

Webpass IP Reader

WEB Configuration Manual

WEBPASS version : v0.09 Aug-24th-2009 (HW.1.0)
WEBPASS Web version : v1.4 Build date : Aug-18th-2009

Revision History

1. Newly added Event Type : “Alarm” and “IP Camera”.
2. Newly added E-Mail Alert: “Mail From” “SMTP Server” “Mail to” “Mail Carbon copy”.
3. Newly added : IP Camera “Port number” “Type”.

【INDEX】

WEB Configuration	1
WEB Log-On	1
Preparation	1
Use IE Web Browser	1
Main Configuration screen	2
Descriptions for main screen.....	2
Door status monitoring panel.....	3
Door status descriptions:.....	3
User Administration	4
Access Log.....	4
Access Log screen descriptions	4
User List.....	5
User List screen descriptions:	5
User Record modification screen descriptions.....	7
Add New User.....	8
Add New User screen descriptions	8
Terminal	10
Terminal Status.....	10
Terminal status screen description	10
Terminal Setup	11
Terminal Setup screen descriptions.....	11
Password Setup	13
Web Logon and Entrance Password setup descriptions.....	13
System Log	14
System log screen descriptions	15
Clock Setup.....	15
System Clock Setup	15
Access Control.....	17
Time Set	17
Time Set screen descriptions.....	17
Time Zone Set Up	17
Time Zone setup screen descriptions	18
Time Zone Setup screen descriptions	18
Group List	19
Group List screen descriptions.....	19
Group List screen description	20
Holiday Setup.....	20
Holiday Setup screen descriptions	20

Door Setup	21
Door Setup screen descriptions	21
Remote Control	22
Door Status /Security Pass screen descriptions	22
Event Handle	24
Event Handle screen descriptions	24
Tools	28
IP Camera	28
IP Camera screen descriptions	28
Reboot	28
Reboot screen descriptions	29
Firmware Upgrade	29
Firmware Upgrade screen description	29
RESET	29
RESET screen description:	29

Copyright @ 2009. All Rights Reserved.

Document Version: 1.0 All trademarks and trade names are the properties of their respective owners.

— WEB Configuration —

WEB Log-On

WEBPASS with HTTP built-in server is able to communicate with Web browser for administration and configurations.

Preparation

Before starting WEBPASS configuration, make sure :

- Same LAN segment has been physically configured between WEBPASS and Computer.
- Power is ON
- Default IP: 192.168.0.66. To avoid IP confliction your site, please properly set WEBPASS with the same LAN segment IP or turn off other devices until WEBPASS has been successfully configured.

Use IE Web Browser

1. Start Web Browser
2. Complete IP on URL, eg. Default IP: 192.168.0.66, the `http://192.168.0.66`

Communication failure:

No response for WEBPASS, check :

- WEBPASS Installation is correct/ LAN communication is normal/ Power is on or use ping command to test the communication with IP.
 - MS-DOS Command program:
 - Command line, for example: `C:\user\tank>ping 192.168.0.66`
If there is no response or time out, then this could be IP confliction or wrongly IP is given to PC and WEBPASS. (Check next)
- If a PC is using Public IP, then IP for this computer should be changed as between: 192.168.0.1~192.168.0.65 or 192.168.0.67~192.168.0.254 to create a physically communication with WEBPASS. Besides, Subnet Mask should be setting as 255.255.255.0 ◦
- Make sure your computer IP is in the same segment with WEBPASS

➤ Main Configuration screen

Main configuration screen will be pop-up after finished the installation between PC and WEBPASS IP Reader :

User Administration
 Access Log
 View User List
 Add User

Terminal
 Terminal Status
 Terminal Setup
 Password Setup
 System Log
 Clock Setup

Access Control
 Time Set
 Time Zone Setup
 Group List
 Holiday Setup
 Door Setup
 Remote Control
 Event Handle

Tools
 IP Camera
 Reboot
 Upgrade Firmware
 Reset

Refresh

WEBPASS Web Ver1.5
 Build Date 09/07/2009

TERMINAL STATUS

Product Name :	WEBPASS(EM)(20000)
Serial No. :	00022a(182317)
Firmware Version :	0.10.00,Sep 15 2009(HW1.0)
System Time :	09/17/2009 03:34:21
Terminal ID(MAC Address) :	91(00:0e:e3:00:02:2a)
IP Address :	192.168.3.91
Subnet mask :	255.255.255.0
Default Gateway :	192.168.3.1
Primary DNS :	168.95.1.1
Listen Port/Software IP(status) :	2000 / 0.0.0.0 (Offline)
Web Management Port :	80
Registered User :	1000
Available User Capacity:	19000
Access/System Log Count :	0/0
Control Mode :	Standalone(WG34)
Anti-Pass-Back(Tolerance Timer) :	Disabled(0)
Anti-Duress :	Disabled
Next WEBPASS(status) :	0.0.0.0(Offline)

【Main Screen】 — Article 1

Descriptions for main screen :

- Use left side selection bar for function configuration thru web browser:

User Administration	
Access Log	Switch to Access Log screen
View User List	Switch to User List screen: can be modify, delete, active or inactive users
Add New User	Switch to Add New User screen
Terminal	
Terminal Information	Switch to Terminal information screen(main screen)
Terminal Configuration	Switch to Terminal configuration screen

