LenelS2
1212 Pittsford-Victor Road
Pittsford, New York 14534 USA
Tel 866.788.5095 Fax 585.248.9185
www.LenelS2.com

OSDP and OSDP Secure Channel for Iris ID Readers

OEM Device Configuration Guide Updates

Much of the information in BIOMETRIC DEVICES > Iris Recognition of the OEM Device Configuration Guide has been updated for support of OSDP and OSDP Secure Channel for iCAM7000/7S Series readers. Therefore, the entire content of the Iris Recognition section is included in this document.

Iris Recognition

The iris of every human eye exhibits a distinctive pattern. A captured image or generated template of the iris can be used to verify identity. The iris is the colored, visible ring around the pupil.

When devices such as sensors, cards or mobile credentials are activated by proximity, subjects positioned 12-36 inches away (depending on the iris camera model) can be enrolled and/or verified with audio and visual cues.

Individual images from the live video are taken, then the highest quality images from the multiple images that have been captured are used. The algorithm of the iris recognition process analyzes the patterns in the iris visible between the pupil and sclera and converts them into a digital template. This template can be encrypted and stored in a database or on a SmartCard and used to identify or verify the identity of the person and, if known and correct, the badge number is sent to the access control panel for evaluation of access rights.

Using Iris ID System technology can be done using Iris ID EAC software or by leveraging the native integration available through OnGuard. For detailed set up and configuration of the current generation of iCAM units, please refer to the notes that follow and or review documentation at www.IrisID.com.

When Iris ID is integrated with OnGuard, the iCAM is activated by placing the SmartCard with the stored iris template against the iCAM. The same mirror-assisted, audio-prompted interface helps ensure proper positioning and quick recognition. The camera unit uses a methodology to create, select, and digitize an image to be compared against the value obtained at enrollmentWhen devices such as sensors, cards or mobile credentials are activated by proximity, subjects positioned 12 - 36 inches away (depending on the Iris camera model) can be enrolled and/or verified with audio and visual cues.

OnGuard Iris ID Solutions

Integration	Complimentary
Use Case 1: Native integration between OnGuard and Iris ID System's Iris Recognition suite	**Use Case 2: OnGuard and Iris ID software run independently**
Requires proper OnGuard licensing to enable the Iris ID components available for iris enrollment and SmartCard encoding via OnGuard	Requires properly licensed OnGuard and Iris ID System EAC software based on the number of enrollees (ex. 500 up to 100K licenses are available.) Please see price book.

OnGuard Iris ID Solutions

Integration	Complimentary
Use Case 1: Native integration between OnGuard and Iris ID System's Iris Recognition suite	**Use Case 2: OnGuard and Iris ID software run independently**
Iris templates are generated and encoded to the SmartCard for 1:1 verification with a minimum of 2-factor verification (3-factor verification is also supported). 1:N identification is not currently supported.	One-to-many (1:N) identification, 1:1 verification with cards and PINs as well as 3-factor authentication and encoding templates to supported SmartCard with proper storage capacity.
Minimum OnGuard software licensing: SWG-IRIS IrisAccess Software Interface for OnGuard ES, ADV and PRO Solutions SWG-IRIS-ENT IrisAccess Software Interface for OnGuard ENT Solutions. This license is required for each region in which Iris ID templates will be enrolled.	
Minimum Iris ID System software licensing: One (1) EAC500 software license to enable and configure all functionality with the iCAM7S.	

Install iCAM7000/7S Series Readers

The iCAM7000 Series models and iCAM7000S Series (7S) models are similar, but are also two distinct generations. The current shipping models series are the iCAM7000S series that are available in four model variations. The earlier EOL iCAM7000 series (serial number beginning "RB") and its model variations are End of Life but are still supported, and can inter-operate with the newer 7S series models and software.

