



# AVIGILON Access Control Manager Enrollment Operator User Guide

[Home](#) » [aVIGILON](#) » AVIGILON Access Control Manager Enrollment Operator User Guide 

## Contents

- [1 AVIGILON Access Control Manager Enrollment Operator](#)
- [2 Product Information](#)
- [3 Product Usage Instructions](#)
- [4 Introduction](#)
- [5 External Systems – Defining the Badge Camera for the System](#)
- [6 Documents / Resources](#)
  - [6.1 References](#)

# AVIGILON™

## AVIGILON Access Control Manager Enrollment Operator



## Product Information

- **Product Name:** Access Control Manager™
- **Version:** 6.44.0

## Table of Contents

- Introduction
- Adding an Identity
- Identities
- Assigning Roles to Identities
- Assigning Tokens to Identities
- Assigning Groups to Identities
- Capturing and Uploading Photos of an Identity
- Creating Badges for Identities
- Searching for an Identity
- Editing an Identity
- Enrolling Identities and Issuing HID Origo Tokens
- Issuing a Token to an Enrolled Identity on a Registered Mobile Device
- Registering a New Mobile Device for an Enrolled Identity
- Searching for HID Origo Tokens
- Permissions and Rights
- External Systems – Defining the Badge Camera for the System

## Product Usage Instructions

### Adding an Identity

1. Select “Identities”.
2. Click “Add Identity”.
  - If Identity Profiles are configured, select the profile for the identity and click “OK”. The Identity Add page appears with the details of the identity profile. Otherwise, click “Cancel”.
3. Fill out the Last Name field and the required details.
  - **Note:** Additional fields can be added using the User Forms or User Lists feature.
  - For identities using SALTO devices only, First Name and Last Name are required.
  - For identities using HID Origo tokens only, First Name, Last Name, and Email Address are required to enroll the identity in HID Origo.
4. Click “Save”.
5. Assign roles to the identity as required on the Roles tab and click “Save”.
  - To add an item, select it from the Available list and click “+”.
  - To remove an item, select it from the Members list and click “-”.
  - **Tip:** Use Shift + Click to select items in sequence. Use Ctrl + Click to select individual items.
6. Enter the token details as required on the Tokens tab.
  - By default, the Download checkbox is selected, which downloads the token to the connected panels and associated doors.
  - For identities using SALTO devices only, click the Download button to download the token to the SALTO

server and door.

- For identities using ASSA ABLOY IP devices only, click the Download button to download the token to the DSR and door.

7. Click “Save” when finished.

8. Add more details about the identity on the other tabs if necessary.

- **Note:** The labels of the built-in tabs, such as Identity and Tokens, may be renamed by your System Administrator. A custom form or User Defined Tabs with User Defined Fields may be added at the end of the list.
- The default Enrollment Operator role does not have access to certain tabs. Contact your System Administrator for more details.

## Identities

The Identities screen gives you access to all tokens and operators of the system. An identity is added to the system when a new user needs access to the site. For example, when a person is hired. Access to a site may be physical access to an area or access to the ACM system to manage the site.

## Introduction

This guide provides an overview of the default Enrollment Operator role as defined in the Avigilon Access Control Manager (ACM™) software. This guide is meant to be used and referred to by those assigned the role of an Enrollment Operator within the ACM software.



Enrollment Operators manage identities within the system. They are responsible for creating new identities and maintaining identity records. Enrollment Operators are also responsible for creating, issuing, and printing badges. For more information, see Permissions and Rights on page 18.

**Note:** This guide does not define the role of an Enrollment Operator on all sites. Please contact your System Administrator for more details.

