The Implementer’s Role

A KMS v2.x Software Perspective
### Contents

**Introduction** .................................................................................................................................................. 4

1. **KMS v2 Concepts................................................................................................................................... 5
   1.1 **Profiles ................................................................................................................................................ 5
   1.2 **Control Groups .................................................................................................................................... 5
   1.3 **Profile Groups ..................................................................................................................................... 6
   1.4 **KMS Facility Objects ............................................................................................................................ 7

2. **The KMS v2: The Software .................................................................................................................... 8
   2.1 **General Concepts ................................................................................................................................ 8
       2.1.1 **User Interfaces ............................................................................................................................. 9
       2.1.2 **Notes .......................................................................................................................................... 11
       2.1.3 **Security ...................................................................................................................................... 11
       2.1.4 **User Creation ............................................................................................................................. 12
       2.1.5 **User Roles .................................................................................................................................. 12
       2.1.6 **Communications ........................................................................................................................ 13
   2.2 **What’s Available to You .................................................................................................................... 14

3. **Implementer Tools .............................................................................................................................. 15
   3.1 **Control Groups .................................................................................................................................. 15
       3.1.1 **Creating Control Groups ............................................................................................................ 16
       3.1.2 **Editing Control Groups ........................................................................................................... 17
       3.1.3 **Managing Implementer Membership ........................................................................................ 18
   3.2 **Profile Groups ................................................................................................................................... 19
       3.2.1 **Creating Profile Groups .......................................................................................................... 20
       3.2.2 **Editing Profile Groups ............................................................................................................ 21
       3.2.3 **Managing KCC Membership .................................................................................................... 22
       3.2.4 **KCCs and KMS Authorizations ................................................................................................. 23
   3.3 **Profiles .............................................................................................................................................. 24
       3.3.1 **Creating Profiles ......................................................................................................................... 25
       3.3.2 **Editing Profiles ........................................................................................................................... 28
       3.3.3 **Viewing Profiles ......................................................................................................................... 29
       3.3.4 **Deleting Profiles ......................................................................................................................... 30
       3.3.5 **Managing Profile Group Memberships .................................................................................... 31
Introduction
KMS v2 is a multi-threaded web-based application provided and managed by the Cornell University Police Department’s Access Control Group. It provides facilities for documenting, auditing, and monitoring profile and key data. It is imperative that both profile and key data be managed from the moment of inception throughout their full life cycle, thereby maintaining a reliable chain of custody. Thus, the Implementer role is a vital cornerstone upon which the university’s key management strategy is built.

This document attempts to outline the role played by lock shop staff within the University’s key management strategy from the perspective of the CUPD’s software solution; Key Management System (KMS) v2.0

The Implementer’s role involves the definition and management of key profiles as well as the physical instantiation of the profiles as keys. Profiles record the blue print that defines the attributes that describe the actual cut of the physical keys. Once keys have been cut and recorded in KMS v2, they are then free to be assigned to Key Control Coordinators (KCC), who will then be responsible for the final disposition of the instances, whether assigned to a university key holder or stored for future use.

In the following sections we’ll explain a bit about some of the newer concepts that are unique to the v2.x series of KMS. We can then take a more in-depth look at how best to leverage these tools to assist you in your efforts to create and manage the University’s physical keys and their chain of custody.

A note on context and presentation...
The interfaces shown and described within this manual are those most common to an individual running KMS v2 under the Implementer role. Other handouts may deal with different roles which will often present information differently; depicting more or less functionality.

Versions and Relevance...
This document and the information contained within were considered accurate and up to date as of KMS v2.0.18a.
1. KMS v2 Concepts
Whether you are new to KMS, or you have experience with the original KMS v1 series; there are a few concepts unique to KMS v2 that will be new to you. The following sections will talk about some core KMS v2 functionality that was specifically designed to make the Implementer’s responsibilities easier to manage with less work. The following is strictly to introduce you to the concepts; later in the document we will talk more in-depth about how to leverage this functionality.

1.1 Profiles
Profiles are at the heart of everything an Implementer does in KMS v2. It is unlikely that this is a new concept for you as an Implementer, but we want to say a few words about what we mean when we are talking about a KMS v2 profile.

As described above, profiles are essentially the blueprint from which we instantiate cut physical keys. You could think of this a recipe that tells us how to perform the cut. A profile is expressed via the following data points:

- Lineage title (Master, Sub-Master, etc)
- Manufacturer
- Keyway
- Keyset
- Biting
- A secure flag (on or off)

1.1.1 A word about profile lineage...
Profiles can be based on a parent profile and may be used as a basis for a child profile. Thus, profiles are ideally expressed as a family tree, depicting these relationships at a glance. Each generation can also be described by a title. As an Implementer, you are free to establish the relationships between the profiles you need to record; the titles available to you are:

- Control
- Great Grandmaster
- Grandmaster
- Master
- Sub-Master
- Sub-Sub-Master
- Change

1.2 Control Groups
As an Implementer, the profiles you create are owned by you, are accessible by only you, and can be instantiated into keys by only you. However, we recognize that this can be a daunting task for those managing large numbers of profiles. In KMS v2, you have the ability to grant access to all or some of your profile trees via a new construct: the KMS control group. Any Implementer granted access to a
control group is granted full managerial access to all profiles the group has access to. In this way, your organization is free to employ as many or as few Implementers to manage your profiles trees as makes sense for your individual situation. Implementers are free to create control groups on the fly; thus organization models can be as rigid or as flexible as one can imagine.

It bears mentioning that Implementers must belong to at least one control group. When first entering the system, you will be redirected to the Control Group Manager until you create or are placed into a group.

1.3 Profile Groups
Being introduced for the first time in KMS v2, Profile Groups are the primary organizational unit to be employed by Implementers. The groups serve a couple of purposes:

First, profile groups are owned by control groups. When profiles are created, they are placed in at least one profile group for management. You might imagine an organizational structure such as:

a. Control Group: CIT
   o Profile Group: Rhodes
   o Profile Group: CCC
   o Profile Group: 120 Maple

Under this simplistic example, profiles created to serve Rhodes Hall would be placed in the ‘Rhodes’ profile group, Computer & Communications Center profiles into the ‘CCC’ group, and so on. Note that profiles may belong to more than one profile group, thereby allowing for more complex organizations.

The groups serve a second important purpose; it is through profile groups that you will grant access to Key Control Coordinators (KCCs). KCCs will have full managerial access to all keys instantiated from profiles belonging to their assigned profile groups. KCCs can also belong to multiple profile groups.

In its simplest form, this organization might look similar as to that depicted in FIGURE 1 or as complex as in FIGURE 2.

![Figure 1](image.png)
1.4 KMS Facility Objects

Facility Objects (FO) are a core element of KMS v2. FOs are used to accurately describe and define access and storage locations. The objects are directly related to university facilities, and optionally, rooms. The intent is to aid you in better cataloguing exactly what a key opens or exactly where it is stored (or both).

While the FO system is not an optional component of KMS, it is designed to be non-intrusive for those that do not wish to leverage the functionality. Each facility comes with a NULL object and every room is pre-populated with a generic Door object. Thus, if all you wish to capture is the facility and room, you may do so. On the other hand, if you wish, the system can also accommodate very precise record keeping; have a key stored in an envelope, taped to the inside of the bottom-right drawer of Bob’s desk in room 245 in EHOB? Easily managed!

The facility Object system is designed to be community managed. That is, anyone with a business need in KMS v2 has access to define and edit objects. New objects created, are by default, publicly editable and accessible by the community as a whole. However, you can override this behavior, locking objects so only you can edit them, or even so only you can see them.
2. The KMS v2: The Software

In the following sections, we’ll explore the specific tools made available to you via KMS v2 which are designed to assist Implementer’s in their efforts to fulfill the responsibilities placed upon them. We’ll review the general system, then take a closer look at specific offerings so as to describe how best to use them to achieve desired goals.

2.1 General Concepts

KMS v2 is a fairly substantial offering. Before getting into the various Implementer specific tools, we should examine some of the more general aspects of the software; concepts and functionality that should feel the same regardless of which part of the package you are currently using.