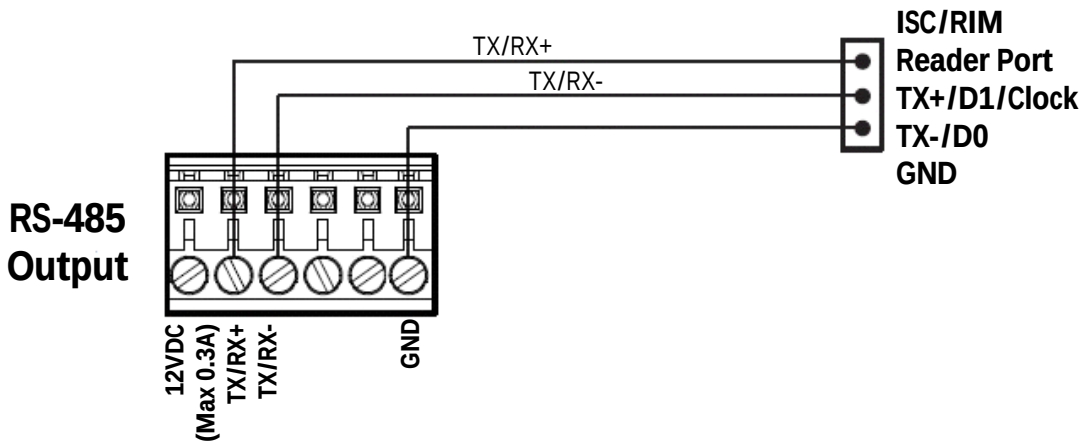
Wire iCAM 7000/7S Wiegand or OSDP Readers

Note: Refer to the applicable iCAM Hardware Guide to correctly wire Wiegand or OSDP to the access panel. This can be found in the documentation accompanying the unit or on the manufacturer's web site at http://www.irisid.com.

Iris Recognition Reader	EAC Software	iCAM Firmware	Wiegand	OSDP
Current model series				
iCAM7000S series models - Serial numbers beginning with "RS", "RN", and "RQ"	3.21	8.22.15	Yes	Yes
End of Life: Still supported				
iCAM7000 series models - Serial numbers beginning with "RB"	3.21	7.21.*xx*	Yes	No

1. Wire the iCAM7000S downstream RS-485 port to the LenelS2 access panel (ISC) or reader interface module (RIM) Reader Port according to the iCAM7000S hardware connections. Older, EOL iCAM7000 series (non "S") do not support OSDP.

Figure 1. iCAM OSDP Reader wiring to ISC/RIM Reader Port



2. On the dual reader interface module, set J2 to Unregulated and set J3 to 2W.

   WARNING: Verify that the wiring is done according to this drawing. Incorrect wiring might cause hardware damage.

External Reader for SmartCard with Iris on Card

If the iCAM does not include a reader inside the unit, an external reader must be installed along with the iCAM. Connect the reader to the Wiegand In and Smart Card ports of the iCAM. For wiring details, refer to the IrisAccess Smart Card Integration documentation (included with the unit or on the manufacturer's web site: http://www.irisid.com.

Configure iCAM7000/7S Series Readers

The iCAM7000/7S Series for iCLASS and DESFire are iris cameras supported by the OnGuard system. Each iCAM unit requires an Ethernet network connection and 12-24 VDC, 24W.

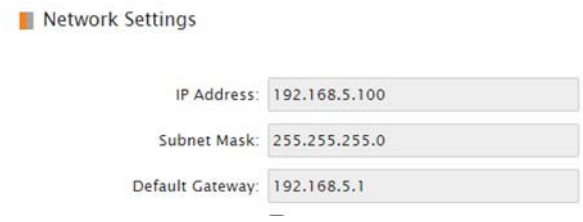
For more information about camera installation and configuring the following settings, refer to the *iCAM7000 / iCAM7000S series manuals* and the *IrisAccess Web Configuration Interface Guide for iCAM Series*.