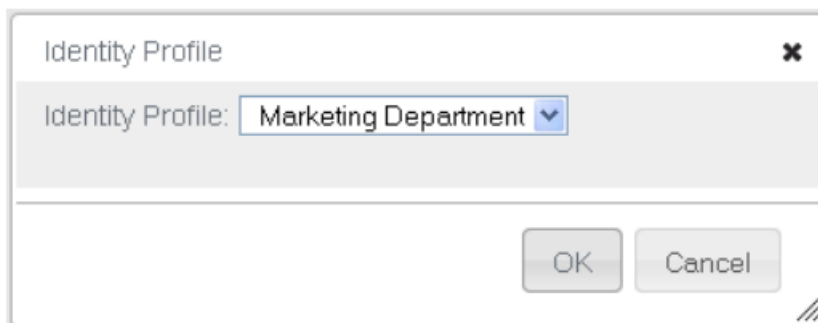
## Adding an Identity

A person with an identity record in ACM can be issued a badge to enter the physical site. A user of the ACM software can be issued a login and password.

### To add a new identity

1. Select  Identities.
2. Click  Add Identity.



If Identity Profiles are configured, select the profile for the identity and click OK. The Identity Add page appears with the details of the identity profile. Otherwise, click Cancel.


A screenshot of a software dialog box titled "Identity Profile" with a close button (X) in the top right corner. Inside the dialog, there is a label "Identity Profile:" followed by a dropdown menu that currently displays "Marketing Department". At the bottom right of the dialog, there are two buttons: "OK" and "Cancel".


3. Fill out the Last Name field and the required details.

**Note:** Additional fields can be added using the User Forms or User Lists feature. Identities using SALTO

devices only. First Name and Last Name are required. Identities using HID Origo tokens only. First Name, Last Name, and Email Address are required to enroll the identity in HID Origo.

4. Click  Save.
5. Assign roles to the identity as required on the Roles tab and click  .|

To add an item, select it from the Available list and click .

To remove an item, select it from the Members list and click .

**Tip:** Use Shift + Click to select items in sequence. Use Ctrl + Click to select individual items.

6. Enter the token details as required on the Tokens tab.

By default the Download checkbox is selected, which downloads the token to the connected panels and associated doors. Identities using SALTO devices only. Click the Download button, which downloads the token to the SALTO server and door. Identities using ASSA ABLOY IP devices only. Click the Download button, which downloads the token to the DSR and door.

When you are finished, click .

7. Add more details about the identity on the following tabs

- **Roles:** Assigns a role to this identity.
- **Tokens :** Creates a token for the identity.
- **Groups:** Assigns the identity to a group.
- **Capture:** Takes a photo of the user.
- **Photos:** Uploads an existing photo of the user.
- **Badge:** Assigns a badge to the user.
- **Timed Access:** Assigns timed access to the user.
- **Access:** View the identity's access privileges including roles, access groups and doors.
- **Transactions:** View transactional data associated with the identity.
- **Audit:** View a log of all the changes that have been made to this identity.

The default Enrollment Operator role does not have access to this tab. Contact your System Administrator for more details.

**Note:** The labels of the built-in tabs, such as Identity and Tokens, may be renamed by your System Administrator. A custom form or User Defined Tabs with User Defined Fields may be added at the end of the list.

## Identities

The Identities screen gives you access to all tokens and operators of the system. An identity is added to the system when a new user needs access to the site. For example, when a person is hired. Access to a site may be physical access to an area or access to the ACM system to manage the site.

Physical access to the site allows a user to access areas and doors. Access to the ACM system allows users to manage the site, such as adding users or monitoring events.



For a user to have access to the system or physical access to the site, they must have an identity.

- If the user requires access to the system, they are issued a login and password. This allows the user to access areas of the system. The areas of the system the user has access to depends on their role.
- If a user requires physical access to the site, they are issued a token. The token gives the user physical access to the site. This allows the user to access areas on the site. The areas the user has access to depends on their role in the system.

## Assigning Roles to Identities

A role defines what a user has access to. For identities to have access to the system or physical access to the site, they must be assigned a role. Each role contains access groups and/or delegations. Access groups allow a user to have physical access to the site. Delegations allow a user to have access to the system. The user will be assigned a role depending on their position in the organization.

To assign roles to an identity





1. Click  Identities.
  2. From the Identities Search page, perform a search for an identity.  
For more information, see Searching for an Identity on page 14.
  3. Click on the name of the identity you want to edit.
  4. Select the Roles tab.
  5. From the Available list, select all the roles that you want to assign to the user, then click The role is added to the Members list to show that it is now assigned.  
To remove a role from the user, select the role from the Members list, then click .
- Note:** You can select multiple items by using the Ctrl or Shift key.
6. Click  Save.