KMS v2 was specifically written and designed to behave in much the same way as most software that you have been using for many years. When you first log in, you will be presented with a rather benign interface such as depicted in figure 3. Navigation along the top edge compartmentalizes functionally independent areas, while the menu down the left-side offers various options for the module or tab you are currently viewing. The yellow banner running along the top is a system message that may be presented to you when KMS administrators feel the need to communicate with the community.

![Figure 3](image-url)
Taking a closer look at the navigation...

1. **Tabs**: different KMS roles will have access to different modules of functionality. Clicking on a tab will load that module with its options listed on the left and the main interface loaded on the right.

2. **Show/Hide Menu**: due to KMS’ data needs; some of the displays may be fairly wide, scrolling to the right. Clicking this button will hide the menu giving you additional screen real-estate to work with.

3. **Account verification**: Once logged in, you should see your name followed by your KMS role (more on roles in a bit). This serves only as a visual confirmation of the credentials under which you are currently logged in. KMS makes use of Cornell University’s CUWebAuth tools for single sign on authentication. A visual cue of your credentials is especially useful in areas where computers are shared.

4. **Module Options**: the rest of the left column is dedicated to the module navigation menu. Selecting links on the left should load interfaces on the right. These options will change from tab to tab.

2.1.1 **User Interfaces**

While there are a few exceptions, most interfaces will work the same; regardless of which tool you are running. You’ll be presented with a list-based display of relevant data, filters to help sort through the information, and buttons that will launch small dialogues; each designed to operate specifically on the data at hand. An example of one of these manager displays can be seen in FIGURE 5.
For example, before you could filter the display to show you only the profiles within a specific profile group, you would first need to select a control group, so that the filter will understand which profile groups are relevant to your request.

*Note that while the dialogues are separate windows of functionality, they are not traditional pop-up windows and will not be affected by modern browser pop-up protection.*

One of the primary design principles behind the development of the KMS v2, was to put as much useful data as possible at the user’s fingertips without cluttering the display or negatively impacting performance. As such, there are a lot of little displays that can be discovered when your mouse hovers over specific data points. When viewing a manager display for the first time, we encourage you to move your mouse around to explore and learn about the additional information that is available to you.
2.1.2 Notes
KMS v2 employs a new flexible note system that allows you to attach a note to virtually any data element you come across. If working in groups, you can access and edit each other’s notes, or if need be you can restrict access to yourself. Each dialogue will provide you with the opportunity to attach a note to whatever element you happen to be working with (key, user, profile, group, etc).

Each managerial interface will include a column with a folder icon which denotes the presence of notes on that specific element; allowing your mouse to hover over the icon will tell you how many. Clicking the icon will expand a hidden menu of notes that have been attached to the element.

The notes are presented as a list, with the first sixty-four (64) bytes of the message displayed. If you move your mouse to hover over one of the notes, the full message will appear in a tool tip. Clicking the note at this point will launch the note editor with the message loaded for editing.

![Figure 8: Profile Manager with Notes list expanded](image_url)

2.1.3 Security
The KMS v2 suite of tools assumed a strong security posture early on in its development cycle. Virtually all functionality is tied to appropriate security measures intended to ensure the quality of the data taken in, and to protect that data from without. If you are an experienced user of the internet, you may be accustomed to taking certain liberties or short cuts with web-based software; these practices will be discouraged, and more often than not will garner you a KMS Security Error display.

As part of the KMS v2 security package, an extensive auditing practice was employed. That is to say, the software logs most every action taken via the user interface. We utilize these logs in our endeavors to
provide end-user support, development debugging information, and when appropriate, an investigative tool when security-related issues arise.

While the data being stored and managed by KMS v2 would not likely meet the criteria of confidential data, as defined by the university; it is our goal to provide a tool that meets or surpasses the minimum requirements for fitness of purpose of its mission as a university auditing tool.

2.1.4 User Creation
Currently, KMS v2 does not support explicit user creation functionality (though a user management module will be forthcoming). Instead, the process is automated in many places throughout the application where you will see a Cornell NetId solicited.

When you type a Cornell NetId into any of the KMS v2 ‘KMS User’ fields found on many dialogues, the system attempts to locate that user in the KMS v2 database. If he exists, the user is loaded into memory and your requested action can complete.

If the user is not in the database, the system then looks for him in the Cornell directory. If found, the user is loaded into memory, a KMS User account is created, and the new account is given sufficient access to meet the needs of your request.

Note that at the point of creation, the user is assigned a role based on the action you are attempting to complete. As noted above, if it is a new user and you are adding him to be a KCC, then he will be given the KCC role. If he is an existing user, the system will evaluate whether or not his current role is sufficient to meet the needs of the current operation, and make appropriate adjustments. For example, if you add a KCC to a control group, the system will elevate his role to Implementer. If you remove a user from a group, their role is reduced to the highest required level to meet the needs of their remaining assignments.

2.1.5 User Roles
KMS v2 chose not to employ a comprehensive permissive system. We felt that the business rules embodied somewhat of an implicit authorization component within the many possible assignment structures. That is to say, a KMS user is authorized to perform certain activities by assigning them to groups; key groups (for AKCCs), profile groups (for KCCs), and control groups (for Implementers).

As such, it is entirely possible for you to be added to the system as an Implementer, authorized to act as the KCC for another group, an AKCC for yet a third organization, and so on. Within this model, the KMS roles are compounded together and evaluated each time you attempt to utilize any functionality with the highest level of relevant access determining whether or not you may proceed.
While the above example is likely to be rare, if it ever exists at all, it is worth noting that the manager displays are generated within the context of your KMS Role. This means, that while you may have access to the Key Manager because you have been authorized as a KCC, the displays may show more information than a KCC typically sees if your primary role is actually Implementer. However, you will never have access to less data than you need; your primary role is automatically elevated and reduced as your current assignments warrant.

*It is important for you to keep in mind that you are granting authorization when you assign a user to a group.*

2.1.6 Communications
There will be times when communications will be sent to you from KMS in the form of electronic mail. We are conscious of issues surrounding unsolicited communications, and thus do not arbitrarily send a multitude of notices. However, the ability of KMS v2 to monitor and report on the data it is responsible for is what transforms KMS v2 from a static inventory into a rich dynamic data management system.

A monitoring package was developed to run in parallel to KMS; modules (or “monitors”) can be quickly defined and dynamically added to the KMS environment without interruption of daily business. As of this writing, there are currently two (2) such monitors defined and installed in the KMS v2 environment:

The Delayed Transit report
The typical key instance will spend the vast majority of its life span as either assigned to a key holder or in storage. There are a few exceptions to this rule where a key may be marked as “In Transit”. The transit status is intended to be a temporary state. If a key instance is in the transit state for more than five (5) days, a notice will be generated and sent to the responsible KCC, once a day until such time as the keys state is changed to a more suitable one (again, this would typically be assigned or stored).

The Overdue Keys report
Every night, a monitor will run that will look for keys that have gone overdue. A digest report is built and sent to the assignor of the keys informing them of the change in state. This is not an ongoing ‘harassment’ report; it is sent only once on the day the state changes; you will not be notified a second time that the keys have not been returned.
In addition to the above monitors, there are also a couple KMS v2 processes that yield a communication:

**Lost Keys & Key Rings**
If a key holder reports a key or key ring as lost, an email is sent to the individual that assigned the key.

**Found Key or Key Ring**
If a previously reported lost key or key ring is recovered, you can optionally elect to notify the members of your key group (including the KCC) that the key has been found and is back in the system waiting to be managed.

### 2.2 What’s Available to You
The rest of this manual is dedicated to describing the various tools made available to you as an Implementer and also as a community member. Your position as an Implementer will largely drive the options you will see on your menu. These will include:

- **Control Group Manager**, allowing you to add and manage control groups.
- **Profile Group Manager**, adding and managing profile groups as well as KCC membership.
- **Profile Manager**, adding and managing profiles as well as the many features of profiles.
- **Key Review**, review and edit the key instances you have instantiated from your profiles.
- **Profile Searches**, a more elaborate filter set for tunneling into the profile data sets.