Once the iCAM is connected, log into the camera, and then set the IP address, subnet mask, and default gateway for the iCAM. Each iCAM must be changed individually. Do not connect more than one unconfigured iCAM to the network at a time to avoid IP address conflicts.

iCAM Camera Network Settings

1. Wire the iCAM for network and power. For more information, refer to For more information please refer to Wire iCAM 7000/7S Wiegand or OSDP Readers on page 2.

2. Because iCAM series cameras are static IP devices, connect the iCAM units directly to your computer using a direct cable connection. Make sure your computer is in the same IP range as the default iCAM IP address.



Set your computer to the static IP address of 192.168.5.100, subnet 255.255.255.0.
Your computer should look like this:

3. To access the iCAM Configuration web page, open a web browser to connect and type in the default IP address `http://192.168.5.100`.

4. Log in using the default Username: `iCAM7000` and Password: `iris7000` (all case sensitive). The iCAM Configuration screen is displayed:

5. Click [Network Settings].
   a. Enter a new IP address for the iCAM (default = 192.168.5.100).
   b. Enter the new Subnet Mask for the iCAM (default = 255.255.255.0).
   c. Enter the new Default Gateway for the iCAM (default = 192.168.5.254).
   d. Disregard the Server IP and Security ID section.
6. Click [OK] to save the changes.This change will initiate a device reboot. After a few seconds the web browser will resolve to the new IP address (only if the iCAM IP address is on the same subnet as the computer).
7. Ping the production IP address entered in step to verify, and then log in to the iCAM7000/7S Configuration web page to the iCAM Configuration web page following step 3 but this time use production IP address instead of default IP.

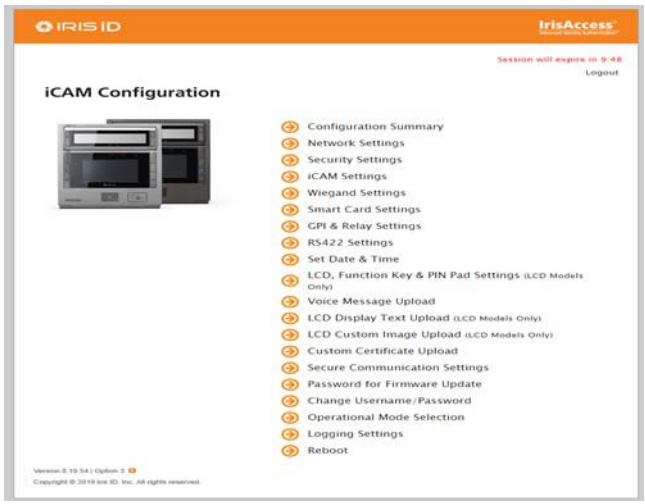
ICAM Operational Mode

Now you will need to change the device operational mode to configure it properly.

1. From the main menu, select **Operational Mode Selection**.
   a. To configure the iCAM7000S/7S, select **Option 3: On-Device Control and Iris Matching Mode** for iCAM readers that are configured for the doors. (The iCAM enrollment reader(s) are configured with **Option 1**.)
   b. Make sure **Iris Template MUST BE Encoded onto SmartCard** is selected.
   c. The device will reboot again.
   d. When the device is online again, reconnect to the configuration web page following step 5. This time you will see more iCAM Configuration options.

e. Click [OK] to save the changes. The device will reboot again.

When the device back online, reconnect to the iCAM Configuration web page. This time more options are available:



iCAM Settings

1. From the main menu, select **iCAM Settings**.
   a. Change the Recognition Mode to **Smart Card (Iris on card) + Iris**.
   b. Set the Verification Time Out to **10 sec**.
   c. For Tilt Assist, select **By Card/PIN** or as required by the site.
   d. For Eye Selection, select **Either** (default setting). Both irises will be captured but only one iris needs to match.
   e. Set Countermeasure and Sound Volume as required by the site.
   f. For iCAM Tamper, select **Detect iCAM Tamper** if needed.
2. Click [OK] to save the changes.

