LENEL OnGuard 2012
Area Access Manager User Guide
# TABLE OF CONTENTS

1.0 AREA ACCESS MANAGER OVERVIEW ........................................... Page 1

2.0 DEFINITIONS .............................................................................. Page 1

3.0 AAM OPERATIONS

| 3.1 | Logging On .................................................................................. Page 3 |
| 3.2 | Change your Password .................................................................. Page 6 |
| 3.3 | Area Access Manager Main Window ........................................ Page 6 |
| 3.4 | View Access Level Assignments ............................................... Page 8 |
| 3.5 | Remove Access Levels from Cardholders .................................. Page 8 |
| 3.6 | Assign Access Levels to Cardholders ....................................... Page 8 |
| 3.7 | Logging Off .............................................................................. Page 13 |

4.0 SERVICE REQUESTS TO SECURITY SERVICES

| 4.1 | Service Level Commitment....................................................... Page 14 |
| 4.2 | How to Submit a Service Request ............................................. Page 14 |
| 4.3 | Blank Access Cards ............................................................... Page 15 |
| 4.4 | PIN Codes ................................................................................ Page 15 |
| 4.5 | Access Levels ......................................................................... Page 15 |
| 4.6 | Batch Load Requests ............................................................. Page 15 |
| 4.7 | Modify Security Device Settings .............................................. Page 15 |
| 4.8 | Request Security Device Report .............................................. Page 15 |

5.0 ANNEXES

| Annex A: Batch Loading of Access Levels .................................. Page 16 |
| Annex B: AAM Reports ............................................................. Page 18 |

This Area Access Manager User Guide is based on the LENEL OnGuard® 2012 Area Access Manager User Guide, product version 7.2.
1.0 AREA ACCESS MANAGER OVERVIEW

1.1 The LENEL OnGuard® 2012 Area Access Manager (AAM) Application allows for the performance of the following three functions:

1.1.1 Assigning access levels to cardholders.

1.1.2 Removing access level assignments from cardholders.

1.1.3 Generating reports to determine who has access to your areas.

Note: Area Access Managers alone are responsible for this. Except for batch loads, do not contact Security Services to assign or remove access.

1.2 There is a daily data exchange between Banner and LENEL to ensure that the information in LENEL is up to date. New students, staff and faculty members are uploaded and departing persons are removed as <active> McGillians. AAMs should report any missing records or problems accessing their system account to McGill Security Services (398-4562).

2.0 DEFINITIONS

2.1 Access Levels – detail the rights granted to individuals to access areas via card readers. Access levels can be linked to schedules, and card readers can have more than one access level associated with them.

2.2 Area Access Manager (AAM) – a designated person within a department or faculty responsible for managing its card reader(s) by assigning and removing cardholder access to their areas and establishing and modifying card reader settings. AAMs receive specific training from Security Services. An AAM is distinct from a subscriber although the same person can assume the responsibilities for both. See also <Subscriber>.

2.3 Badge - a credential used to gain entry to an area having automated access control entry points. See also <Proximity Card>.

2.4 Batch Loading – the assignment of access levels for students is done by Security Services according to rules specified by the AAM. The access levels are assigned for a specified period of time and then they are removed. Since the information is supplied nightly to LENEL by Banner it is not necessary to repeat the procedure in order to detect
newly registered students or recently activated badges.

2.5 Card Only – a setting on proximity card readers that obliges the user to utilize a proximity card with authorized permissions in order to unlock a door. During this setting, the light on a card reader is red.

2.6 Card Reader – is an electronic device that can read a specific identification badge such as a proximity card, verify the access rights associated with that badge and unlock predetermined doors or operate elevators should the access rights be valid.

2.7 First Card Unlock – a feature whereby the door will only unlock if a designated badge is used. This feature is usually used for office or store openings where it is required that a certain person or persons be on site to allow the other employees in.

2.8 Lock or Locked Down - a setting on proximity card readers that locks the card reader to all users regardless of authorized permissions. During this setting, the light on a card reader is red. Only Security Services has the authority to place a card reader on <Lock> mode.