Additionally, there are a couple of other tools made available to all KMS community members such as an inventory of keys assigned to you as an employee, and the Facilities Object editor.
3. Implementer Tools

In the following sections, we will be taking a closer look at the tools available to implementers, including procedures in the expected use of the software. It is from this point forward, that you might consider this document to be the Implementer’s software user manual.

The following sections are provided in the order that we expect an Implementer to need the tools. If you need any assistance with the following material, or even if you just have ideas on how to make this a better manual, please contact us by email at: acg-support@cornell.edu

3.1 Control Groups

As you are likely aware at this point, control groups are a required organizational unit for implementers that serve the dual purpose of authorizing implementer access to a defined domain of profiles. Control groups should be considered to be the highest organizational structure in KMS v2. The name you select should reflect the nature of the group: Central Lock Shop, College of Engineering, NYC Campus would be examples of the level of organization to which we are referring.

*Implementers must belong to at least one control group before they will be allowed to work with any profiles. If you enter KMS v2 before you’ve have joined a control group, you will be continuously redirected to the control groups manager until you create a group or are added to one.

To begin working with control groups, Enter the Control Group Manager by locating the link Manage Control Groups on the left-hand navigation menu under the Keys tab. Once the manager has loaded you should be faced with a list of all control groups to which you have access (or, it may be empty if you are just starting out).

![Figure 9: Navigate to control group manager.](image)
3.1.1 Creating Control Groups

Once you have entered the control group manager, look to the bottom of the list; there, aligned right should be a series of buttons. Locate the button titled Add Control Group and click it. This will launch the Create New Control Group dialogue.

At a Glance …

You are likely noting at this point that control groups are fairly simple constructs defined by only two data items: a name and a default profile group.

- **Names** are unique across the scope of the enterprise. Since you can only see groups you have access to, it is possible that you’ll be told your name is not unique and must be re-defined.
- **Names** must be between one (1) and sixty-four (64) characters in length and may only include alpha-numeric characters and the following symbols: - _ : . / \  
- **Default Profile Groups** have a system-wide default name: Unassigned Profiles. You can edit this name if you so choose. Bear in mind that profile group names are unique across the scope of the control group. The name must also follow the same character rules as control groups.

To create the group:

1. **LAUNCH** the dialogue as described above.  
2. **TYPE** a name for the control group.  
3. Optionally, **TYPE** a new profile group name.  
4. Optionally, **TYPE** any note you would like to add  
5. Optionally, **CHECK** the Restricted Note checkbox if you would like the note to be viewable by only you.  
6. **CLICK** Continue  
7. On the confirmation page, review your new group details.  
8. If you approve of the settings, **CLICK** Submit.  
9. If a mistake was made, **CLICK** Previous and edit the settings, resuming this process with **STEP 6**.

Figure 10: Creating a new Control Group
3.1.2 Editing Control Groups

Editing an existing control group is as easy as defining a new one. To edit an existing group, enter the control group manager to view the list of available groups. Once you have identified the group you wish to edit, SELECT the checkbox located in the far-left column of the list display. Having selected the group, locate the button labeled *Edit Control Group* and CLICK it.

You should now be faced with a dialogue similar to the one in **FIGURE 11**. You’ll note two differences in this dialogue as compared to the creation one:

The *Active* flag indicates that the group is still in use and will still appear in any user interface element in which control groups are listed. If you deselect this flag, you will, for all intents and purposes, delete the group. Don’t worry though, the group is still in KMS and can be brought back up and re-activated at any time.

*Default Profile Group* option is now a menu consisting of all profile groups currently owned/managed by this control group. You can change which group serves as the default by simply selecting a new one from the list.

**To edit the group (all fields are optional):**

1. **LAUNCH** the dialogue as describe above.
2. **EDIT** the *Name* of the group, being mindful of the rules for group names defined in **SECTION 3.1.1**
3. Enable or disable the group by **SELECTING** or **DESELECTING** the *Active* checkbox.
4. **SELECT** a new profile group to serve as the default, from the *Default Profile Group* menu.
5. **TYPE** any *Note* you would like to add to the group regarding this edit.
6. **SELECT** or **DESELECT** the *Restricted Note* checkbox if you would like the note to be viewable by only you.
7. **CLICK** *Continue*
8. On the confirmation page, review the changes to your group.
9. If you approve of the changes, **CLICK** *Submit*.
10. If you wish to make additional changes, **CLICK** *Previous* and edit the settings, resuming this process with **STEP 7**.
3.1.3 Managing Implementer Membership

As mentioned previously, if you are the creator of the group, then you will be automatically added as a member. If you do not create the group however, then you must wait for someone to add you to it. In this section we’ll discuss how to manage the users you wish to add to or remove from the group.

*Note, when you add a user to a control group, they receive the same level of authorization as you; even over the group itself! Always be mindful of your changes before committing them.

This dialogue functions a bit differently than what you have seen so far (and differently than most others). KMS sports two different models in its dialogues, the simple forms that you have seen already, and what we refer to as the accumulator model. In these types of dialogues, you never leave the main page; changes happen instantly as you make them with the dialogue updating to reflect those changes.

The Implementers menu lists all Implementers that currently have access to your group.

To add a user to the group:

1. **TYPE** a Cornell Net Id into the KMS User field. The user does not have to be a KMS user, but they must have a Net Id.
2. **CLICK** Commit, you should see the user moved up to the Implementers menu.

To remove a user from the group:

1. **SELECT** one or more users in the Implementers menu.
2. **CLICK** Commit, the user should disappear from the menu.

Figure 12: Managing implementer group access

*Note that you can add and remove users at the same time. When you click Commit, the system will remove anyone highlighted in the menu and add anyone in the KMS User field.
3.2 Profile Groups

KMS v2 profile groups are the second level of organization available to Implementers. Profile groups are owned and managed by the control group in which they were created. In keeping with the previous example where we named a control group *Central Lock Shop*, you might further organize your groups to reflect buildings, zones, or any other structure that makes sense to your business model.

The important thing to be mindful of when creating your profile groups is that they also serve as the authorization tool for Key Control Coordinators (KCC). When you add a KCC to a profile group, they receive full managerial rights to any key instance that was cut from profiles managed by this profile group.

To get started with profile groups, locate and click the link *Manage Profile Groups* located on the left-hand navigation menu. On the right of the interface, you should now be faced with a list-based display similar to:

![Figure 13: Profile groups managerial interface](image-url)

Figure 13: Profile groups managerial interface
3.2.1 Creating Profile Groups
Once you have entered the profile group manager, look to the bottom of the list; there, aligned right should be a series of buttons. Locate the button titled Add Profile Group and CLICK it. This will launch the Create New Profile Group dialogue.

This dialogue will likely look familiar as there is little difference between creating a control group and a profile group.

At a glance...
- A Ctrl Group must be selected as the owner of the profile group.
- Names are unique across the scope of the control group that owns the profile group.
- Names must be between one (1) and sixty-four (64) characters in length and may only include alpha-numeric characters and the following symbols: - _ : . / \
- The Default Group flag allows this new group to take over as the parent control group’s default profile group.

To create the group:

1. LAUNCH the dialogue as described above.
2. SELECT a control group from the Ctrl Group menu.
3. TYPE a Name for the new profile group, observing the rules defined above.
4. Optionally, SELECT or DESELECT the Default Group flag.
5. Optionally, TYPE any note you would like to add.
6. Optionally, CHECK the Restricted Note checkbox if you would like the note to be viewable by only you.
7. CLICK Continue
8. On the confirmation page, review your new group details.
9. If you approve of the settings, CLICK Submit.
10. If a mistake was made, CLICK Previous and edit the settings, resuming this process with STEP 7.
3.2.2 Editing Profile Groups

To edit an existing group, enter the profile group manager to view the list of available groups. Once you have identified the group you wish to edit, select the checkbox located in the far-left column of the list display. Having selected the group, locate the button labeled Edit Profile Group and click it.

