for: dialog.



4. At **Search for**, type the value you want to search for and click . This example has 32 as the value.



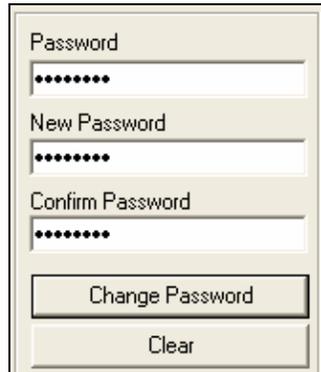
The search results are highlighted with a light-blue background and are reflected in the display.

5. Follow *Steps 2 and 3 in Section 15.3 Scanning and Changing Controller IP Address Data* on page 25 to change the desired data.

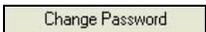
15.6 Changing the Password



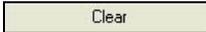
1. At the Main menu **Start→Task** field, select **Change Password** to open the password dialog.



2. Complete the **Password**, **New Password**, and **Confirm Password** fields and click



You can erase all fields by clicking



The results are reflected in the status screen to indicate success or failure.



Bosch Security Systems
130 Perinton Parkway
Fairport, NY 14450-9199
Customer Service: (800) 289-0096
Technical Support: (888) 886-6189

© 2006 Bosch Security Systems
F01U027397B



Recyclable



BOSCH