2.9 Mask – a setting whereby the security device remains armed but does not send an intrusion alarm to the Security Operations Centre. See also <Unmask>.

2.10 Operating Hours – refers to the hours when a building, room, or area is open. Where a building, room, or area is on <card only> 24/7, the default operating hours are defined as 08h00-18h00, the daytime working hours of the majority of employees. Operating hours for major academic buildings are generally 07h00–22h00. Operating hours for smaller academic and office buildings are more circumscribed. See also <Silent Hours>.

2.11 Password – a confidential alphanumeric code used to authenticate users when they call Security Services.

2.12 PINs – Personal Identification Numbers can be added as a feature to card readers as an extra measure of security. The latest version of LENEL still does not allow Area Access Managers to enter PIN numbers for readers. To have the PIN number of a cardholder added, a work ticket request must be made to Security Services via the online form.

2.13 Proximity Card - a generic name for contactless integrated circuit devices used for security access. McGill University uses three types of proximity cards: (1) the McGill staff and student card with photo; (2) a blank proximity card for temporary employees and visitors; and (3) the McGill Service Provider ID card for employees of contracted firms working at McGill.

2.14 Silent Hours – refers to the time when a building, room or area is closed and access is
restricted to authorized users only. Where a building, room, or area is on <card only> 24/7, the default silent hours are defined as 18h00-08h00. Silent hours for major academic buildings are generally 22h00-07h00. Silent hours for smaller academic and office buildings are generally more extended. See also <Operating Hours>.

2.15 Subscriber - a faculty, department, or outside agency at McGill University operating a security device. A subscriber representative who manages a card reader is referred to as an Area Access Manager. See also <Area Access Manager>

2.16 Unlock – a card reader or electric lock setting that unlocks the door permitting unfettered access. During this setting, the light on the card reader is green.

2.17 Unmask – a setting whereby the system resumes sending intrusion alarms to the Security Operations Centre. See also <Mask>.

2.18 Users – are members of the McGill community who use, work or study in, or have authorized access to the area protected by the security device installed by the owning faculty or department. Also known as <cardholders>.

3.0 AAM OPERATIONS

3.1 Logging On
Open Internet Explorer and go to the website at https://plenelaam.campus.mcgill.ca/
The link will open up the previous screen:

Sign in using your McGill active directory (AD) credentials.

**Domain\user name:** Enter your e-mail address.
Must be **first.last@mcgill.ca** or **first.last@mail.mcgill.ca**

**Password:** Enter your DAS password

The following window should appear below:

Select the Area Access Manager Application icon and the following window below should be displayed. Click on [Connect].
Some users (depending on which version of Windows you are running) will be asked to sign in again, use the same McGill credentials as before.

You will then be prompted to log on to the Area Access Manager Application (below) with your AD user name and password and click the [OK] button.

You will then be prompted to log on to the Area Access Manager Application (below) with your LENEL user name and password and click the [OK] button.
3.2 Change your Password

It is recommended that you change your Area Access Manager password when you log on for the first time as your given password is generic. Passwords should be changed regularly thereafter.

From the Application menu select Change Password – the following window appears:

![Change Password Window]

Enter your old password and new password in the appropriate fields. Password standards are:

i. passwords cannot be blank;
ii. passwords cannot be the same as the user name;
iii. passwords cannot be LENEL keywords;
iv. passwords should contain numbers and letters; and
v. passwords are not case-sensitive.

A message confirms that you have successfully changed your password. Click the [OK] button.

3.3 Area Access Manager Main Window

Once you log in you will see the Area Access Manager main window. Here you can:

i. display cardholders in a selected access level;
ii. display personal information about a selected cardholder;
iii. select cardholders to be assigned to access levels; and
iv. select cardholders to be removed from access levels.
1. Lists the access levels that can be assigned and removed from a cardholder's active badges.