Wiegand Settings

1. From the main menu, select **Wiegand Settings**.
   a. Make sure **Wiegand In** is enabled.
2. Under Wiegand Out:
   a. Make sure **Wiegand Out** is enabled.
   b. Select **Bypass the user's Card ID (Hexadecimal) data to Wiegand Output without bit interpretation**. ("Bypass" will pass through the Wiegand format and Facility Code without changes.)
   c. For iCAM iClass:
      i. Set Pulse Duration to **40 usec**.
      ii. Set Bit Period to **2140 usec**.
   d. For iCAM DESFire:

i. Select **Output the user's Card ID (Decimal) data to Wiegand Output in the format defined below**. The Card ID of the smart card is stored in the data area of the card.

ii. Select **Lenel FASC-N**.

iii. Set Active State to **Low**.

iv. Set Pulse Duration to **40** and the Bit Period to **2148**.

3. Click [OK] to save the changes.

iCAM OSDP/RS422 Settings

1. From the main menu, select **OSDP/RS-422 Settings**.
   a. From the **Serial Communication** drop-down, select "OSDP (RS-485)".
   b. **Installation Mode** should be enabled when the **OSDP: Secure Channel** is selected for iCAM OSDP Output Readers. (In OnGuard, the **OSDP: Secure Channel** is selected for the iCAM OSDP reader on the General form. From System Administration, select ***Readers and Doors*** from the ***Access Control*** menu.)
   c. Click [OK] to save the changes.

Smart Card Settings

1. From the main menu, select **Smart Card Settings** (when iris templates are stored on the card).
2. Select the Smart Card Type:
   a. If you are using iCLASS (for iCAM units with SmartCard readers built in only):
      i. Set the Smart Card Type to **iCLASS**.
      ii. Enter the authentication key.
      iii. For the Block Offset (hexidecimal), enter **13** (this is the default setting).
      iv. When encoding with the iCAM, set the Data format in Smart Card to **GSC-IS Format**. If you are using a stand-alone encoder, set the Data format in Smart Card to either **GSC-IS Format** or **Lenel Format**.
      v. For Book, select the same type (Book 0 or Book 1) configured for the IrisAccess card format in the access control software.
      vi. For the Encryption Algorithm, select the same type (AES, DES, DES3, or None) configured for the IrisAccess card format in the access control software.
      vii. Click [Encryption Key File]. Choose the key file. (This should have been generated using the access control software and stored to a file.)
   b. If you are using DESFire (for iCAM units with MIFARE/DESFire card readers only):
      i. Set the Smart Card Type to **DESFire**.
      ii. Make sure the option where smart card used as a **Prox Card** is not selected. The Book and Block Offset settings do not apply.
      iii. For DESFire, specify Lenel for Communication.
      iv. When encoding with a stand-alone DESFire encoder, (like SmartID/Pro or Digion 24 (MIFARE/DESFire), set the Data format in Smart Card to **GSC-IS Format**.
      v. For the Encryption Algorithm, select **None**.

vi. Enter the Authentication Key. This should be one of the three keys that make up the composite master key.

c. If you are using HID iClass:

i. Set the Smart Card Type to **HID iClass**.

ii. In the Application Configuration section: Enter **13** as the Offset and enter the Authentication Key. The key must match the Iris card format in OnGuard.

iii. Set Book to the same format (**Book 0 or Book 1**) as required.

iv. Set Offset (hexadecimal) to **13**.

v. Set the Application Key (hexadecimal) as required by the site. Authentication Key. This Key must match the Iris card format in OnGuard.

vi. Set the Data Format to the same format (**GSC-IS Format** or **Lenel Format**) that will be used to encode the iris data onto the smart card.

Note: If you are using the specific Lenel Format, the software does not support writing to Book 1/16kbits/2 Application Areas or Book 1/16kbits/16 Application Areas.

vii. Set the Encryption Algorithm and Encryption Key File as required by the site.