Password Setup	Switch to WEB Log-on and Password setup screen
System Log	Switch to System log screen
Clock Setup	Switch to system time Clock setup screen
Access Control	
Time Set	Switch to Time Set configuration screen
Time Zone	Switch to Time Zone configuration screen
Group List	Switch to Group List configuration screen
Holiday Setup	Switch to Holiday configuration screen
Door Setup	Switch to Door Setup configuration screen
Remote Control	Switch to Door Status and Security Bypass configuration screen
Even Handel	Switch to Event Handel configuration screen
Tools	
IP Camera	Switch to IP Camera configuration screen
Reboot	Switch to system Reboot screen
Upgrade Firmware	Switch to Firmware upgrade screen
Reset	Switch to Reset and Factory Default screen
Button	
Refresh	To Refresh WEB status

Door status monitoring panel

Real time monitoring status will show on the main screen panel :



Door status descriptions:

Step by Step

1. Click START key to refresh door status panel continually
2. Indicators for Door Status :
 - Green : Door Close
 - Yellow: Door Open
 - Gray: No response
 - Red: Exceptions
3. Monitoring status will be showing on this panel upon any access movements to a door:
 - User ID 、 Date 、 Time 、 Door Nr.
4. Click STOP key to stop the Refresh schedule. You may process modify, delete, save when Refresh has stopped

➤ User Administration

Access Log

Click Access Log to get into the screen :

ACCESS LOG

Query From/To (mm/dd/yyyy) 9 17 2009 -- 9 17 2009

No.	User ID	User Name	Date	Time	IN/OUT	Door	Note.
1.	58(S)		09/17/2009	03:38:34	IN(0)	1	(C)
2.	58(S)		09/17/2009	03:38:32	IN(0)	1	(C)
3.	58(S)		09/17/2009	03:38:31	IN(0)	1	(C)
4.	58(S)		09/17/2009	03:38:30	IN(0)	1	(C)
5.	58(S)		09/17/2009	03:38:27	IN(0)	1	(C)
6.	58(S)		09/17/2009	03:38:26	IN(0)	1	(C)
7.	58(S)		09/17/2009	03:38:25	IN(0)	1	(C)

Total 7 Record(s)

<< End of List... >>

【Access Log】 — Article 2

Access Log screen descriptions:

Query	
USER ID	Query by USER ID
CARD No.	Query by CARD No.
From/To (MM/DD/YY)	Query by pull down menu for DATE selection
Start(Button)	Start to query

Operation :

- Using Pull down menu to determine your query conditions.
- Press SATART to start query

Access log list description	
No.	Sequence numbers on the list
USER ID	User ID for users. Click the USER ID would direct to a screen to Modify User List (Article 4). It would be failed only USER registration information has been removed. ※ User authorized level can be 1~10, can be shown followed the ID.
USER NAME	User Names for IN/OUT access records. User name could be blank if USER NAME hasn't been filled while registration.
DATE	Date for IN/OUT records
TIME	Time for IN/OUT records

IN/OUT	IN: Access by WEBPASS OUT: Access by Wiegand Reader ※ APB level will be shown followed the IN/OUT
DOOR No.	A door no. which is installed with a WEBPASS
NOTE	Special note for access logs: Events like APB · Fire Alarm.....etc.
First Page	Direct to First page of Access Log IN/OUT information
Previous 10 Page	Move ahead to previous 10 page from current page
1 2 3...N	Direct to specific Access log IN/OUT record page
Next 10 page	Move to next 10 page from current page
Last Page	Direct to last page of the Access Log record

User List

View User List from main screen:

User LIST

Search User : By User ID By Card No. By User Name

No.	User ID	User Name	User Type	Active	*Reg Type:P(Password) , C(Card)		Bypass Level
					P	C	
<input type="checkbox"/> 1.	1		Normal		<input type="radio"/>	<input checked="" type="radio"/>	1
<input type="checkbox"/> 2.	2		Normal		<input type="radio"/>	<input checked="" type="radio"/>	1
<input type="checkbox"/> 3.	3		Normal		<input type="radio"/>	<input checked="" type="radio"/>	1
<input type="checkbox"/> 4.	4		Normal		<input type="radio"/>	<input checked="" type="radio"/>	1
<input type="checkbox"/> 5.	5		Normal		<input type="radio"/>	<input checked="" type="radio"/>	1
<input type="checkbox"/> 6.	6		Normal		<input type="radio"/>	<input checked="" type="radio"/>	1
<input type="checkbox"/> 7.	7		Normal		<input type="radio"/>	<input checked="" type="radio"/>	1
<input type="checkbox"/> 8.	8		Normal		<input type="radio"/>	<input checked="" type="radio"/>	1
<input type="checkbox"/> 9.	9		Normal		<input type="radio"/>	<input checked="" type="radio"/>	1
<input type="checkbox"/> 10.	10		Normal		<input type="radio"/>	<input checked="" type="radio"/>	1
<input type="checkbox"/> 11.	11		Normal		<input type="radio"/>	<input checked="" type="radio"/>	1
<input type="checkbox"/> 12.	12		Normal		<input type="radio"/>	<input checked="" type="radio"/>	1
<input type="checkbox"/> 13.	13		Normal		<input type="radio"/>	<input checked="" type="radio"/>	1
<input type="checkbox"/> 14.	14		Normal		<input type="radio"/>	<input checked="" type="radio"/>	1
<input type="checkbox"/> 15.	15		Normal		<input type="radio"/>	<input checked="" type="radio"/>	1
<input type="checkbox"/> 16.	16		Normal		<input type="radio"/>	<input checked="" type="radio"/>	1
<input type="checkbox"/> 17.	17		Normal		<input type="radio"/>	<input checked="" type="radio"/>	1
<input type="checkbox"/> 18.	18		Normal		<input type="radio"/>	<input checked="" type="radio"/>	1
<input type="checkbox"/> 19.	19		Normal		<input type="radio"/>	<input checked="" type="radio"/>	1
<input type="checkbox"/> 20.	20		Normal		<input type="radio"/>	<input checked="" type="radio"/>	1