## Assigning Tokens to Identities

Tokens are used to authenticate individuals and allow or deny them physical access to your site. Tokens are assigned to personnel identity records along with access cards, biometric data such as fingerprints, or connected devices such as smartphones with apps that can be presented for authentication at readers.

To further restrict access, identities can be assigned to specific roles within your site.


To create tokens and assign them to an identity


1. Select  Identities > Identities.
2. Search for an identity.  
For more information, see Searching for an Identity on page 14.
3. Click the name of the identity you want to edit.
4. Select the Tokens tab.
5. **If only one token has been defined, the Token:** Edit page appears.  
If more than one token has been defined, the Tokens list appears. Click Add Token.
6. Enter the details as required.  
**Note:** If you are assigning HID Origo tokens, see Enrolling Identities and Issuing HID Origo Tokens on page 16.
7. Click  and then  to return to the identity search.
8. Click Download to download the token to the connected panels and associated doors.
9. To assign this token to a badge, select the Badge tab.  
From the Badge Token drop down list, select the internal number you want to assign to the badge.
10. Click .


## Assigning Groups to Identities

Groups are used to group physical and/or system components. Groups are assigned to identities primarily for batch updates. For example, if all the badges are close to expiry and they are assigned to the same group, the expiration date can be extended through a batch job.

**To assign groups to an identity**

1. Click  Identities.
2. From the Identities Search page, perform a search for an identity. For more information, see Searching for an Identity on page 14.
3. Click on the name of the identity you want to edit.
4. Select the Groups tab.

From the Available list, select all the groups that you want to add the user to, then click .

5. The group is added to the Members list to show that the user is now a member. To remove a user from a group, select the group from the Members list, then click .

**Note:** You can select multiple terms by using the Ctrl or Shift key.

6. Click  Save.

### Capturing and Uploading Photos of an Identity

Capture or upload photos of a person from the Photos tab on a person's Identity page. Then you can select a photo from this page to appear on that person's Identity page or printed on an access badge.

**Captured photo:** A photograph taken by a badge camera connected to your computer and to the ACM system, and saved in the ACM system. Captured photos are in JPG format.

**Uploaded photo:** A graphics file in JPG, PNG, or GIF format that you upload from any location your computer can access and save in the ACM system. Typically, you would upload a JPG file for access badges.

**Note:** The Microsoft Edge web browser supports only the uploading of JPG files. Do not attempt to upload any other file format if you are using the ACM client in the Microsoft Edge web browser. Using photos taken directly from a mobile phone is supported.

Photos saved in the ACM system can be cropped, resized, and rotated to meet the standardized requirements of the badge templates defined in your system.

You can use two types of cameras as a badge camera to capture a photo

- Local Camera — Any camera connected directly to your computer or built into your computer or monitor.
- IP-based camera — Any IP-based camera previously connected to your network and added to your ACM system.

### Before you can

- Use a camera to capture photos, you must specify the badge camera you want to use in your user profile. For more information, see External Systems – Defining the Badge Camera for the System on page 20.
- Generate and print a badge, at least one badge template must be defined in your system.

After a photo has been added to the Photos tab of an identity, you can edit the photo to suit the requirements of your badge templates. Then you can create a badge with that photo. For more information, see Creating Badges for Identities on.

### Capturing a photo

1. There are two ways to access the Capture page

From the Identities Search page, click  from the Image Capture column.

From the Identities Search page, click on the name of an identity, select the Photos tab, then click Capture a Photo.

2. If you are using

- A local camera that you have not used before, this page will not appear unless you allow your web browser to access your camera. The first time you access the Capture page, you are prompted to allow your browser to access your local camera. Click Allow.
- An IP-based camera and the camera requires authentication, this page will not appear until you have entered your login credentials.