You’ll note three differences in this dialogue as compared to the creation one:

The Active flag indicates that the group is still in use and will still appear in any user interface element in which profile groups are listed. If you deselect this flag, you will, for all intents and purposes, delete the group. Don’t worry though, the group is still in KMS and can be brought back up and re-activated at any time.

Default Profile Group flag allows you to take over as the control group’s default, or relinquish that role.

The New Default menu is a list of all profile groups owned by the parent control group. If your group was the default, and you elected to give that up, you must select another group to take over that role.

To edit the group (all fields are optional):

1.-launch the dialogue as described above.
2. edit the name of the group, being mindful of the rules for group names defined in section 3.2.1
3. enable or disable the group by selecting or deselecting the Active checkbox.
4. take over as or relinquish the default profile group role by selecting or deselecting the Default Group checkbox.
5. select a new profile group to serve as the default, from the New Default menu if you elected to relinquish the role with the current group.
6. type any Note you would like to add to the group regarding this edit.
7. select or deselect the Restricted Note checkbox if you would like the note to be viewable by only you.
8. click Continue
9. on the confirmation page, review the changes to your group.
10. if you approve of the changes, click Submit.
11. if you wish to make additional changes, click Previous and edit the settings, resuming this process with step 8.
3.2.3 Managing KCC Membership

As mentioned previously, profile groups serve as the authorization mechanism for Key Control Coordinators (KCC). KCCs added to profile groups will receive full managerial access to all keys which have been instantiated from profiles managed by the profile group.

*Note, when we talk about “authorization” within the current section, we are talking about authorization as opposed to authentication, a security concept; while not immediately relevant, the distinction will be an important one. See SECTION 3.2.4 for details concerning KCCs and KMS Authorizations.

To manage KCC memberships:

The KCC membership management dialogue functions similarly to the Implementer group manager discussed in SECTION 3.1.3. The dialogue is of the accumulator model, meaning all updates happen instantly without confirmation and without leaving the initial page.

The KCCs menu lists all KCCs that currently have access to your group.

To add a user to the group:

3. **TYPE** a Cornell Net Id into the KMS User field. The user does not have to be a KMS user, but they must have a Cornell Net Id.

4. **CLICK** Commit, you should see the user moved up to the KCCs menu.

To remove a user from the group:

3. **SELECT** one or more users in the KCCs menu.

4. **CLICK** Commit, the user should disappear from the menu.

![Figure 16: Managing profile group access for KCCs](image)

*Note that you can add and remove users at the same time. When you click Commit, the system will remove anyone highlighted in the KCC menu and add anyone in the KMS User field.
3.2.4 KCCs and KMS Authorizations

When you add a new KCC to a profile group, he will likely not have immediate access to the contents of the group. There exists another authorization component within the Cornell University bureaucracy that is out of scope for the KMS tools. That is to say, the true authorization happens outside of the software.

When authorization has been approved and granted, a KMS Administrator will authorize the assignment you made. Note that we are specifically authorizing the assignment to the profile group. However, the university authorization is being made on another level, which may cause some confusion.

Example:

Bob is authorized by the Dean of the College of Engineering to administer keys. You create a profile group CoE and assign Bob. The KMS Administrators validate the authorization and authorize the assignment; Bob should now see the profile group CoE in all of his displays and can now administer the group.

However, if you should decide for some reason that you need a new profile group that is within Bob’s purview and you create: CoE-Facil and then add Bob to it. Bob would again need to be authorized for the new assignment even though he has technically been authorized by the University bureaucracy.

There is a module slated for some time in 2014 which will automate much of the University authorization piece, but until then, you’ll simply have to make the assignment and then contact a KMS Administrator to complete the process.

You can however monitor the status of the assignment via the Profile Group Manager interface. Look for the group you recently made an assignment to, and then hover your pointer over the icon in the KCCs column. You should see something like that depicted in Figure 17:

The shield icon next to Curtis’ name indicates that his assignment has been authorized and he should have full access.

The hour-glass icon next to Eric’s name indicates that authorization for his assignment is still pending.
### 3.3 Profiles

KMS profiles are at the heart of everything an Implementer does. All of the tools you have seen so far, as well as those to be detailed later in this document, all exist to support profiles in one way or another.

While it isn’t strictly necessary, we’ll suggest that you have put some thought into your organizational structure and have profile groups created and waiting to be used prior to starting to work with profiles.

To get started with profiles, locate and click the link **Manage Profiles** located on the left-hand navigation menu. On the right of the interface, you should now be faced with a list-based display similar to:

![Figure 18: Launching the profile manager interface](image)

As with all of the managerial interfaces, we’ll encourage you to move your mouse around; there is quite a bit of information to be found in various tooltips. The main interface should provide you with most everything you will need to work with and effectively manage profiles. We’ll discuss the options in detail in the following sections, but at a glance, you will be able to:

- View profile details and vital statistics
- Add new profiles
- Edit existing profiles
- Add/remove profiles to/from profile groups
- Manage profile access locations
- Create key instances & more!
3.3.1 Creating Profiles

Once you have entered the profile manager, look to the bottom of the list; there, aligned right should be a series of buttons. Locate the button titled Add Profile and click it. This will launch the Create New Profile dialogue. While looking familiar, and essentially behaving in a familiar way, this dialogue is actually a bit different than most in that it is somewhat of a limited wizard which will walk you through the profile creation process:

At a glance...

- A Manufacturer must be selected from a pre-defined list. *If your manufacturer does not exist on the list, contact KMS Support to have it added to the system.* Currently supported Manufacturers are:
  - Best
  - Medeco
  - Russwin
  - Sargent
  - Schlage
  - Yale
- A Title must be selected from the provided menu. Titles are hereditary labels intended to indicate a profile’s general position within its profile tree.
- The Keyway describes the groove along the side of the key and must be between one (1) and eight (8) characters in length and may only include alpha-numeric characters.
- The Biting describes the depths of the teeth of the key and must be between one (1) and eight (8) characters in length and may only include alpha-numeric characters.
- The Keyset is a profile identifier used to uniquely identify a profile. The keyset must be between one (1) and sixteen (16) alpha-numeric characters long.
- The profile’s Secured flag indicates whether or not a key can be duplicated without the express permission of the managing KCC.

*Note that KMS v2 only supports key duplication for keys with the Broken, Destroyed, or Lost status. Also, be aware that the Secured flag offers no functionality to protect your key; it exists solely as a reminder to the implementers.*
To define the profile (step 1 of 4):

1. **LAUNCH** the dialogue as described above.
2. **SELECT** a manufacturer from the **Manufacturer** menu.
3. **SELECT** a **Title** for the new profile.
4. **TYPE** a **Keyway**, observing the rules above.
5. **TYPE** a **Biting** value.
6. **TYPE** a **Keyset** value.
7. Optionally, **SELECT** the **Secured** flag.
8. Optionally, **TYPE** any **Note** you would like to add to the new profile.
9. Optionally, **CHECK** the **Restricted Note** checkbox if you would like the note to be viewable by only you.
10. **CLICK** **Continue** to proceed to Step 2.

![Figure 19: step 1 - define the basic profile](image)

To assign to a profile group (step 2 of 4):

11. Optionally, **CLICK** **Previous** to return to step 1.
12. **SELECT** a control group from the **Ctrl Group** menu; this will populate the **Prfl Group** menu.
13. **SELECT** a profile group from the **Prfl Group** menu; Optionally, if you wish to define a new profile group, you should **SELECT** the **add new group** option.
14. Optionally, if you selected **add new group** in the **Prfl Group** menu, then **TYPE** in a name for the **New Group**.
15. **CLICK** **Continue** to proceed to Step 3.