Total 1000 User(s)

<< [First](#) | [Prev 10](#) | [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#) | [Next 10](#) | [End](#) >>

Activate, Deactivate or Delete SELECTED Employee

【User List】 — Article 3

User List screen descriptions:

Search for User

By User ID	Select for searching by USER ID
By Card ID	Select for searching by Card ID
By User Name	Select for searching by User Name
GO (button)	Start searching

Operation :

1. Fill User ID, Card ID or User Name for conditionally search.
2. Press "Go" button for starting search.

User Record

No.	Sequence number for User list. Ticking the box before the sequence no. to Active/ Inactive / Delete users authorization. Selection can be multiple.
USER ID	Displaying User ID, click the ID could direct to User Modification page(Article 4)
USER NAME	Displaying User name
USER TYPE	There are 4 user types: User/Administrator/Visitor/Tour Guard
ACTIVE	Green light for user authorization is being active or not
P	Green light for Password has been registered for a user
C	Green light for CARD No. for a user has been registered.
Bypass Level	Displaying user bypass level : L1~L4
First Page	Direct to first page of user list
Previous 10 Page	Direct to previous 10 page from current page
1 2 3...N	Direct to specific page
Next 10 page	Direct to next 10pages from current page
End of List	Direct to last page

Buttons

ACTIVE	Active user' s authorization
DEACTIVE	Deactive user' s authorization
DELETE	Delete user' s registered information

User RECORD

Modify User Record

User ID : (1 ~ 20000)

Card No. :

Name : (Max 31 chars.)

Expire Date Check : Disable Enable

From (Y) / (M) / (D) (H) (M)

To (Y) / (M) / (D) (H) (M)

Status : Activate Deactivate

User Type :

Group : 1. 2. 3. 4.

Bypass TZ Level :

Personal Password : (4 ~ 8 digits.)

Personal Confirm :

【Modify User Record】 — Article 4

User Record modification screen descriptions :

USER RECORD	
USER ID	1~20000 digits allowed only
CARD No.	Can be manually typed in or use Card Decoder to enroll the card no.
USER NAME	15 characters at most
Expire Date Check	Enable or Disable a user by ticking the check box
From ~ To	Date information required if expire date check is enabled Pull down selection menu for: Year/Month/Date/Hour/Minute
Status	Activate or Deactivate user by ticking the check box
USER TYPE	Select a user type for user by pull down menu, there are 4 types : Normal User/Administrator/Visitor/Patrol Tour Administrator: No restraint for APB policy Visitor: Use Expire Date Check to define and restraint visitors Patrol Tour: Door will not be opened but access logs will be stored for this type of user after flash card
GROUP	Each one user can be designated to 4 different groups. Pull down selection menu would provide all existing group names for selection. Default Group is Free Time Group
Bypass TZ Level	User Bypass Time Zone level, there are L1~L4 levels. When a user Bypass TZ Level is higher than Door's Time Zone level then Door Time Zone Level will become invalid
Personal Password	4~8 digits is required

Personal Confirm | Reconfirm Personal Password

BUTTONS

Previous	Modify previous user record
SAVE	Save the modified record
DELETE	Delete existing user record
Next	Modify next user record

Add New User

Add a new user profile.

User RECORD

Add New User

REG : **Single** **Continuous** **Amount :**

User ID : (1 ~ 20000)

Card No. :

Name : (Max 31 chars.)

Expire Date Check : **Disable** **Enable**

From 2009 (Y)/ 09 (M)/ 17 (D) 3 (H) 42 (M)

To 2009 (Y)/ 09 (M)/ 17 (D) 3 (H) 42 (M)

Status : **Activate** **Deactivate**

User Type : Normal User

Group : 1. Free Time Group 2. Free Time Group 3. Free Time Group 4. Free Time Group

Bypass TZ Level : LV1

Personal Password : (4 ~ 8 digits.)

Personal Confirm :

save

【Add New User】 — Article 5

Add New User screen descriptions :

Add New User

REG	Single: Can register one user in a time Continuous: Can register 1~20,000 users in a time by defining an actual user count to it. Support successively card no. ONLY.
USER ID	1~20,000 digits allowed only
CARD No.	Can be manually typed in or use Card Decoder to enroll the card no.
USER NAME	15 characters at most
Expire Date Check	Enable or Disable a user by ticking the check box
From ~ To	Date information required if expire date check is enabled Pull down selection menu for: Year/Month/Date/Hour/Minute

Status	Activate or Deactivate user by ticking the check box
USER TYPE	Select a user type for user by pull down menu, there are 4 types : Normal User/Administrator/Visitor/Patrol Tour Administrator: No restraint for APB policy Visitor: Use Expire Date Check to define and restraint visitors Patrol Tour: Door will not be opened but access logs will be stored for this type of user after flash card
GROUP	Each one user can be designated to 4 different groups. Pull down selection menu would provide all existing group names for selection. Default Group is Free Time Group
Bypass TZ Level	User Bypass Time Zone level, there are L1~L4 levels. When a user Bypass TZ Level is higher than Door's Time Zone level then Door Time Zone Level will become invalid
Personal Password	4~8 digits is required
Personal Confirm	Reconfirm Personal Password
Button	
SAVE	SAVE the record