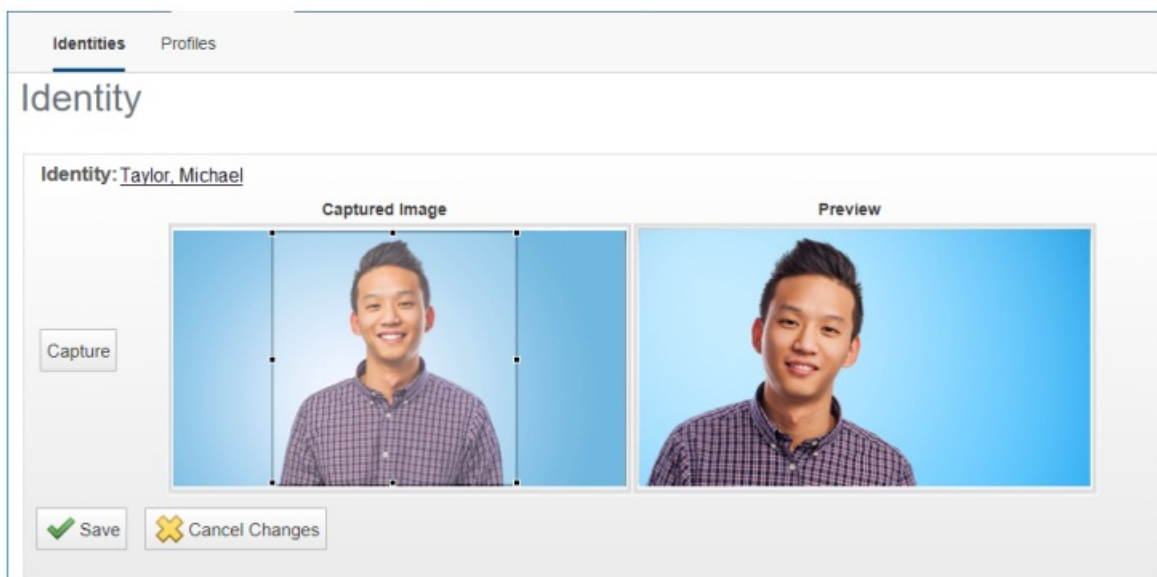
Enter a user name and password, then click OK.

The Capture page appears, with the live preview from the camera showing on the right.

3. Click Capture.

The page refreshes to show the captured photo on the left and the live preview on the right.

A cropping overlay is imposed over the photo, The aspect ratio of the overlay is determined by the values set on the System Settings page for Badge Template Photo Height and Badge Template Photo Width.



4. Click:

✓ Save to save the photo that part of the image highlighted in the cropping overlay is saved. Cropping the photo using this aspect ratio ensures that the photo will fit exactly into the photo area on the badge without any distortion.

5. Save and Edit to save the photo and open the photo editing tool, or ✓ Save to add the photo directly to the Photos tab.

Identity page and access badge.

6. Click Save ✓ .

## Uploading a photo

1. From the Identities Search page, click on the name of an identity, select the Photos tab, then click Upload a Photo.

The screen expands to include more fields.

2. Click Choose File and navigate the directory to find the photo you want to upload.

Click Open to select the photo. You can upload files in JPG, PNG, or GIF format.

3. On the Photos tab, click the Primary checkbox if you want this photo to appear on this person's Identity page

and access badge. If no primary photo is selected, the first photo on the list is used.