Note: The Encryption Algorithm and Encryption Key File settings must match the Card Format settings. For more information please refer to Configure iCAM7000/7S Series Readers on page 3.

3. Click [OK] to save the changes.

GPI & Relay Settings

1. From the main menu, select **GPI & Relay Settings**.
2. In the Access Settings section:
   a. Make sure **The PACS (Physical Access Control System) controls the user's Access Rights** is selected.
   b. Make sure **Wait for Access Control Panel response** is not selected. (Using this selection requires an extra dedicated wire from the panel back to the iCAM.)
3. In the Relay Settings section:
   a. Set Relay 1 - Door Control to **Disable**.
   b. Set Relay 2 - Tamper Notification to **Disable**.
4. For the Access Door tab, configure the settings as desired. or For door control and monitoring, configure the settings as desired.
5. For the GPO tab, configure the settings as desired. or For GPI, configure the settings as desired.
6. Click [OK] to save the changes, and then reboot from main menu to make sure all changes took place.
   The username and password may be required to reboot.

Card Formats in OnGuard

The following should be configured in System Administration on the Card Formats form.

1. Choose the application.
2. Click [Modify].
   a. If you are using iCLASS:

i. Set the Application to **IrisAccess (iCLASS)**.

ii. The Application Key should be configured using the iCAM Configure web page.

iii. Select the Iris data format (**GSC-IS Format** or **Lenel Format**) from the drop-down. Make sure to choose the same format that will be used to encode the smart card. When an iCAM device will be used to encode IrisAccess credentials, make sure to select "GSC-IS Format".

iv. Choose the memory configuration.
When **Book 1/16kbits/2 Application Areas** or **Book 1/16kbits/16 Application Areas** is selected, the IrisAccess application will be written to Book 1 according to the selected card layout. Book 0 remains untouched. If Book 0 is selected, Book 1 remains untouched.

Note: When encoding with the iCAM, the application key and memory configuration in OnGuard are not used. Instead, the application key should be configured using the iCAM Configuration web page.

v. Next to the Iris Data Encryption Method, click [Change].

vi. Select the encryption algorithm (AES, DES, or DES3) from the drop-down.

vii. Click [Generate New Key].

viii. If you selected [Store Key to File], a new key is automatically generated. If you want to store the key in an encrypted file, click [Store Key to File], enter the file name and click [Save].

b. If you are using DESFire:

i. Set the Application to **DESFire (TWIC 1.02 Data Model)**.

ii. For the Biometrics option, select **Iris**.

iii. Click [Enter/Modify CKMC] and enter the three parts of the composite master key.

3. Click [OK] to save the changes.

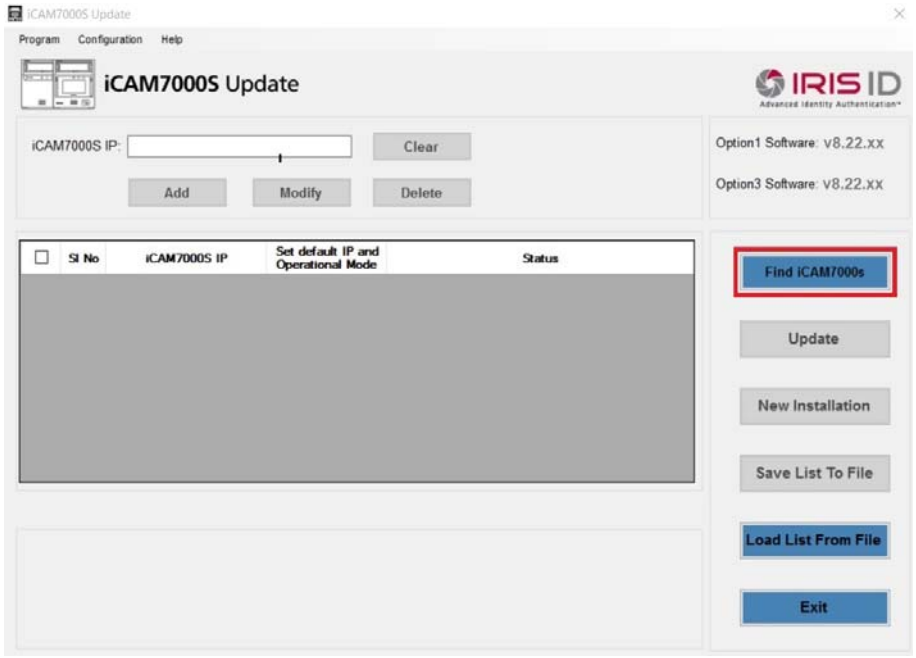
Once the card format is configured, assign the smart card format application to the badge type. This can be done in System Administration or ID CredentialCenter in the Badge Types Folder, on the Encoding Form. For more information, refer to the System Administration or ID CredentialCenter User Guides.