➤ Terminal

Terminal Status

Showing current Terminal system and network configuration status:

TERMINAL STATUS

Product Name :	WEBPASS(EM)(20000)
Serial No. :	00022a(182317)
Firmware Version :	0.10.00, Sep 15 2009(HW1.0)
System Time :	09/17/2009 03:43:14
Terminal ID(MAC Address) :	91(00:0e:e3:00:02:2a)
IP Address :	192.168.3.91
Subnet mask :	255.255.255.0
Default Gateway :	192.168.3.1
Primary DNS :	168.95.1.1
Listen Port/Software IP(status) :	2000 / 0.0.0.0 (Offline)
Web Management Port :	80
Registered User :	1000
Available User Capacity:	19000
Access/System Log Count :	7/0
Control Mode :	Standalone(WG34)
Anti-Pass-Back(Tolerance Timer) :	Disabled(0)
Anti-Duress :	Disabled
Next WEBPASS(status) :	0.0.0.0(Offline)

【Terminal Status】 — Article 6

Terminal status screen description :

Terminal Status	
Product Name	WEBPASS model name
Serial No.	WEBPASS serial no.
Firmware version(Hardware version)	WEBPASS firmware and hardware version
System Time	WEBPASS system time
Terminal ID (MAC Address)	WEBPASS Terminal ID and MAC address
IP address	WEBPASS IP address
Subnet Mask	Subnet Mask
Default Gateway	Default Gateway IP
Primary DNS	Primary DNS IP

Listen Port/Software IP/(Status)	Software communication Port No. / Software IP/ (Status: Online or Offline)
WEB management Port	WEBPASS communication port no.
Registered User	Registered user count (0~20,000 only)
Available User Capacity	20,000 – Registered user count = Available user capacity
Access/System log count	Access and System logs total entries
Control Mode	Standalone or Reader mode
Anti-Pass-Back (Tolerance Time)	APB function status (enable or disable) and Tolerance time
Anti-Duress	Enable or Disable function
Next WEBPASS(status)	Next WEBPASS device IP address and (Status :offline or online)

Terminal Setup

TERMINAL CONFIGURATION

Terminal Setting : Terminal ID :

*IP Address : . . .

*Subnet Mask : . . .

*Gateway : . . .

*DNS Server : . . .

Listen Port : *TCP Port(Software Used) : *Software IP :

Control Mode : Standalone IN Dummy Reader OUT Dummy Reader

Web Language : ▾

Anti Pass Back : Enable Disable

Tolerance Timer (Minute, Maximum 65535, 0 means No Tolerance)

Anti Duressed : Enable Disable

Password (Max 3 digits,default is 9)

WEB Management Port: Http Port:

Next WEBPASS(for APB): IP Address : . . .

Terminal may need to restart after configuration saved.

SAVE

【Terminal Configuration】 – Article 7

Terminal Setup screen descriptions:

Terminal Configurations	
Terminal ID	Default ID =1, max at 65535 (Terminal ID shouldn't be duplicated)
IP address	IP for WEBPASS
Subnet Mask	Subnet Mask
Default Gateway	Default Gateway IP

DNS Server IP	DNS Server IP address. Default ID is: 168.95.1.1
Listen Port	
TCP Port(Software used)	Port no. for Webpass and Software communication. Default is: 2000
Software IP	Software IP that communicates with WEBPASS. Default is: 0.0.0.0
Control mode	
Standalone	WEBPASS will be working as Standalone mode
Reader	WEBPASS will be working as Reader mode: Webpass should be connecting with SEMAC under Reader Mode
Web Language	
English	Select English language for Web management language
Chs	Select Chs language for Web management language (Chinese: GB)
Others	Select Others for Web management language (Chinese: BIG-5, Taiwan) and other languages supported
Anti Pass Back (APB)	
Enable	Enable APB function
Disable	Disable APB function
Tolerance Time	Recovery time for back to normal APB standby status after APB event has been triggered. Minimum scale is: Minute. Maximum is 65535. 0 = No Tolerance Time gave, required to remove APB alarm manually
Anti Duress	
Enable	Enable Anti Duress function
Disable	Disable Anti Duress function
Password	Password for Anti-Duress situation. Default = 9 or 3 digits allowed at most
WEB Management Port	
HTTP Port	WEB Port no. for Webpass. Default =80
Next WEBPASS for APB (anti pass back)	
IP address for APB	IP address for next WEBPASS IP Reader. This only supports multiple WEBPASS IP Readers have been connected. APB signal will be updated from one to other WEBPASS based on IP configured
Button	
Save	Save Terminal Information

Password Setup

WEB Logon Setting

Administrator WEB Logon User Name :	<input type="text" value="admin"/>	(47 Char. Max)
Administrator WEB Logon Password :	<input type="password" value="•••••"/>	(35 Char. Max)
Operator WEB Logon User Name :	<input type="text" value="user"/>	(47 Char. Max)
Operator WEB Logon Password :	<input type="password" value="••••"/>	(35 Char. Max)
USER WEB Logon User Name :	<input type="text" value="user0"/>	(47 Char. Max)
USER WEB Logon Password :	<input type="password" value="•••••"/>	(35 Char. Max)

Entrance Password

Common Password :	<input type="text" value="1234"/>	(4 ~ 8 digits.)
-------------------	-----------------------------------	-----------------