2. Opens the Access Level Assignment Wizard, which allows you to assign access levels to cardholders.

3. Removes the assignment of the selected cardholder(s) from the access level that displayed in the Access Panel dropdown list. This tab is grayed out until at least one cardholder checkmark is placed next to the name of the cardholder in the listing window.

4. Displays cardholder, badge, and access level information for the selected cardholder record. This button is grayed out until at least one cardholder is selected.

5. Display the current list of cardholders assigned to the selected Access Level.
3.4 View Access Level Assignments

On the Area Access Manager main window in the Access Level dropdown list box, select an access level to display. This box lists all access levels that you have permission to manage. Note: The access levels are set up for you by McGill Security Services.

Cardholders in the currently selected access level will automatically be displayed. Only cardholders with active badges will be shown.

To view All Access on a card, see Annex B.

3.5 Remove Access Levels from Cardholders

You can remove one or many cardholders from an access level.

1. In the Access Level dropdown list on the Area Access Manager main window, select the access level from which you want to remove a cardholder. The current cardholders with that access level are displayed.

2. Select the cardholder(s) from the listing window by clicking on the icon to the left of the last name.

3. Click the [Remove] button, and a warning that says the following will be displayed: “The people selected will have the current access level removed (from all badges). Are you sure you want to continue?”

4. Click the [Yes] button. The currently viewed access level will be removed from the selected cardholders.

3.6 Assign Access Levels to Cardholders

You can assign one or many cardholders to one or many access levels easily using the Access Level Assignment Wizard.

1. On the Area Access Manager main window, click the [Assign] button. The Access Level Assignment Wizard will begin, and the Find People window will be displayed, as on the next page.

2. If you know it, type the McGill ID number to access the person’s profile quickly. Otherwise, specify the search criteria by typing a full or partial entry in the field(s) on which you wish to search. For example: Type “Smith” in the Last Name field to find all records that have the last name that begins with “Smith”. Searches are case
sensitive. The dropdown lists in the Cardholder view contain no information, so use the “Student” or “Staff” tabs to search by other fields that help to refine your search.

a. The Student view displays Faculty and Degree fields, and the Staff view displays Primary Org field. You have the ability to choose students from a particular faculty or staff from one department. Note that the entire faculty name must be entered under the Faculty tab (i.e. “Faculty of Science”, not just “Science”), and the entire degree in the Degree tab (i.e. “Bachelor of Arts”, not just “Bachelor”).

b. Also note that for each view (cardholder, student, and staff) all cardholders are searched. So if you have typed something under Faculty in the Student tab, and then click back on the Cardholder tab, the Faculty entry in the student tab will remain and will be used in your search. Therefore, it is important to remove unnecessary or unsuccessful search terms before searching again.
Always enter at least one search criteria before clicking the [Next] button. If you leave the fields blank all cardholders will be displayed. As there are more than 40,000 cardholders, this search will take a long time. To cancel a search, click the [Cancel] button.

3. Click the [Next] button.
4. If only one cardholder matches your search criteria, continue with Step 6. Otherwise, depending on what you entered as your search criteria, one of the following will occur:

a. If more than one cardholder matches the search criteria, the Select People window will be displayed, as shown below:

![Select People Window](image)

From this list, select the cardholder(s) that you want to assign access levels to by placing a checkmark next to their last name(s). Then click the [Next] button.

b. If no cardholder matches the search criteria you entered, a message will be displayed that says “No people with active badges were found that match your search criteria. Please try entering less specific criteria.” If this happens, enter new search criteria and click the [Next] button.

c. If you entered no search criteria, all cardholders will be displayed in the Select People window. This is not recommended; click the [Cancel] button and refine your search.
5. If you are only managing one access level, continue with **Step 7**. If you are managing more than one access level, the **Select Access Levels** window will be displayed, as shown below. Select the access levels you want to assign to the cardholder(s) you selected in the previous step. You must choose one or more access levels to assign. The currently viewed access level (on the Area Access Manager main window) is selected by default.