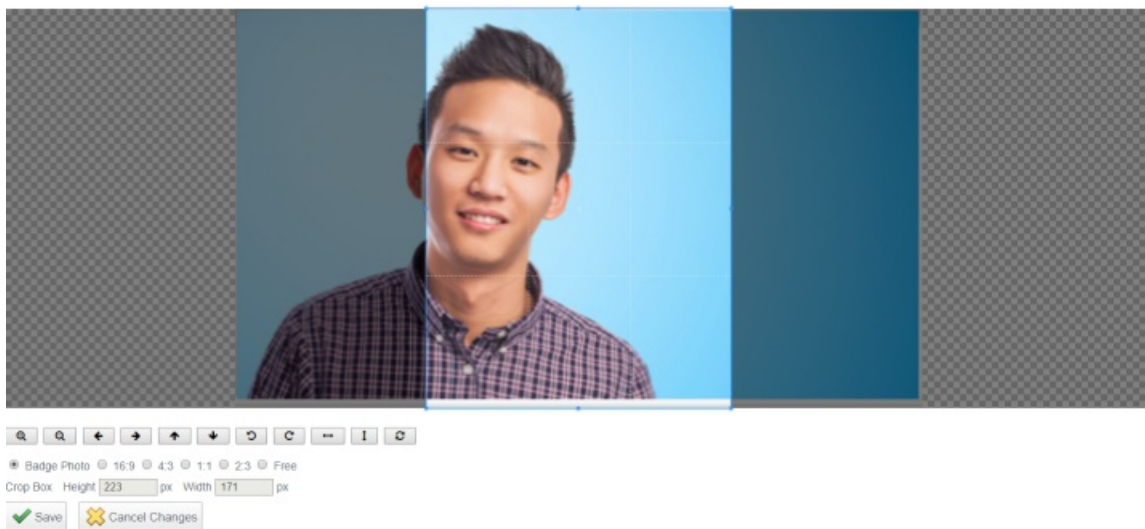
4. Click  Save.

### Editing a photo

You can edit a captured photo when you first save it by clicking Save and Edit. You can edit any saved photo by clicking on its filename link or thumbnail photo on the Photos tab.

The photo is displayed with a brighter cropping overlay imposed over it. The overlay is preset to the Badge Photo aspect ratio. This ratio is determined by the values set on the System Settings page for Badge Template Photo Height and Badge Template Photo Width. Cropping the photo using this aspect ratio ensures that the photo will fit exactly into the photo area on the badge without any distortion.

Use the mouse in combination with the control buttons under the photo to crop, resize, rotate and flip the photo. You cannot edit the actual photo, or change its resolution by zooming in and out. The dimensions shown in the Crop Box options are read-only and cannot be entered directly, but are dynamically updated as you manipulate the cropping overlay with the mouse.



#### 1. Adjust the overlay.

- To reposition the overlay over the photo
- Click inside the cropping overlay.
- Drag the mouse to move the overlay.
- To resize the overlay
- Click on the bounding frame. The mouse cursor will change to indicate the direction the overlay can be resized.
- Resize the overlay. The selected aspect ratio (usually the Badge Photo aspect ratio) is retained.
- To change to a different aspect ratio
- Click to select the required aspect ratio.
- To resize the overlay freely
- Click Free.
- Click on the bounding frame. The mouse cursor will change to indicate the direction the overlay will be resized.
- Drag the mouse to resize the overlay. The overlay will be resized only in the direction of the cursor.
- To rotate the overlay
- Click outside the current overlay.
- Drag the mouse to draw a new overlay.



- To replace the overlay
- Click outside the current overlay.
- Drag the mouse to draw a new overlay.

## 2. Adjust the photo.

- To enlarge or reduce the photo
- Use the + and – magnifier control buttons to adjust the photo size in stepped increments.
- To reposition the photo
- Use the up, down, left and right control buttons to adjust the photo position in stepped increments.
- To rotate the photo
- Use the counterclockwise circular arrow to rotate the photo to the left by 90°.
- Use the clockwise circular arrow to rotate the photo to the right by 90°.
- To flip the photo
- Use the horizontal double-ended control button to flip the photo left to right.
- Use the vertical double-ended control button to flip the photo top to bottom.
- To reset the photo
- Use the reset control button to cancel your changes and revert the photo to its previously saved version.

## 3. Save the photo

- Click Save.
- The Photos tab is displayed with the saved photo.
- When you save the photo, that part of the image highlighted in the cropping overlay is saved.


**Note:** The saved photo replaces the original photo. The original photo cannot be restored.

## Specifying the Primary photo

If you have several photos saved on the Photos tab, the first photo is used on that person's Identity page and is selected by default for the access badge. To use another photo instead, select the Primary checkbox of the photo you want.