【Web Logon Setting /Entrance Password】 — Article 8

Web Logon and Entrance Password setup descriptions :

Web Logon Setting	
Administrator WEB Logon User Name	Administrator logon name for Web management. 47 characters at max. Default is: admin
Administrator WEB Logon Password	Administrator logon password. 35 digits at max. Default is: admin
Operator WEB Logon User Name	Operator logon name for Web management 47 characters at max. Default is: user
Operator WEB Logon Password	Operator logon password for Web management 35 digits at max. Default is: user
User WEB Logon User Name	User logon name for Web management 47 characters at max. Default is: user0
User WEB Logon Password	User logon password for Web management 35 digits at max. Default is: user0

For Administrator, Operator, User authorizations for access Web management site , has shown below Reference Table.

Button	
SAVE	SAVE the information

Entrance Password

Common Password

Can be using only if Common Password has been configured on a Door open Time Zone. Default is:1234

Button

SAVE

Save the information

Web Logon Authorization Reference table: ● for Permission granted

Web function	Administrator	Operator	User
Upgrade Firmware	●		
Password Setup	●		
Terminal Setup	●		
Door Setup	●		
Event Handle	●		
Reboot	●		
Clock Setup	●		
Reset	●		
Upgrade Firmware	●		
Password Setup	●		
Terminal Setup	●		
User Data	●	●	
Time Set	●	●	
Time Zone Setup	●	●	
Group List	●	●	
Holiday Setup	●	●	
Lift Setup	●	●	
Multi Badge Group	●	●	
Remote Control	●	●	
Access Log	●	●	●
View User List	●	●	●
Terminal Status	●	●	●
System Log	●	●	●
IP Camera	●	●	●

System Log

System Log

No.	Date	Time	Description
1.	09/17/2009	04:00:01	System Warm Start
2.	09/17/2009	04:00:00	Reboot System from Web
3.	09/17/2009	03:47:05	System Warm Start
4.	09/17/2009	03:47:03	Reboot System from Web

Total 4 Record(s)

<< End of List... >>

【System Log】 — Article 9

System log screen descriptions :

System Log

No.	Sequence no. for logs
Date	Log data
Time	Log time
Description	System log content

※ System log capacity is 1536 entries only, could be overview not providing data transfer.

Clock Setup

SYSTEM CLOCK SETUP

Time Server : Disable Enable

Recommend: time.windows.com or time.nist.gov

Time Zone:

New Date : (mm/dd/yyyy)

New Time : (hh:mm:ss)

【Clock Setup】 — Article 10

System Clock Setup :

Time Server

Disable	Network Time Server will be disconnected
Enable	Network Time Server will be connected. IP or URL for this Time Server is required to be filled and a properly Time Zone should be selected
Time Zone	Default is (GMT-England)

Save	Save the configuration
Date	Date information for current connection PC. Acceptable for manually input a Date for date adjustment. Date format is:MM/DD/YYYY
Time	Time for current connection PC. Acceptable for manually input a Time for time adjustment. Time format is: HH/MM/SS
SAVE	Save information to proceed to Date/Time adjustment for connected PC

➤ Access Control

Time Set

Time Set

Time Set List :

000	00:00 ~ 00:00		001	00:00 ~ 23:59	
002	08:30~17:30	DELETE			

Time Set : From H : M To H : M

【TIME SET】 — Article 11

Time Set screen descriptions :

Time Set list	
Time Set List	Displaying all configured Time Sets. System Default Time Sets are: 00:00~00:00 and 00:00~23:59
Time Set	Select Time Set by a pull-down menu. There will be 255 time sets can be of services. System built-in time sets is 000 and 001
From ~ To	Give a Time Set with a time period. For example: Set 8:00AM to 5:00PM for Time Set 002, we should give : From 08 : 00 To 17 : 00 ... and so on
Button	
Delete	Remove a Time Set
Set	Set a new Time Set

Time Zone Set Up

Time Zone List

Time Zone List :

000	Deactivate		001	Any Time	
002	2	DELETE			

Time Zone ID :

【TIME ZONE】 — Article 12

Time Zone setup screen descriptions :

Time Zone	
Time Zone List	Displaying all existing Time Zones. Each Time Zone information can be checked by clicking by each one
Time Zone number	Select Time Zone by a pull-down menu. There will be 120 time zones can be of services. System built-in time sets is 000 and 001
Time Zone Name	Time Zone can be modification by clicking in each Time Zone
Buttons	
Delete	Delete a Time Zone
Time Zone information	Displaying the main Time Zone configuration screen

Below Time Zone information screen is showing the Weekday (including weekend) or Holiday that allowing users to be accessible for doors:

Time Zone Information -- 002

Day : Monday ▼

Time 1: 001 -- 00:00 ~ 23:59 ▼	Time 2: 000 -- 00:00 ~ 00:00 ▼	Time 3: 000 -- 00:00 ~ 00:00 ▼	Time 4: 000 -- 00:00 ~ 00:00 ▼
Time 5: 000 -- 00:00 ~ 00:00 ▼	Time 6: 000 -- 00:00 ~ 00:00 ▼	Time 7: 000 -- 00:00 ~ 00:00 ▼	Time 8: 000 -- 00:00 ~ 00:00 ▼
Time 9: 000 -- 00:00 ~ 00:00 ▼	Time 10: 000 -- 00:00 ~ 00:00 ▼	Time 11: 000 -- 00:00 ~ 00:00 ▼	Time 12: 000 -- 00:00 ~ 00:00 ▼
Time 13: 000 -- 00:00 ~ 00:00 ▼	Time 14: 000 -- 00:00 ~ 00:00 ▼	Time 15: 000 -- 00:00 ~ 00:00 ▼	Time 16: 000 -- 00:00 ~ 00:00 ▼