6. Click the **[Set Activation Dates…]** button to add an activation or deactivation date to the access level.

7. Select an activation and deactivation date. Once the dates are chosen, click the **[Set]** button and the **[OK]** button in that order, and then click **[Next]**.

8. The **Summary window** will be displayed. If you agree with the summary of the access level that is going to be assigned, click the **[Finish]** button. Upon finishing, the access levels will be assigned to the selected cardholders.
The Personal Information Window

Use the [Personal Information] button to display details about a selected cardholder, including the picture that appears on their McGill ID card. This button is found on the Area Access Manager main window and on the Select People window. Alternatively, you can double-click on a person’s name to see the Personal Information window.

3.7 Logging Off

1. Select Log Off from the Application menu. All open data entry forms will be closed. The main window will open again as it did before you logged in and most of the toolbar and menu options will be dimmed.

2. Select the Exit choice from the Application menu.

3. Close your Remote Desktop session. Please do not forget this step as we have a limited number of licenses.
4.0 SERVICE REQUESTS TO SECURITY SERVICES

4.1 Service Level Commitment

Please refer to our online Service Level Commitment document which details the service support we provide. Please note that some services are considered supplemental and are billable.

4.2 How to Submit a Service Request

Go to: http://www.mcgill.ca/security/services-0/access-control/area-access-manager-section

Service requests to Security Services should be made using the online forms found on our website. You will have to logon to authenticate yourself. Please allow for at least two business days to process the request. Emergency service requests can be made by calling 398-4562 between 08h30-17h00.

If you are not sure which form to use, please use the <Other> form.
4.3 Blank Access Cards

Blank Access Cards can be ordered via our online forms. For guidance on their employment, please refer to the Terms and Conditions of Use document available in the <Access Control> section of the Campus Public Safety website.

4.4 PIN Codes

For Card Readers with PIN pads. AAMs can set or reset pins via the Request <Modify Card Holder Information> online form found on our website.

4.5 Access Levels

Use this form to submit requests to add or modify LENEL access levels. Remember, card readers can have more than one access level associated with them and access levels can have time restrictions placed on them.

4.6 Batch Load Request

Use this form to submit requests to add or modify a batch load. For more information about batch loads, please refer to Annex A.

4.7 Modify Security Device Settings

Use this form to modify opening and closing hours, alarm monitoring hours, etc. Please be specific as you can when identifying the security device whose settings need to be modified.

4.8 Request a Security Device Report

For reports you can produce on your own, please refer to Annex B.

Some restricted areas, especially where government regulatory compliance is in force, reader reports can be provided on a regular basis. For all other areas, requests for reader reports must be accompanied by the reason for the report. Requestors should include as many relevant details so that we can approve the request without delay. This is to prevent possible misuse of a security device. For example, reader report requests will not be approved if the requestor intends to use the report to confirm payroll hours or work attendance. This requires approval from Human Resources. Similarly, reader report requests will not be approved if the requestor intends to use it for a criminal investigation as this is the purview of Security Services.
Batch Loading of Access Levels

Bulk updating of student access levels onto the LENEL OnGuard system is possible depending on specified criteria (see below). Access will be generated and removed according to dates provided.

Manually assigned access levels will not be affected by the batch loading. It is important to note that access assigned manually has to be managed carefully by the AAM. Manually assigned levels will stay on a cardholder’s card until the card is no longer valid if no end date is assigned.

Please note that should the AAM want to revoke the access of a student to his/her building or lab, the access may be removed manually. However, the system will reinstate the access when there is any LENEL-related change made to the student’s Banner record.

Batch loads go into effect at the beginning of the Fall, Winter and Spring/Summer semesters. Security Services will inform AAMs to submit their Batch Loading – Access Levels Form by mid-August. Once the batch loads are programmed, the AAM will receive an e-mail confirmation. Security Services will enter the rules into Banner and the following night the access levels will be automatically assigned to the selected group.