Update iCAM7000S Software via the iCAM7000SUpdate Utility

The iCAM7000SUpdate Utility is designed for use with iCAM7000S (iCAM7S) series camera units only. This utility requires a network connection to the iCAM. If there are multiple iCAMs in the system, it is recommended that each unit be given a unique static IP Address prior to using this utility.

Note: The iCAM7000S software must be updated to version 8.22.15 or higher to use iCAM7000S OSDP readers in OnGuard. OnGuard 8.0 and higher support OSDP Baud Rate 9600/19200/38400/115200 and Secure Channel for OSDP readers.

1. Open "iCAM7000SUpdate" (located in the ***IrisAccess EAC / Upgrade and Setup Tools*** folder on the desktop). The application window is displayed:



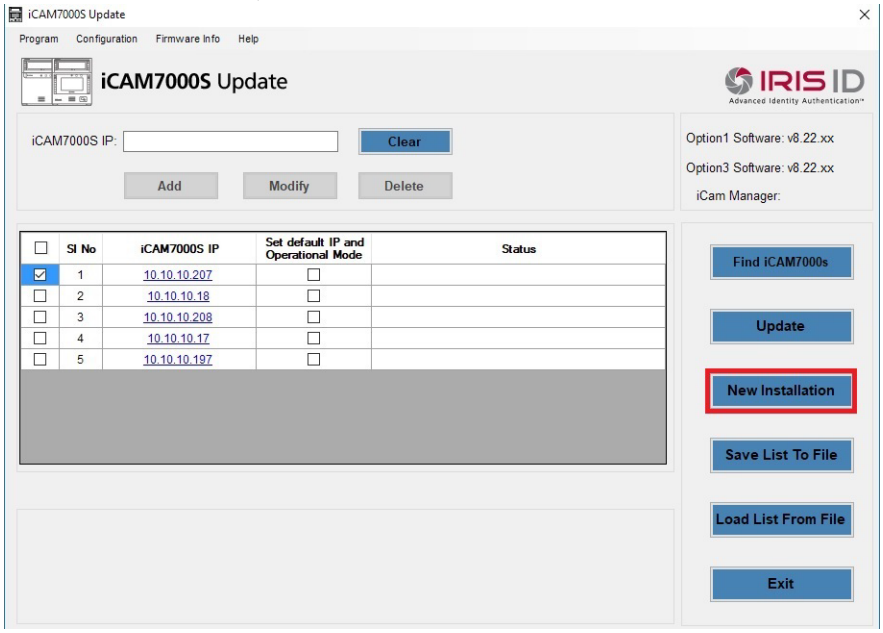
   a. Click [Find iCAM7000s] or select **Find iCAM7000s** from the ***Program*** menu. The find feature searches the network for available iCAM7S units and displays them in the list.

   b. (Alternatively) Enter a valid **iCAM7000S IP** address, and then click [Add] or select ***Add*** from the ***Configuration*** menu. The Add option is used to add the iCAM7000S unit's IP Address to the list.