	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday	Holiday
Time 1:	001 -- 00:00 ~ 23:59	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00
Time 2:	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00
Time 3:	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00
Time 4:	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00
Time 5:	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00
Time 6:	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00
Time 7:	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00
Time 8:	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00
Time 9:	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00
Time 10:	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00
Time 11:	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00
Time 12:	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00
Time 13:	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00
Time 14:	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00
Time 15:	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00

【Time Zone information】 — Article 13

Time Zone Setup screen descriptions:

Time Zone Information	
Day (weekday)	Select and configure Monday to Sunday and Holiday then select proper Time zones to each day

Time 1~Time 16	There are 16 Time Sets can be selected to each weekday (Monday to Sunday and Holiday) but Time Set option should be pre-configure by Time Set page, or there are two default time sets can be option.
-----------------------	---

Buttons

Save	Save Time Zone information
Cancel	Cancel or Modify Time Zone information

Select specific Time Zone from Time Zone List will direct to a Time Set information screen to display all pre-configured Time Zone and Time Set list

Group List

Group List

Group List :

000	Disallowed Group		001	Free Time Group	
002	2	DELETE			

Group ID : 003

【Group List】 – Article 14

Group List screen descriptions :

Group List

Group List	Display all pre-configured Groups. By clicking Group Name from the list will direct to Group List screen
Group ID	System Default group ID is: 000 and 001. Pull Down menu will list all Group ID for option. There are 255 groups can be option.

Buttons

Delete	Delete a group
Set	Set to get into Group Configuration screen

To configure a door (allowed door) with a specific Time Zone that allowed to be access, below is an example :

Group Information

Allowed Door :

1.

Time Zone ID :

001 Any Time

【Group Information】 – Article 15

Group List screen description:

Allowed Door	
Door Nr.	Tick a door nr. box to determine a group user can be access to a door within a specific Time Zone
Time Zone ID	Select Time Zone ID from the pull down Time Zone list
Buttons	
Save	Save Group information
Cancel	Cancel or Modify Group information

Holiday Setup

Holiday setup

01 Month / 01 Date

Holiday List :

01 / 01

【Holiday Setup】 — Article 16

Holiday Setup screen descriptions:

Holiday Setup	
Month	Select a holiday Month from pull down selection menu
Date	Select a Date from pull down selection menu
Buttons	
Set	Add a new Holiday
Delete	Remove a holiday

Door Setup

Door Setting

L4 Card+Personal Password Time Zone : Deactivate

L3 Common Password Time Zone : Deactivate

L2 Card Only Time Zone : Deactivate

L1 Card or Common Password Time Zone : Any Time

Lock Release Time Zone : Deactivate First Card

Exit Button TZ : Any Time

Anti Pass Back Level : IN : OUT : (0 - 255)

Lock Release Time : Sec (1 - 65535, 10 = default)

Door Open Delay Time : Sec default

Access Log :

【Door Setting】 — Article 17

Door Setup screen descriptions:

Door Setting

<p>Card + Personal Password Time Zone (L4)</p>	<p>Setting a door open time zone level as Card+Personal Password (default: None). User should use both Card and Personal Password to access a door but no restraint for identifying card card Identification can be process by Card then Password or Password then Card.</p> <p>※ When user Bypass security level is L4 then this user can access a door by Card only without Password if door security time zone has been set as lower level L1~L3 or equal to L4.</p> <p>※ If a door setting is activated as Lock Release Time Zone then this door can be accessible directly without C+P limit</p>
<p>Common Password Time Zone (L3)</p>	<p>Door setting is Common Password (default is None), user should access a door with Common Password.</p> <p>※ When user Bypass security level is L3~L4, user can use card to access a door.</p> <p>※ I If a door setting is activated as Lock Release Time Zone then this door can be accessible directly without this limit</p>
<p>Card Only Time Zone (L2)</p>	<p>Door setting is Card only (default is None),user should access a door with Card</p> <p>※ When user Bypass Security Level is L2 ~ L4, user should access door with Card</p> <p>※ If a door setting is activated as Lock Release Time Zone then this door can be accessible directly without limit</p>

Card or Common Password Time Zone (L1)	Door setting is Card or Common Password (default is Anytime), user should access door with Card or Common Password ※When user Bypass Security Level is L1 ~ L4, user may access a door by Card only If a door setting is activated as Lock Release Time Zone then this door can be accessible directly without C+P limit
Lock Release Time Zone	Door setting can be Lock Release Time Zone (default is None), users could access a door freely without any security check. If Primary Card is required to release a door at first then user could use any registered card to activate this Lock Release Time Zone level to a door.
Exit Button Time Zone	Door setting can be Exit Button , support OUT from a door only (default is Anytime)
APB Level : IN/OUT	APB level 0~255 for door IN/OUT
Lock Release Time	Door setting for lock release time. Default is 10sec
Door Open Delay Time	Door open delay time. Default is 10sec
Access Log	Ignore or Keep Access log. Default is “Keep record”

Remote Control

Remotely control Door Status Monitoring and Bypass Security Level:

Door Status Monitoring

No Response
 close
 open
 Circuit short,Circuit open,Intrude,Open too long

Door	
Door State	<input checked="" type="radio"/>
BF50 Status	X
Fire Alarm Detection	on

Security Bypass

State
Normal

Pulse Open Door
Force Close
Back To Normal
Force Open

Fire Alarm Detection ON
Fire Alarm Detection OFF

Alarm OFF

【Door Status Monitoring】 — Article 18

Door Status /Security Pass screen descriptions :

Door Status Monitoring

Door Status	<p>Displaying doors real time status:</p> <p>LED off: No response</p> <p>Green : Door Close</p> <p>Yellow : Door open</p> <p>Red: Exception (eg. Circuit short 、Circuit Open 、Intruder 、Door open too long …etc)</p>
Fire Alarm Detection	Displaying Fire Alarm detection is ON or OFF
Security Bypass	
Status	<p>Displaying door' s bypass security status:</p> <p>Normal/Force Open/Force Close</p>
Pulse Open Door	Click Pulse Open door to remotely open a door. Function only works under Bypass Security is Normal.
Force Close	Click Force Close to close a door remotely. Door status will be displaying “Force Close” , users cannot access the door by Card
Back to Normal	Door Bypass security will be back to normal after clicking Back To Normal
Force Open	Click Force Open to remotely Open a door. Door Status will be displaying “Force Open” , door lock will be released under this status until Back To Normal is set
Fire Alarm Detection ON	Function ON when Fire Alarm Detection is ON. Door status will be displaying ON.
Fire Alarm Detection OFF	Function OFF when Fire Alarm Detection is OFF. Door status will be displaying OFF.
Alarm OFF	Click Alarm OFF to put off all triggered alarms

Event Handle

Event Handle

Event Type	
Unregistered User	Latched time : 0 <small>(sec,Max 65535 : 0 means unlimited)</small> Level : 0
Alarm Trigger Level :	5
Alarm :	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
IP Camera :	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
E-mail Alerts	
Location :	<input type="text"/> (max59)
SMTP Mail Server :	<input type="text"/> (max47)
Mail from :	<input type="text"/> (max47)
SMTP Server Requires Authentication :	<input type="text"/> No <input type="text"/> username : <input type="text"/> (max45) <input type="text"/> password : <input type="text"/> (max29)
Mail To :	<input type="text"/> (max47)
Mail Cc :	<input type="text"/> (max47)
<input type="button" value="Set"/>	

Event	Latched Time	Level
Unregistered User	0	0
Deactivated User	0	0
Not Allowed Door	0	0
N/A	0	0
Time Zone Violation	0	0
Expired User	0	0
Anti Pass Back Violation	0	0
Door open too long	0	0
N/A	0	0
Tamper Switch Breakdown	0	0
N/A	0	0
Door Intruded	0	4
Duress Alarm On	0	4
Fire Alarm On	0	5

【Event Handle】 — Article 19

Event Handle screen descriptions :

Event Type

Unregistered User	<ol style="list-style-type: none"> Selected an event type : Unregistered User by pull down menu. This case, when an unregistered user passed a door, an unregistered record will be recorded, and if a selected Event Type level is higher than Alarm Trigger Level, Relay will be triggered then sent an E-mail to all addresses which have been pre-configured this page. If Latched Time=0, then you have to go back to Door Setting monitoring page to click "<u>Alarm Off</u>" to put off the alarm trigger status
Inactive User	<ol style="list-style-type: none"> Selected an event type as Inactive User: When Card has been inactivated for one user, there' ll be an Inactive User record to be recorded to Access log. If a selected Event Type level is higher than Alarm Trigger Level, Relay will be triggered then sent an E-mail to all addresses which have been pre-configured this page. If Latched Time=0, then you have to go back to Door Setting monitoring page to click "<u>Alarm Off</u>" to put off the alarm trigger status. Default= 0

<p>Not Allowed Door</p>	<ol style="list-style-type: none"> 1. Select an event type as Not Allowed Door: If a Group setting for an user is not matched, a Not Allowed Door record will be recorded to Access log list. If a selected Event Type level is higher than Alarm Trigger Level, Relay will be triggered then sent an E-mail to all addresses which have been pre-configured this page. 2. If Latched Time=0 ,then you have to go back to Door Setting monitoring page to click “Alarm Off” to put off the alarm trigger status. Default= 0
<p>Time Zone Violation</p>	<ol style="list-style-type: none"> 1. Select an event type as Not Allowed Door: When Group Time Zone for user is not matched to Time Zone for Doors. A Time Zone Violation record will be recorded to Access Log. If a selected Event Type level is higher than Alarm Trigger Level, Relay will be triggered then sent an E-mail to all addresses which have been pre-configured this page. 2. If Latched Time=0 ,then you have to go back to Door Setting monitoring page to click “Alarm Off” to put off the alarm trigger status. Default= 0
<p>Expired User</p>	<ol style="list-style-type: none"> 1. Select an event type as Not Allowed Door: If validation for a user has been expired, a Expired User record will be log to Access Log record. If a selected Event Type level is higher than Alarm Trigger Level, Relay will be triggered then sent an E-mail to all addresses which have been pre-configured this page. 2. If Latched Time=0 ,then you have to go back to Door Setting monitoring page to click “Alarm Off” to put off the alarm trigger status. Default= 0
<p>APB Violation</p>	<ol style="list-style-type: none"> 1. Select an event type as APB Violation : If Door APB level has been granted, when user use card and APB level has a confliction to the door, APB Violation record will be log to access log list. If a selected Event Type level is higher than Alarm Trigger Level, Relay will be triggered then sent an E-mail to all addresses which have been pre-configured this page. 2. If Latched Time=0 ,then you have to go back to Door Setting monitoring page to click “Alarm Off” to put off the alarm trigger status. Default= 0
<p>Door Open too long</p>	<ol style="list-style-type: none"> 1. Select an event type as Door Open too long : If door open time has exceeded to configured time after flashed card, a Door Open Too Long record will be recorded. If a selected Event Type level is higher than Alarm Trigger Level, Relay will be triggered then sent an E-mail to all addresses which have been pre-configured this page. 2. If Latched Time=0 ,then you have to go back to Door Setting monitoring page to click “Alarm Off” to put off the alarm trigger status. Default= 0

