



Napco Access Pro is a division of Napco Security Technologies Inc.  
(Nasdaq Symbol: NSSC) consisting of Access Control Brands  
Continental Access and E-Access

Continental **Access**

**CA4K**<sup>®</sup>

CardAccess Software V1.2.x

## Integration Devices BAS-IP

NAPCO Security Technologies Inc.  
355 Bayview Avenue, Amityville, NY 11701  
Telephone: 631-842-9400 Fax: 631-842-9135  
[www.NapcoAccessPro.com](http://www.NapcoAccessPro.com)

Publicly traded on NASDAQ Symbol: NSSC

The CA4K Software “Device Integration” feature allows the software to interact with third-party devices such as BAS-IP and MadEye, in order to perform certain operations.

## Enable Device Integration in System Settings

- To enable device integration, go to the **System Settings > System-wide Settings > General** tab, and enable the 'Enable Device Integration' option. Then press **Save**. (You must do a full download to all your panels/locks after enabling)
- Once enabled, under '**Configuration**' you will see a new menu called '**Integration Devices**' and also an '**Integration Profile**' drop down on the general tab under the **Configuration > Reader's** screen.

The image displays two overlapping screenshots from the CA4K software interface. The background screenshot shows the 'System-wide Settings' window, specifically the 'General' tab. In the 'General' section, the 'Enable Device Integration' checkbox is checked and highlighted with a red rectangle. Other settings like 'Enable Video System', 'Enable Activity Linking', and 'Enable Holiday Calendars' are also visible. The foreground screenshot shows the 'Configuration' menu, which is open and displays a list of options. The 'Integration Devices' option is highlighted with a red rectangle. The 'Integration Profile' dropdown menu is also visible, showing a list of profiles.

## “New Integration Profile Shown Under Reader Screen”

Readers x

New Delete Save Cancel Search Refresh Export Grid to Excel Print Grid Download Close

Reader	Description Text	Enabled	Ext Shunt	Escort
1 - 1	Reader 1 - UniVerse - HID 53	Yes	No	No
1 - 2	Reader 2 - HID 20 - OSDP	Yes	No	No
2 - 1	Wireless Lock - N95J1	Yes	No	No
3 - 1	Reader 1 - SuperTwo	Yes	No	No
3 - 2	Reader 2 - SuperTwo	Yes	No	No

Device Name Reader 1 - UniVerse - HID 5355 Partition Group Admin Partition

General Door Control Options Category Counters Priorities DVR Maps Location / Remarks Geo Fence

Panel uniVerse Reader # 1

OSDP Address 0

Reader Type  Door  Badge Validator  Wireless Lock

Assign to Access Group from Reader None

Bluetooth MAC (Last 8 digits)

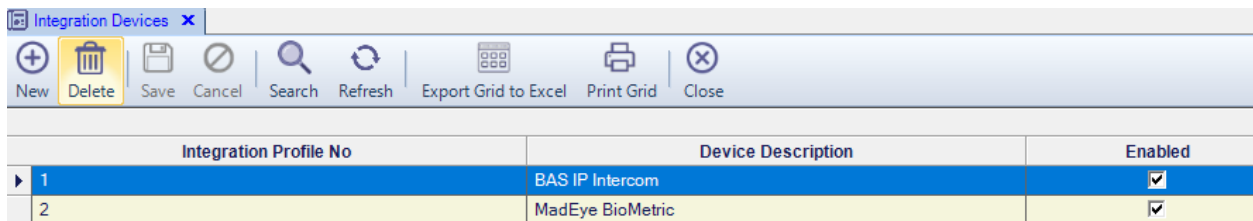
Integration Profile

- Enabled
- Report Bypass
- Bypass Unlocks
- No Transaction for Valid
- Time Schedule Violate Override
- Report Access After Open
- Badge Use Limit Controller
- Escort Enabled
- ATM Mode
- Double Read Holds Door Unlocked
- Alarm Shunt Reader