## Deleting a photo

To delete a photo from the Photos tab


1. Click .
2. Click  Save.

## Creating Badges for Identities

Badges are identification cards that are used to verify a user's identity or association to an organization. Badges may also be used as access cards if they are printed directly on the person's RFID badge.

**Note:** Before you can print a badge, you must connect a badge printer to the network and configure it. For instructions on how to configure your badge printer, refer to the printer's user guide.

To create a badge for a user:

1. Click  Identities.
2. From the Identities list, click on the name of the identity you want to edit.
3. Select the Badge tab.

4. From the Badge Photo drop down list, select a photo for this badge.

Only the photos that have been previously uploaded or captured for this identity appear in this list.

5. From the Badge Token drop down list, select the token you want to associate with this badge. Only the tokens that have been previously defined for this user appear in this list.

6. From the Badge Template drop down list, select the badge template that you want to use for this badge.

Only the badge templates that have been previously defined appear in this list.

7. Click  Save.

8. To print the badge, click Create Badge. The badge appears in a preview window.

9. Click Print.

**Note:** When printing the badge, ensure that the Header and Footer settings are turned off or set to blank.

### Searching for an Identity

Use Identity Search to find an identity.

1. Fill out the following fields

- Last Name field.
- (Optional) First Name and/ or Internal Number fields.
- (Optional) Group field.

2. Blank entries will return all identities.

**Note:** Identities using SALTO devices only. First Name and Last Name are required. Identities using HID Origo tokens only. First Name, Last Name, and Email Address are required to enroll the identity in HID Origo.

Identities using DMP intrusion panels. Identities are defined by their DMP user name, ID and DMP panel name.2. Add other search criteria.

- Search Field drop down list.
- Search Value field.
- Click Add Criteria to add another search field and value.

To clear all fields, click Clear Search. To remove a search row, click Remove.

3. To the right of the Search button, select either

- And to find all identities that fit all entered criteria.
- Or to find identities that fit one or more of the entered criteria.

4. Click Search.

The page displays your search results.

### Editing an Identity

An identity must be edited when user information changes. For example if a user changes roles, their identity would need to reflect this. If the role is not updated, the user would not be able to access areas required for their new role.

### To edit an existing identity

1. Click  Identities.


2. Search on the Identity Search screen, then click on the identity you want to edit.

3. Navigate through the tabbed pages and make the required changes.

- **Identity:** The identity details.
- The default Enrollment Operator role cannot edit this page. Contact your System Administrator for more details.
- **Roles:** Assigns a role to this identity.
- **Tokens :** Creates a token for the identity.
- **Groups:** Assigns the identity to a group.
- **Capture:** Takes a photo of the user.
- **Photos:** Uploads an existing photo of the user.
- **Badge:** Assigns a badge to the user.
- **Timed Access:** Assigns timed access to the user.
- **Access:** View the identity's access privileges including roles, access groups and doors.
- **Transactions:** View transactional data associated with the identity.
- **Audit:** View a log of all the changes that have been made to this identity.

The default Enrollment Operator role does not have access to this tab. Contact your System Administrator for more details.


**Note:** The labels of the built-in tabs, such as Identity and Tokens, may be renamed by your System Administrator. A custom form or User Defined Tabs with User Defined Fields may be added at the end of the list.

**Note:** Remember to click  to save the changes on each page.

## Enrolling Identities and Issuing HID Origo Tokens



**Note:** Before you begin, configure the Enroll Settings section in the HID Origo Management Portal.

### To enroll an identity and issue an HID Origo token

1. Select Identities > Identities and click Search to select an identity already created.
2. Click the Tokens tab and enter
  - **Token Type:** HID Origo
  - **Mobile ID Type:** The mobile ID to be issued to the registered device.
3. Click  Enroll. An invitation is sent to the email address of the identity.
4. Instruct the identity to follow the steps in the email, including clicking an app store link to install the HID Mobile Access app and then clicking the invitation code link to enroll.
5. After the identity accepts the invitation, the HID Origo token will be available in their mobile app.