![Figure 20: step 2 - join a profile group](image)
To define an access location (step 3 of 4):

16. Optionally, **CLICK Previous** to return to step 2.
17. Optionally, skip to the bottom of the dialogue and **CHECK** the box **Skip Access Assignments** if you’d like to defer this step to a later time.
18. If you are skipping this step, **CLICK Continue**, otherwise move on to **STEP 19**.
19. The **Building** menu can be sorted by either facility code or facility name; **SELECT Code** or **Name** to indicate your preference.
20. **SELECT** a facility from the **Building** menu.
21. Optionally, **SELECT** a room from the **Room** menu (if applicable; not all facilities list rooms).
22. **SELECT** one (1) or more **Objects** to identify the profile’s access point.
23. **CLICK** **Continue**.

*Note* this step of the process is provided only as a convenience for a quick assignment; You’ll likely need to use the Access Locations dialogue which will allow you to add as many access location points as you may need. See **SECTION 3.3.5** for additional details.

Once you have moved forward from this step of the new profile process, you’ll be brought to a confirmation of your settings and options. **CLICK** **Submit** at this point to add the new profile to the system.

### 3.3.1.1 A word about child profiles...

What we’ve described above is what KMS v2 refers to as a **Genesis Profile**; that is, it is the root of a tree, it has no parent. Thus, a **Child Profile** is one that has a parent. Other than two caveats, the process for creating a child profile is exactly the same as for a genesis one:

24. To create a child profile, simply select a parent from the main list by selecting the checkbox on the far-left side of the interface; THEN**CLICK** the **Add Profile** button.
25. A child’s parent **must** be at least one generation higher in the profile tree than the new profile. For example, if the parent you selected is a Master, then the child **must** be a Sub-Master or lower.
3.3.2 Editing Profiles

Editing profiles is a simplified version of the creation process; you needn’t worry about groups or access locations, only the profile’s vital statistics are relevant. The rules for the data fields are the same as those defined in Section 3.3.1 Creating Profiles.

To edit a profile (all fields are optional):

1. On the main interface, locate the button labeled Edit Profile and CLICK.
2. SELECT a manufacturer from the Manufacturer menu.
3. SELECT a new Title for the profile.
4. EDIT the Keyway, observing the rules above.
5. EDIT the Biting value.
6. EDIT the Keyset value.
7. SELECT or DESELECT the Secured flag.
8. TYPE any Note you would like to add to the profile.
9. Optionally, CHECK the Restricted Note checkbox if you would like the note to be viewable by only you.
10. CLICK Continue to confirm your changes.

Figure 22: Editing an existing profile
3.3.3 Viewing Profiles

There exists quite a bit of information as relates to profiles. KMS v2 provides a dialogue which brings all this data together in one place in a read-only state. Once you have entered the profile manager, look to the bottom of the list; there, aligned right should be a series of buttons. Locate the button titled View Profile and CLICK it. This will launch the View Profile dialogue.

The intention of this dialogue is to present you with an at a glance view of everything you were ever likely to need to know about a profile. When the dialogue first loads, you will see a small display of the profile’s vital statistics, such as in FIGURE 23 below:

Following the initial profile view, there are a number of collapsible data elements intended to provide you with information related to the profile. With the exception of the historical information, all of this data can also be found in various other dialogues:

- **The profile’s lineage**, a small graphical display is presented illustrating the profiles relative position within its profile tree. Ancestors and direct descendants are shown.
- **Profile group memberships**, a table of all profile groups to which the profile belongs. Hovering your pointer over the KCC column will show you who manages the group.
- **Profile access locations**, locations are displayed in tabular form. As the list can be long, only the first ten locations are shown. If more than ten exist, a link will appear allowing you to launch the Access locations dialogue.
- **Notes attached to the profile**, all notes related to this profile are provided in a collapsible table format. The first thirty characters of the note are displayed; clicking on the note itself will expand the full message.
- **The profiles history**, the full history of the profile, from inception to destruction is recorded and can be viewed here. *Currently, this is the only interface for viewing the historical record.*
3.3.4 Deleting Profiles
Under limited circumstances, KMS supports the ability to delete profiles. A profile may be deleted if and only if all of the following checks are passed:

a) the profile has no child profiles
b) no keys have been instantiated from the profile
c) the profile has attached no access locations

To delete a profile:

1. **Select** one (1) or more profiles from the main interface by checking the appropriate checkbox on the far left of the interface.
2. On the main interface, locate the button labeled *Delete Profile* and **click**.

If there are no errors or conflicts, then the profiles will be removed from the listing. If something is considered to be an issue, then a small dialogue will appear; stopping the process and warning you of the nature of the conflict.

*Note, exercise great care when contemplating the use of this functionality. This tool truly deletes the profile; it is not a merely hidden away to be retrieved later. Profiles removed in this way cannot be recovered!*
3.3.5 Managing Profile Group Memberships

Among the command buttons, located at the bottom of the Profile Manager interface, you should find a button labeled Manage Groups. Select the profile you wish to work with by selecting the checkbox located to the far-left of the main interface, and then click the Manage Groups button. This should load the Profile Groups Membership Editor dialogue.

The membership dialogue is of the accumulator model, meaning changes you make will happen live without confirmation and without leaving the dialogues main interface. To start, you’ll need to define the control group you wish to work in. Select the appropriate group from the Ctrl Group menu. Having done this, any profile groups within that control group that the profile belongs to will be listed in the Subscribed Group(s) menu. Any profile groups that are owned by the control group and are available for you to join, will appear in the Available Groups(s) menu.

To join a profile group:

1. **SELECT** one or more groups in the Available Group(s) menu.
2. Optionally, **SELECT** the Auto Include flag.
3. **CLICK** Commit. The selected group(s) should now appear in the Subscribed Group(s) menu.

To leave a profile group:

1. **SELECT** one or more groups in the Subscribed Group(s) menu.
2. **CLICK** Commit. The selected groups should now appear in the Available Group(s) Menu.

At any point in this process, you can attach a note to the profile being actively managed. You can also join groups and leave groups at the same time.

*Note: By selecting the Auto Include flag when you join a new group, you are telling the system to automatically add all of the profile’s children to the group as well. Not only the children that currently exist, but also any new children that are ever created.*
3.3.6 Managing Access Locations

When we cut a physical key based on the definition of a profile, that key will be mated to a lock core installed somewhere in one or more locations within your enterprise. Access locations are how we track the specifics of what the key will be able to open.

Once you’ve entered the profile manager, look to the command buttons aligned below the main interface; Select a profile to work with and click the button labeled Access Locations. If the selected profile has any recorded access points, they should be displayed in a table which includes the facility code, facility name, the room identifier (if applicable), and the object name. Clicking anywhere on a given row will reveal any notes that happen to be attached to the object.

To add a new access location:

1. From the Access Location dialogue’s main interface, CLICK the small building icon:
2. You should now be working from the Define Access Location form.
3. SELECT a Facility Order to tell KMS how you would like the Building menu sorted.
4. SELECT a facility from the Building menu; this should populate the Room menu.
5. Optionally, SELECT a room name from the Room menu.
6. SELECT the appropriate object from the Object menu. Hint: SELECT Null if you don’t wish to identify a specific object.
7. TYPE any Note you would like to add to the profile.
8. Optionally, CHECK the Restricted Note checkbox if you would like the note to be viewable by only you.
9. CLICK Continue; you will be brought to a confirmation of the new access point you have defined.
10. CLICK Previous if you wish to make any changes.
11. CLICK Submit to commit the new access point to the list.

*Note: It’s important to be aware of the fact that access locations are automatically propagated up the profile tree. For example, if you have a tree such as: Master > sub-Master > Change and you add a new access location to 'Change', then Sub-Master and Master will also gain the new access point.
Deleting access locations...

There are use cases under which an implementer may wish to remove one or more of a profile's access locations. We allow this if and only if the profile in question does not have any descendants that also register the same access location.

For example, suppose you had a small tree of profiles such as is depicted in FIGURE 40:

![Figure 40: Example profile tree](image)

Let’s further assume that all three profiles share an access location to room 215 in CCC. You will receive an error if you attempt to remove the CCC access location from Master:Best-L-A because Change:Best-L-AA is a descendant of Master and it also shares the access location.

However, you may delete the access location from Change:Best-L-AA since it has no descendants.