Currently the types of rules are:

i. the student’s campus;
ii. the student’s faculty;
iii. the student’s department and graduate/undergraduate status; and
iv. the student’s course.

Below, you will find an example for each rule:

<table>
<thead>
<tr>
<th>RULE TYPE</th>
<th>SELECTION</th>
<th>ACCESS LEVEL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Student’s campus</td>
<td>Macdonald</td>
<td>Macdonald Campus Staff/Students</td>
</tr>
<tr>
<td>Student’s faculty</td>
<td>Faculty of Arts</td>
<td>EMF Labs, Staff Access Always</td>
</tr>
<tr>
<td>Student’s department</td>
<td>Physics</td>
<td>Meakins, Main entrance/ LAB219, Access Always</td>
</tr>
<tr>
<td>Student’s course</td>
<td>ECSE210</td>
<td>McConnell Eng Rm 502, Access Always</td>
</tr>
</tbody>
</table>

The date the rules are set and the term that the student is registered will affect which access levels are generated.
Security Services will use default dates unless the AAM requests otherwise. Fall dates must be between August and December inclusive, winter dates must be between January and June inclusive, and summer dates must be between May and September inclusive. Each pair of set dates must fall within the same calendar year.

<table>
<thead>
<tr>
<th>FALL</th>
<th>WINTER</th>
<th>SUMMER</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sep 01, 2006 to Dec 22, 2006</td>
<td>Jan 02, 2007 to Apr 30, 2007</td>
<td>May 1, 2007 to Aug 31, 2007</td>
</tr>
</tbody>
</table>

LENEL Batchload Request

Use this form to submit requests to Add/Modify Batchload

Contact Information

McGill ID

Full Name

McGill Email

Phone

Batchload parameter: Complete only the fields required:

Name of batchload to create/modify

Is this a new or existing batchload: New

Define Batchload conditions:

Faculty

Department

Course

Residence

Card readers associated

Please ensure you fill in the fields above correctly to avoid a delay in processing your request.

Question / Message

Submit
AAM Reports

AAMs can run access reports to see which cardholder has access to their area(s).

1. From the View menu, select Reports. You will get the following pop-up:

   ![AAM Reports Pop-up](image)

   - Select the **[Access Level Assignments to Cardholders]** by placing a check in the check-box. (**Note**: both types of reports available will provide the same information as the system has not been divided into segments).

2. Click the **[Preview]** button. Please wait while the report is generated.

3. Once generated, the report will appear. AAMs can choose to export these report to other formats using the export button found at the top left corner of the main window. An export window will appear.
5. In the format field, select the file format you would like to generate. In the destination field, select [disk file] and click [OK]. An export option window will appear. Click [OK].

6. You will be prompted to select a destination to save the file. Under Computer, select [C on Computer Name]
7. Then double-click on [Users] (Windows 7) or [Documents and Settings] (Windows XP).

8. You can then double-click on your DAS McGill username and then choose where you would like to save the report on your computer (i.e. Desktop, Documents, etc.).
AAMs can run access reports to see which access level is on a cardholder.

1. From the View menu, select Reports. You will get the following pop-up:

   ![Report Menu](image1)

2. Select the **[Access Levels by person for AAM]** by placing a check in the check-box.
3. Click the **[Preview]** button. Please wait while the report is generated. You will then be prompted to enter parameter of your search:

   ![Enter Parameter Values](image2)
4. Enter the information in both field (Key sensitive) and click the [OK] button to generate the report.  
(If you are not sure on how the name is written, you can enter a minimum of 2 letters for each field).

Take note:

1. When you select the report [Access Levels by person for AAM] - click on [Preview] and click [cancel]; This causes an issue where you cannot select any buttons as it is greyed out.

2. To bypass this issue. Click on another report, for example [Access Level Assignments to Cardholders]. Click the [Preview] button. Close the report [X]. You should now be able to select the [Close] button in the Reports screen.

SECURITY AND SAFETY ARE EVERYONE’S RESPONSIBILITY