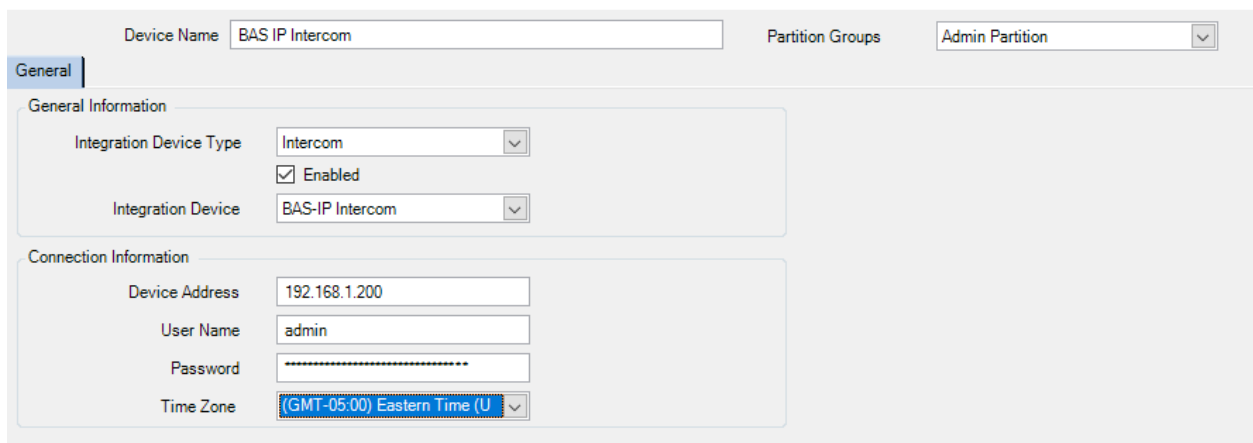
## Integration (Bas-IP) Configuration

1. Under **Configuration > Integration Devices**, Press **New** and Enter a **Device Name**.
2. Select **Intercom** as the **Integration Device Type** and **BAS-IP Intercom** as the **Integration Device**
3. Enter the **Device IP Address** along with the **username** and **password** for that device
4. Select the device **Time Zone** (This is the Time Zone of your BAS-IP Device)
5. Press **Save** when complete

**Note:** To find the Integration Device IP address, open a Windows command prompt and type "arp -a". This command will show you the connected IP addresses along with their MAC addresses. You can then locate the MAC address of the Integration Device from the list. The username and password are the Integration Devices administration credentials.



Integration Profile No	Device Description	Enabled
1	BAS IP Intercom	<input checked="" type="checkbox"/>
2	MadEye BioMetric	<input checked="" type="checkbox"/>



Device Name: BAS IP Intercom      Partition Groups: Admin Partition

**General**

General Information

Integration Device Type: Intercom  
 Enabled  
Integration Device: BAS-IP Intercom

Connection Information

Device Address: 192.168.1.200  
User Name: admin  
Password: .....  
Time Zone: (GMT-05:00) Eastern Time (U)

6. After creating an integration profile, navigate to the reader screen **Configuration > Readers** and assign the integration profile to the selected reader, then press **Save**.

Reader	Description Text	Enabled	Est Short	Escort
1-1	Reader 1 - Universe - HD 535	Yes	No	No
1-2	Reader 2 - HD 20 - GSDP	Yes	No	No
2-1	Wireless Lock - N9511	Yes	No	No
3-1	Reader 1 - SuperTwo	Yes	No	No
3-2	Reader 2 - SuperTwo	Yes	No	No

Device Name: Reader 1 - Universe - HD 535 Partition Group: Admin Partition

General | Door Control | Options | Category Counters | Priorities | DVR | Maps | Location / Remarks | Geo Fence

Panel:  Reader #:

OSDP Address:

Reader Type:  Door  Badge Validator  Wireless Lock

Assign to Access Group from Reader:

Bluetooth MAC (Last 8 digits):

Integration Profile:

Enabled  
 Report Bypass  
 Bypass Unlocks  
 No Transaction for Valid  
 Time Schedule Violate Override  
 Report Access After Open  
 Badge Use Limit Controller  
 Escort Enabled  
 ATM Mode  
 Double Read Holds Door Unlocked  
 Alarm Shunt Reader

- Go to **Access > Access Groups** and add the reader to an access group. You must set a “Time Schedule” for the reader. Then press **Save**.
- After the programming is complete, you can test the integration profile by following the steps below.
  - In CA4K, go to **Personnel** to create a new badge
  - Enter a **First/Last Name** and **Badge Number**
  - Set an **Activation Date Time** and an **Expiration Date Time**. (If you leave both fields blank, the badge is activated immediately and expires in 20 years)
  - Click on the **Access Group** tab and assign the access group to the user
  - Press **Save**
  - After the new badge has been saved, login to your Bas-IP web portal
  - Go to **Access management > Identifiers** tab, where you should see your newly created badge information. Under **Access Management > Access Restrictions** you will see the Activation and Expiration Times for your Badge.