To delete an access location, simply select the appropriate entry in the dialogue and click the delete button:

![Figure 41: deleting an access location](image)
3.3.7 Exporting Profile Trees

A need has been identified for Implementers to be able to send profile information to a KCC for use in efforts to document keys that do not yet exist in KMS. This could be due to a number or reasons such as a new KCC adopting KMS, an existing KCC mapping out the locks/keys of a new building, etc.

The KMS Profile Spreadsheet Generator will assist you in fulfilling this need. You simply select a tree of profiles, identify who needs the data, and KMS will generate a spread sheet containing all the appropriate fields for documenting one’s keys, and will e-mail the file to the identified recipient.

The intention is that the KCC can later use the spreadsheet to import a batch of new keys along with their managerial organization (key groups, etc.).

To export a profile tree:

1. **Enter** the Profile Manager and locate the root profile of the full tree that you would like to include in the spread sheet. That is, **Select** the profile that is the top most profile; all of its children will automatically be included.
2. **Enter** a Cornell NetId in the *Recipient* field. This should be the NetId of the KCC that will receive the spreadsheet.
3. **Click** *Continue*, you’ll be prompted to confirm your settings; **click** *Previous* if you need to make changes.
4. **Click** *Submit* when ready. The file will be generated and e-mailed to the user you identified in *STEP 2*.

*The generated spread sheet will be accessible to you for a short period of time via the final confirmation of the export process.*

![Figure 26: The profile export work flow](image-url)
3.3.8 Searching for Profiles

KMS v2 includes limited support for searching profiles. That is to say, the functionality is really more of an advanced filter than an open-ended search capability.

The search interface is available to you on the Keys tab under the Profiles menu. Clicking this link will bring you to an advanced filter form where you can define values to help you isolate the exact subset of profiles that you need to work with.

Once you have defined the criteria of your search, simply click Search Profiles; you will be brought to the Profile Manager with your search results loaded and ready to be worked with.

Note that when you enter the Profile Manager from the search page, the page is loaded in Search Results mode. The only difference between normal and search results mode is that search results do not provide you with the filter tools as it was deemed to be redundant. All other tools are available via their usual methods.

Be aware that the search process will limit possible results to profiles that exist within control groups to which you have been granted access.
3.4 Keys
The instantiation of the profiles into cut physical keys and the management of those keys is really what KMS is all about. Once we have a cut key and it’s been delivered, the KCC will handle the vast majority of the key management. However, the start of the chain of custody lays with you the implementer; the key must be documented from the very moment that it comes into existence.

To assist the Implementer with this responsibility, we’ve provided a couple of tools: The key instantiation dialogue and the key review tool.

The dialogue will guide you through the process of creating keys, either one at a time or in batches of any size you wish. The review tool is an implementer-specific view into the KMS v2 key data; allowing you the ability to view a key’s vital statistics and to edit those values.

The creation dialogue is accessible via the command button labeled Create Instance in the Profile Manager. The Key Review tool however, has its own interface which you can reach by clicking the appropriate link on the Key tab menu.

Figure 29: Accessing the key review tool
3.4.1 Creating Keys

Keys can be created individually or in batches; we’ll take the time to look at both approaches independently below. Not that the approaches are radically different so much as just to limit the opportunities to create confusion.

To get started, you will need to access the Profile Manager from the Keys tab. Along the bottom, you will find a series of command buttons; clicking the button labeled Create Instance will launch the key creation dialogue.

To create a single key:

1. **Enter** the Profile Manager and locate & **select** the profile you wish to instantiate.
2. **Click** the button labeled Create Instance.
3. **Type** in the Key Stamp value for the new instance. The Key Stamp is limited to alpha numerical characters and can be no longer than sixteen (16) characters in length.
4. **Select** the Mode of ‘Single’.
5. **Type** in the Sequence number to be applied to the key. The dialogue will load with a recommended value (number of existing keys + 1)
6. **Type** any Note you would like to add to the profile.
7. Optionally, **check** the Restricted Note checkbox if you would like the note to be viewable by only you.
8. **Click** Continue; **Step 2** Add to Key Group should load.
9. **Select** an appropriate Profile Group from the menu; this should load available groups in the Key Group menu.
10. **Select** a Key Group to manage the new instance. If you are unsure of where to place the key, select the default key group which is identified on the interface.
11. Optionally, **click** Previous if you need to make changes.
12. **Click** Continue when you are ready. You should now be looking at a confirmation of your selected options.
13. Optionally, **click** Previous if you need to make changes.
14. **Click** Submit when you are done.

At this point, you should have a new key record which you can go review in the Implementer’s Key Review interface (see **Section 3.4.2**).

*Note that the Key set and Key cut values are supplied for reference only.*
Figure 30: The key creation process for a single key.
To create a batch of keys:

The main difference between creating a single key and a batch of keys is that when you select Multiple Mode, the Sequence field will disappear and be replaced with two new ones:

![New instance.

- **Mode:** How many instances would you like to define?
- **Start of Sequence:** The key sequence will start with this value.
- **Instances:** The number of keys to be cut; defaults to 10.

**Note:**

![Figure 31: Differences in creating multiple keys.](image)

The **Start of Sequence** is the same as **Sequence** under Single Mode, only this is now a starting point; the system will automatically increment the sequence number as it creates the instances.

The **Instances** field simply tells KMS how many keys should be instantiated starting from the value in the **Start of Sequence** field. Thus, using **Figure 31** above as an example, we would be asking KMS to create ten (10) keys; with sequence numbers: 4 – 13. *KMS provided default values of 4 for the Start of Sequence and 10 for the Instances field.

Aside from the above description, the rest of the process is the same as Single Mode. Simply **Continue** to the next page, add to a **Key Group**, **Confirm**, and **Submit**.
3.4.2 Reviewing Keys
KMS provides you with a view into the key data that is tailored to your needs as an Implementer. Tools are available for viewing key vital statistics as well as editing the data of record. When you load the review page, you should see all keys that were instantiated from profiles that fall under control groups of which you are a member:

To be clear, KMS v2 **does not expect** implementers to manage key instances. The chain of custody for each key begins with you, but once the KCC takes receipt of the key, the management becomes his responsibility. This tool is provided to you as a convenience only and is in no way intended to imply additional responsibilities for the Implementers.
3.4.3 Viewing Keys

As with profiles, keys also generate a good deal of related information. The View Key dialogue in the Review Keys interface provides you with a static view into all key-related data.

Once you have entered the Review Keys interface, look to the bottom of the list; there, aligned right should be a series of buttons. Locate the button titled View Key and click it. This will launch the View Key dialogue.

The intention of this dialogue is to present you with an at-a-glance view of everything you are ever likely to need to know about a key. When the dialogue first loads, you will see a small display of the key’s vital statistics, such as in Figure 33 below.

Following the initial key view, there are a number of collapsible data elements intended to provide you with information related to the key:

- **The key’s profile**, a small display, similar to that in the View Profile dialogue (see Section 3.3.3), detailing the specific data elements that make up the key’s profile record.
- **Notes attached to the key**, all notes related to this key are provided in a collapsible table format. The first thirty characters of the note are displayed; clicking on the note itself will expand the full message.
- **The key’s history**, the full history of the key, from instantiation to destruction is recorded and can be viewed here. *Currently, this is the only interface for viewing the historical record.*
3.4.4 Editing Keys
A simplified version of the KMS key editor is provided for your use in the event that you need to make minor changes to the key’s data of record. Additionally, only the Implementer role is allowed to mark a key as Destroyed, thus you would need this interface in the event that you have permanently retired a key instance.

*If you happen to have KCC access to any part of the KMS inventory, you will notice that this key editor is different from the one made available to KCCs; Please defer to the KCC manual for assistance when reading documentation concerning the editors.