Note: Network settings, windows firewall, available ports, routers, and anti-virus applications can block the applications' ability to detect iCAM7000Ss on the network.

   c. Click [OK] to confirm the message reporting that the find function will not detect iCAMs on other subnets.

2. Select the iCAMs that need to be upgraded. (This places a check mark in the column to the left of the iCAM IP address.)



   a. Click [New Installation] or select ***New Installation*** from the ***Program*** menu.
   b. If a password is requested:
      i. Enter the default password of `icam7$47`. (This is case sensitive.)
      ii. Click [OK] to continue with the upgrade.
3. After a successful installation, the iCAM will reboot automatically.

> ***Warning:*** Do not disturb the iCAM7S that is being upgraded. During this warning, do not turn off or disconnect power to the iCAM or corruption of the software may occur. The process may take up to 10 minutes per iCAM. The iCAM will not be operational during the upgrade period.

Enrollment

Note: Enrollment must be done with an iCAM7000/7S configured for **Option 1**.

To use the iCAM for capturing iris data and enrolling, it should be connected to the network. Use a workstation to access the iCAM for enrollment.

In addition to the configuration that was done through the IrisAccess Web interface, the iCAM unit must be configured in the access control software:

1. On the Encoders/Scanners form > General tab, enter a name for the iCAM.
2. Select the workstation name.
3. For the Device type, select **IrisAccess iCAM (iCLASS)**.
4. For the Credential technology, select **iCLASS**.
5. On the Communications tab, enter the IP address. This IP address must match what was set up for the iCAM network settings.

Iris capture and verification can then be performed from Multimedia Capture, accessed on the Cardholders form. For detailed information, refer to the System Administration User Guide or ID CredentialCenter User Guide.

Note: The HID Access Control (iCLASS) application must be present on the card in order to verify the IRIS ID credential at the reader. The HID application may be encoded from OnGuard or comes encoded on cards purchased as such from HID.

Limitations

The current system architecture does not permit the use of an iCAM camera for both enrollment and verification purposes without being rebooted into mode 1/enroll or mode 3/verification. When connecting to an iris camera, connect only one workstation at a time.

Verification

In System Administration, configure IrisAccess biometric and HID (iCLASS) AccessControl smart card formats for encoding cardholder data. The reader's card format should be Wiegand. In the card format application, set the Iris data format to the same format that will be used to encode the smart card and the Encryption method to AES/DES/DES3.

Biometric and access control data must be encoded on the badge. Select either the available encoder optionally available from Lenel to perform template encoding or use the internal encoder available in the iCAM7S series model iCAM7010S-H1B or iCAM7111S-H1B. (The HID RW4000 is no longer available as an option.) Connect and configure an HID (iCLASS) RW4000 Prog encoder. Assign the configured smart card formats to a badge type (for instance, to Employee) for the encoding procedure. Choose a cardholder with a valid badge and iris biometric templates and encode the cardholder's data to blank 16K/2 or 16K/16 or 32K/2 or 32K/16 Application Areas.

Verify the data encoded by presenting the encoded badge to the HID (iCLASS) reader inside the iCAM7S.

The current system architecture does not permit the use of a camera for both enrollment and identification/verification purposes unless it is rebooted into and properly configured between the Option 1 and Option 3 settings.

Note: When presenting the card for verification, keep the card positioned on the reader after it beeps and announces "Please center your eyes in the mirror." Do not remove the card until instructed to "look into the camera".

Software Upgrades

Refer to the manufacturer documentation included with the device to upgrade the software, or use the iCAM web page to upgrade an iCAM7000/7S. The upgrade procedure might vary depending on your current version of the software, so use the appropriate documentation.

Firmware upgrades, if applicable, are performed to the iCAM7000 using the web user interface.