Tamper Switch open	<ol style="list-style-type: none"> 1. Select an event type as Tamper Switch triggered : If terminal (webpass) has been enforced to be opened, a record for Tamper Switch open will be recorded. If a selected Event Type level is higher than Alarm Trigger Level, Relay will be triggered then sent an E-mail to all addresses which have been pre-configured this page. 2. If Latched Time=0 ,then you have to go back to Door Setting monitoring page to click “Alarm Off” to put off the alarm trigger status. Default= 0
Door Intruded	<ol style="list-style-type: none"> 1. Select an event type as Door Intruded: If door has been intruded by an exception method, will keep a Door Intruded record to log. If a selected Event Type level is higher than Alarm Trigger Level, Relay will be triggered then sent an E-mail to all addresses which have been pre-configured this page. 2. If Latched Time=0 ,then you have to go back to Door Setting monitoring page to click “Alarm Off” to put off the alarm trigger status. Default= 4
Anti Duress alarm	<ol style="list-style-type: none"> 1. Select an event type as Anti Duress: If user triggered Anti Duress alarm when passing door with this anti duress password → # before flashing card, Anti Duress will be triggered then keep a record to system. If a selected Event Type level is higher than Alarm Trigger Level, Relay will be triggered then sent an E-mail to all addresses which have been pre-configured this page. 2. If Latched Time=0 ,then you have to go back to Door Setting monitoring page to click “Alarm Off” to put off the alarm trigger status. Default= 4
Fire Alarm	<ol style="list-style-type: none"> 1. Select an event type as Not Allowed Door: If Fire Alarm detection has been triggered, a Fire Alarm record will be recorded to system. If a selected Event Type level is higher than Alarm Trigger Level, Relay will be triggered. 2. If Latched Time=0 ,then you have to go back to Door Setting monitoring page to click “Alarm Off” to put off the alarm trigger status. Default= 5
Latch Time	Latched time triggered should be 0~65535 seconds. If Latch Time=0 stands for no recovery time, should be back to Door Setting Monitoring page to manually put off the Latch time alarm.
Even Type Level	If a Event Type level is higher than Alarm Trigger level, will trigger alarm rely
Alarm Trigger Level	If a Event Type level is higher than Alarm Trigger level, will trigger alarm rely
E-mail alerts	
Equipment Name	Fill the name of object
SMTP Mail Server	SMTP mail server IP
Mail 1	Email address 1 for sending mail alert

Mail 2	Email address 1 for sending mail alert
SET(Button)	Save the configuration

➤ Tools

IP Camera

IP Camera(IP) :	PORT	TYPE
<input type="text" value="192.168.2.221"/>	<input type="text" value="1"/>	<input type="text" value="VIVOTEK IP7133/7330"/>
<input type="button" value="SET"/>	<input type="button" value="Refresh"/>	

Door

----,UID=0,07/30/2009,14:46:32



【IP Camera】 — Article 20

IP Camera screen descriptions:

IP Camera	
IP Camera	IP address is required
Door	Displaying latest access person' s photo
Set (button)	Save the record
Refresh (button)	Refresh IP Cam status

Reboot

Click REBOOT to get into the main screen :

[Reboot System](#)

【Reboot System】 — Article 21

Reboot screen descriptions:

Botton

Reboot

Warm start the WEBPASS

Firmware Upgrade

Click Firmware Upgrade from left site selection menu :

FIRMWAVE UPGRADE

Warning: Upgrade must NOT be interrupted

Please select a file to upgrade : 瀏覽...

UPGRADE

【Firmware Upgrade】 — Article 22

Firmware Upgrade screen descriptions:

Step by Step

Press “瀏覽” button to browse the firmware code folder

Press Upgrade to execute firmware upgrade

Special operation notice

Upgrade “System Code” first then upgrade “WEB code”

RESET

Click RESET to get into Reset All screen:

Reset All

User Data Access Logs Group Time Zone Time Set Holiday System Logs

SELECT ALL

DELETE

Reset System to Factory Default -

【Reset All】 — Article 23

RESET screen descriptions:

Reset All

User Data

Tick and Reset will remove all User List information

Access Logs

Tick and Reset will remove all Access Logs

System Logs	Tick and Reset will move all System logs
Group	Tick and Reset will remove all Group list information
Time Zone	Tick and Reset will remove all Time Zone information
Time Set	Tick and Reset will remove all Time Set information
Holiday	Tick and Reset will remove Holidays information

Button

Select All	All items to be deleted will be selected
Delete	Delete object

Step By Step :

1. Select the objects you are going to reset
2. Click DELETE to

Reset system to factory default

Factory Default	System back to Factory Default
------------------------	--------------------------------