To edit a key instance:

1. Enter the Review Keys interface and SELECT a key to be edited.
2. LOCATE & CLICK the button labeled Edit Key; this will launch the Edit Key dialogue.
3. Optionally, SELECT a new Key Status if applicable.
4. Optionally, TYPE in a new key Sequence value. Note that if you provide a value that would create a duplicate key, the edit process will be halted, unless the key’s status is ‘Destroyed’.
5. Optionally, TYPE a new Key Stamp value. The Key Stamp is limited to alpha-numerical characters and can be no more than sixteen (16) characters in length.
6. TYPE any Note you would like to add to the profile.
7. Optionally, CHECK the Restricted Note checkbox if you would like the note to be viewable by only you.
8. CLICK Continue, this will bring you to a confirmation of the changes you have made.
9. Optionally, CLICK Previous, if you’d like to change any values.
10. CLICK Submit when done.

Figure 33: an Implementer’s key editor
4. Community Tools

KMS v2 provides a few tools that are made more broadly available than to just one or two roles. There are currently two such distinctions made within the software; what KMS considers to be the Working Community and the Vested Community.

The KMS Working Community is considered to be all KMS roles that exist for the purpose of managing one aspect or another of the KMS data set. That is to say, if a role is intended to work with the data in any respect, we consider them to be a part of the working community. This community includes: Administrators, Implementers, KCCs, and AKCCs.

The KMS Vested Community is considered to be any and all individuals from across the enterprise that has any reason at all to interact with the KMS system. This includes everyone from KMS Administrators on down to any user within the enterprise whose only connection to KMS is that they have been assigned a key that is managed by KMS. The vested community includes all KMS roles: Administrator, Implementer, SKCC, KCC, AKCC, Bureaucrat, Key-Holder, & Guest.

In the following pages we will talk about the KMS community tools in greater depth. When doing so, when we need to talk about who has access and why, we will refer to the community roles as we have defined them above.
4.1 Facility Object Manager

Facility Objects (FOs) are a new concept to KMS v2, and considered to be a core component. FOs allow us to abstract away the concept of an access location and/or a storage location from the actual entity being locked or used for storage. We are able to create any object we can conceive of and add it to any building or building/room combination. This allows us to be very precise in identifying what a profile opens or where a key is stored. Additionally, this provides us with great flexibility in future development since we can leverage existing data elements to support additional functionality such as tracking a managing unmanaged keys (furniture or cabinet keys for example).

FOs can be related to one another in a parent/child structure; allowing you to create a path of objects which can relate a great deal of detail regarding, for example, where a key is stored. It is entirely possible to have a key stored in: East Hill Office Building, Rm 245, Dave’s Desk > Bottom-Right-Drawer > Lock Box #2 > 2nd Tray. This level of detail is not required; it is entirely up to you how much or how little you leverage the system.

FOs are, by default, accessible and editable by the entire KMS Working Community (see SECTION 4). Due to its purpose, the object database will be very large; KMS is installed with more than 68,000 objects. Once users begin adding objects to meet their specific needs, the number of managed objects will grow very quickly. Thus it is to all of our benefit if we are able to leverage an object that has already been defined by another. For example, if Bob adds a second door to some room, I don’t want to have define a new door when I need to reference that room; I should just find the door already listed and make use of it. In this way, the object database will be defined by the community. I can also open Bob’s door record and edit it if I discover a mistake or if a change needs to be made.

Now, while the default behavior of the FOs is to be open to the world for both use and editing; this does not have to be the case. When you define an FO, you will have the option to lock an FO in such a way that others can use it, but only you can edit it. You can even restrict an FO to such an extent that only you can see it.

You can load the Facility Object Manager by clicking the Facilities tab and then clicking the Manage Facility Objects link found under the Objects menu.

![Navigating to the Facilities Object Manager](image-url)
Once you have entered the Facility Object Manager, you will be looking at an interface that is somewhat similar to what we have seen before. The singular difference is the tree browser navigational tool which replaces the filters we’ve seen previously. As you navigate the tree, the list on the right will update, providing you with a contextually accurate display. Selecting a facility on the left will provide you with a list of every object in that facility, on the right. Selecting a room under a facility will filter the list to restrict the domain to that of the objects within that specific room.

Figure 36: Facilities Object Manager

*Note:* that you can delete objects if and only if they are not in use in any capacity. You can identify objects that are in use by referring to the ‘in-use’ column of the main interface (see Figure 36 above).
4.1.1 Creating Facility Objects

Currently, Facility Objects (FO) are used to serve two purposes (this is likely to change as KMS v2 evolves): to create objects to serve as an access point for profiles, and to serve as a storage location for keys. Of course, creating an object that serves both purposes is entirely possible.

You may create a singular object (e.g. Cabinet) or if you wish to extend an object, you may select it and create a child object (e.g. Cabinet > top-shelf). These objects are all defined by six properties:

- **Type**, an object type is a general classification such as Box, Cabinet, Desk, Door, etc.
- **Label**, a short descriptive term such as “north door” or “Dave’s Desk”. Labels may contain any text, but cannot be any longer than thirty-two (32) characters in length.
- **Configuration**, can this object be used as an access location, as storage for keys, or both?
- **Publicly Editable**, is it ok to let the KMS working community edit the object? The system defaults to ‘yes’.
- **Restricted**, should the object be restricted to you so that only you can see, edit, and use the object?

*If you mark an object as restricted, then any children of that object that you later define will also be restricted.

**To create a new object:**

1. Enter the Facility Objects Manager interface as described in [SECTION 4.1](#).
2. Using the tree browser, NAVIGATE to the facility and room you wish to create the object in.
3. LOCATE & CLICK the button labeled Create; this will launch the KMS Facilities Object Editor dialogue (see [FIGURE 39](#) below).
4. SELECT a category for your object from the Type menu.
5. ENTER a label for the object.
6. Under Mode, SELECT single object (see [SECTION 4.1.2](#) for information concerning batch creation).
7. Optionally, if you wish for your object to be available as an access location, SELECT the check box next to **can be locked**.
8. Optionally, if you wish for your object to be available to store keys, SELECT the check box next to **can store keys**.
9. Optionally, if you want the object to be available and editable by the KMS community, SELECT the check box next to **publicly editable**. **Note that objects not editable are still available for public use as access locations or storage containers.**
10. Optionally, if you wish for the object to be hidden from view, usable and editable by only you then SELECT the check box next to **restrict access**.
11. Optionally, if you would like to attach a note to this object at creation time, SELECT the check box next to **attach a note to this new object**; a notes field will appear.
12. CLICK Submit
13. Review your settings; if you wish to change something, CLICK Back.
14. When you are satisfied, CLICK Submit
To create a child object:

As mentioned earlier, you can chain objects together to relate them or otherwise provide a greater degree of context to them. For example, you will likely often see cabinets with hook children. The process for creating a child differs only in how you launch the dialogue; that is, you select a parent object, launch the dialogue, then proceed as normal.
4.1.2 Facility Object Batch Creation
KMS v2 supports the notion of object batch creation; as either a new object or as children of another. For example, this would be useful to populate a key cabinet with a large number of hook objects.

The process is the same as for creating a single object. The difference is that under *Mode*, you will select *batch of objects*. When you do this, two new fields will appear such as in *Figure 41* below:

- Start counter at
- Number of objects

The number of objects is literally the number of instances we are to create. The counter is used as an appendage to the object label and must be numerical. So, if you were to define five (5) objects with the label ‘Key Hook’, and you started the label at 1, then you would end up with five objects named:

- Key Hook 1
- Key Hook 2
- Key Hook 3
- Key Hook 4
- Key Hook 5

*Figure 37: Object batch creation*
4.1.3 Editing Facility Objects

Editing a Facility Object (FO) is fairly straightforward with the process being almost identical to that of creating objects. The main difference is that when editing, rather than a Mode option, you will instead have access to fields which will enable you to relocate an object from its current location to a new one. When doing so, you may optionally elect to move an object’s children with it.