### Issuing a Token to an Enrolled Identity on a Registered Mobile Device


If you need to issue to an identity an additional credential with a different mobile ID, you can issue another token

1. Click  Add Token on the Tokens tab and enter
  - **Token Type** :HID Origo
  - **Mobile ID Type** : The HID mobile card that is not already issued to the device.
2. Click  Issue Token.
3. Select the mobile device in the Device Selector.

4. Click Submit. The token is displayed in the list of tokens in the ACM application. Another token is displayed in the HID Mobile Access app.


### Registering a New Mobile Device for an Enrolled Identity

If an identity has swapped devices or if an invitation has expired, you can send another invitation

1. Click  Send Invitation on the Tokens tab.
2. Instruct the identity to follow the steps in the email, including clicking an app store link to install the HID Mobile Access app and then clicking the invitation code link to enroll.

### Searching for HID Origo Tokens

To search for HID Origo tokens that were issued, or are being issued, to identities

1. Select  Identities > Identities.
2. Use Identity Search to find an identity.
  - In Search Field, select HID Origo Token Status.
  - In Search Value, select Issued or Issuing. To search for both statuses, leave blank.
3. Click Search.

### Permissions and Rights

The following table describes the permissions and rights the default Enrollment Operator Role allows. All roles are made up of delegations. Each delegation is made up of rights.

#### Permissions :Rights

- Add new identities. Cannot update fields after initial identity setup.
  - Identities My Account
  - Identities Listing Identities Show
  - Identities Advance Search
  - Identities Date Search
  - Identity Profiles Listing
  - Identity Profiles Show List
  - Identities New
  - Identities Create
  - Identities Edit
  - Identity Profiles Populate Values
- Force the identity to change the password at the next login to the ACM system.
  - Force Password Change
  - Add, modify, and update available roles
  - Identities Roles List Identities Roles Update

**Note:** The Stop Dates on the Role page and Role Report are different due to the UTC (Coordinated Universal Time) time server difference.

For example, 12/31/2037 23:59:59 is displayed in the former and 01/01/2038 23:59:59 is displayed in the latter. In ACM 6.18 and later releases, there is no stop date for the role that has Never Expire enabled.

## Permissions Rights

- Add, modify, and update tokens
  - Tokens Listing
  - Tokens Show
  - Tokens New
  - Tokens Create
  - Tokens Edit
  - Tokens Update
  - Tokens Set Free Pass Identity Profiles Tokens Listing
- Add and modify groups
  - Identities Groups List
- View assigned access permissions
  - Identities Show Access
- Capture live photos and save
  - Identities Image Capture
  - Identities Image Save
  - Identities Code Image
  - Identities Photo Capture
  - Identity Profiles Show Access
  - Identities Groups Update
  - Add and upload photos
  - Identities Photo Edit
  - Identities Photo Update
  - Identities Photo Render
  - Identities Upload Photo
- View transactional data
  - Identities Transactions
- Print and issue badges
  - Identities Badge Show
  - Identities Badge Screen
  - Identities Print Badge
  - Identities Badge Render
  - Identities Update Badge Preview
  - Identities Update Badge


## External Systems – Defining the Badge Camera for the System

Once all cameras or other imaging devices have been added as part of an external system, you can set which camera to use when creating badges for identities.

1. Select  My Account.

2. Under the Profile tab, select a camera from the Badge Camera drop down list:


- Local Camera — Any camera connected directly to your computer or built into your computer or monitor.
- P-based camera — Any IP-based camera previously connected to your network and added to your ACM system.

3. When you're finished, click  .

- Next time you create a badge, the selected camera is used to take the identity photo.

External Systems – Defining the Badge Camera for the System

## Documents / Resources

  Enrollment Operator Guide <small>Access Control Manager™</small> <small>Version 4.0.0</small>	<a href="#">AVIGILON Access Control Manager Enrollment Operator</a> [pdf] User Guide Access Control Manager Enrollment Operator, Access, Control Manager Enrollment Operator, Manager Enrollment Operator, Enrollment Operator, Operator
--	--

## References

- [A End-to-End Security Solutions | Avigilon \(Openpath & Ava\)](#)

Manuals+.