**To edit an object:**

1. Enter the *Facility Objects Manager* interface as described in [SECTION 4.1](#).
2. Using the tree browser, navigate to the facility and room the object resides in.
3. Select the check box on the far-left of the main interface that corresponds to the object you wish to edit.
4. Locate & click the button labeled *Edit*; this will launch the *KMS Facilities Object Editor* dialogue with the object details pre-loaded.
5. Optionally, select a category for your object from the *Type* menu.
6. Optionally, re-enter a label for the object.
7. Optionally, under *Relocate*, select a new building or building/room combination.
8. Optionally, if relocating an object, and you wish for its children to go with it, select the check box next to *include child objects*.
9. Optionally, if you wish for your object to be available as an access location, select the check box next to *can be locked*.
10. Optionally, if you wish for your object to be available to store keys, select the check box next to *can store keys*.
11. Optionally, if you want the object to be available and editable by the KMS community, select the check box next to *publicly editable*. *Note that objects not editable are still available for public use as access locations or storage containers.*
12. Optionally, if you wish for the object to be hidden from view, usable and editable by only you then select the check box next to *restrict access*.
13. Optionally, if you would like to attach a note to this object at creation time, select the check box next to *attach a note to this new object*; a notes field will appear.
14. Click *Submit*
15. Review your settings; if you wish to change something, click *Back*.
16. When you are satisfied, click *Submit*
Please note that some editing options may not be available to you. The business rules that govern the creation and management of objects are fairly complex and conflicts easily arising. For example, you may not be able to clear an objects storage flag if someone has stored keys there. The dialogue will inform you if you attempt to make a change that is not permissible under the current system.

Some general guidelines are:

- Only the creator of an object can edit those objects flagged as non-editable.
- Only the creator of an object can set the restricted access flag.
- Only the creator of an object may set an editable object to un-editable.
- Restricted objects may be set to unrestricted by the creator and only if the object has no children.
- Storage and lockable flags can be edited off only if the objects are not in use in that particular regard. These flags may be freely edited on.
- Objects set to restricted access, cannot be set to publicly editable.
- Children of a restricted access object cannot be set unrestricted.
4.1.4 Deleting Facility Objects
Under certain circumstances, you may delete one or more facility objects. Note that this is a true deletion and cannot be recovered, so use carefully.

Before you can attempt to delete an object, you must have the right to edit it. If for some reason the object cannot be edited by you, then it is protected from deletion. Furthermore, to protect against complex conflicts that can arise in the stored data, you will not be allowed to delete any object that is in any way in current use. If any other element within the KMS system references that object, even a note, it will not be eligible for removal. Note that the main interface has a column labeled IN USE which will tell you at a glance if something is using the object.

To delete an object:

1. Enter the Facility Objects Manager interface as described in SECTION 4.1.
2. Using the tree browser, NAVIGATE to the facility and room the object resides in.
3. SELECT the check box on the far-left of the main interface that corresponds to the objects you wish to delete (you may select multiple).
4. LOCATE & CLICK the button labeled Delete; this will launch a confirmation of your intended action. It will also warn you that this process cannot be undone.
5. CLICK the button labeled Delete Objects.

If your attempt to remove the objects was successful, the dialogue will close and the main list will refresh with the objects gone.
4.2 View My Keys

KMS v2 introduces an entirely new feature, open to the full vested community; that is, anyone within the enterprise is free to come in and view an inventory of all KMS-managed keys and key rings that have been assigned to them.

The interface is a straightforward list of keys which can be viewed as is or from a key ring perspective. Allow your pointer to hover over the hierarchical title and a list of the relevant access locations will be presented to you via an extended tooltip.

Under the current version of KMS, this functionality is limited to reporting and allowing a key-holder to report a key as lost or broken; this will change considerably as KMS evolves.

**Reporting keys as lost or broken:**

As it is a straightforward and trivial process, we’ll describe the functionality to report lost and broken keys here. Simply select the key you wish to report and click the button labeled *Report Lost or Broken*. You’ll need to indicate if the key is lost or broken. There is an optional space provided for you to add some additional information if you so desire. Once you submit the dialogue, a report will be sent to the individual that assigned the key to you. The reported key will then be removed from your inventory.
5. How Do I...?

Have a question that this document failed to answer? Send e-mail to acg-support@cornell.edu; if your question would benefit everyone, we’ll include it in this section of the document with a detailed answer.
## Table of Figures

<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Navigate to control group manager.</td>
<td>15</td>
</tr>
<tr>
<td>2</td>
<td>Creating a new Control Group</td>
<td>16</td>
</tr>
<tr>
<td>3</td>
<td>Editing a Control Group</td>
<td>17</td>
</tr>
<tr>
<td>4</td>
<td>Managing implementer group access</td>
<td>18</td>
</tr>
<tr>
<td>5</td>
<td>Profile groups managerial interface</td>
<td>19</td>
</tr>
<tr>
<td>6</td>
<td>Creating a new profile group</td>
<td>20</td>
</tr>
<tr>
<td>7</td>
<td>Editing a profile group</td>
<td>21</td>
</tr>
<tr>
<td>8</td>
<td>Managing profile group access for KCCs</td>
<td>22</td>
</tr>
<tr>
<td>9</td>
<td>Profile Manager with Notes list expanded</td>
<td>23</td>
</tr>
<tr>
<td>10</td>
<td>Launching the profile access manager</td>
<td>24</td>
</tr>
<tr>
<td>11</td>
<td>Managing profile group access for KCCs</td>
<td>25</td>
</tr>
<tr>
<td>12</td>
<td>Editing an existing profile</td>
<td>26</td>
</tr>
<tr>
<td>13</td>
<td>Profile Static View</td>
<td>27</td>
</tr>
<tr>
<td>14</td>
<td>Managing a profile's group membership</td>
<td>28</td>
</tr>
<tr>
<td>15</td>
<td>The profile export work flow</td>
<td>29</td>
</tr>
<tr>
<td>16</td>
<td>KCC authorization status</td>
<td>30</td>
</tr>
<tr>
<td>17</td>
<td>Profile Manager with Notes list expanded</td>
<td>31</td>
</tr>
<tr>
<td>18</td>
<td>Accessing the key review tool</td>
<td>32</td>
</tr>
<tr>
<td>19</td>
<td>The key creation process for a single key</td>
<td>33</td>
</tr>
<tr>
<td>20</td>
<td>Differences in creating multiple keys</td>
<td>34</td>
</tr>
<tr>
<td>21</td>
<td>Static key view</td>
<td>35</td>
</tr>
<tr>
<td>22</td>
<td>an Implementer's key editor</td>
<td>36</td>
</tr>
<tr>
<td>23</td>
<td>Navigating to the Facilities Object Manager</td>
<td>37</td>
</tr>
<tr>
<td>24</td>
<td>Creating a new object</td>
<td>38</td>
</tr>
<tr>
<td>25</td>
<td>Creating a new child object</td>
<td>39</td>
</tr>
<tr>
<td>26</td>
<td>Editing a facility object</td>
<td>40</td>
</tr>
<tr>
<td>27</td>
<td>Object batch creation</td>
<td>41</td>
</tr>
<tr>
<td>28</td>
<td>Creating a new object</td>
<td>42</td>
</tr>
<tr>
<td>29</td>
<td>Editing a facility object</td>
<td>43</td>
</tr>
<tr>
<td>30</td>
<td>Creating a new child object</td>
<td>44</td>
</tr>
<tr>
<td>31</td>
<td>Differences in creating multiple keys</td>
<td>45</td>
</tr>
<tr>
<td>32</td>
<td>Static key view</td>
<td>46</td>
</tr>
<tr>
<td>33</td>
<td>an Implementer's key editor</td>
<td>47</td>
</tr>
<tr>
<td>34</td>
<td>Navigating to the Facilities Object Manager</td>
<td>48</td>
</tr>
<tr>
<td>35</td>
<td>Creating a new object</td>
<td>49</td>
</tr>
<tr>
<td>36</td>
<td>Creating a new child object</td>
<td>50</td>
</tr>
<tr>
<td>37</td>
<td>Object batch creation</td>
<td>51</td>
</tr>
<tr>
<td>38</td>
<td>Editing a facility object</td>
<td>52</td>
</tr>
<tr>
<td>39</td>
<td>Differences in creating multiple keys</td>
<td>53</td>
</tr>
<tr>
<td>40</td>
<td>Static key view</td>
<td>54</td>
</tr>
</tbody>
</table>