The Key Control Coordinator’s Role

A KMS v2.x Software Perspective
Contents

Introduction .................................................................................................................................................. 4

1. KMS v2: New Concepts ......................................................................................................................... 5
   1.1 Profiles ................................................................................................................................................ 5
   1.2 Profile Groups ..................................................................................................................................... 6
   1.3 Community Tools ................................................................................................................................ 6

2. KMS v2: The Software ........................................................................................................................... 7
   2.1 General Concepts ................................................................................................................................ 7
       2.1.1 User Interfaces ............................................................................................................................. 8
       2.1.2 Notes .......................................................................................................................................... 10
       2.1.3 Security ...................................................................................................................................... 11
       2.1.4 User Creation ............................................................................................................................. 11
       2.1.5 User Roles .................................................................................................................................. 12
       2.1.6 Communications ........................................................................................................................ 13
   2.2 What’s Available to You .................................................................................................................... 14

3. Key Control Coordinator Tools ............................................................................................................ 15
   3.1 Key Groups ........................................................................................................................................ 15
       3.1.1 Creating Key Groups .................................................................................................................. 16
       3.1.2 Editing Key Groups ..................................................................................................................... 17
       3.1.3 Managing AKCC Memberships ................................................................................................. 18
   3.2 Keys ................................................................................................................................................... 18
       3.2.1 Viewing Keys .............................................................................................................................. 21
       3.2.2 Editing Keys ................................................................................................................................ 22
       3.2.3 Managing Key Group Membership ........................................................................................... 24
       3.2.4 Adding Keys to a Key Ring ......................................................................................................... 25
       3.2.5 Assigning Keys to Key Holders ................................................................................................. 26
       3.2.6 Renewing and Purging Key Assignments ................................................................................. 27
       3.2.7 Recovering Lost Keys ................................................................................................................ 29
       3.2.8 Storing Keys ................................................................................................................................ 30
   3.3 Key Rings ........................................................................................................................................... 32
       3.3.1 Viewing Key Rings ...................................................................................................................... 33
       3.3.2 Creating Key Rings ................................................................................................................... 34
**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. We believe 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 Key Control Coordinator (KCC) role is a fundamental cornerstone upon which the university’s approach to key management is established.

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

The KCC’s role involves the many aspects of key management including the organization of stores, assignments to users, auditing, record keeping and much more.

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 manage key assignments, inventories, and transactions.

---

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 Key Control Coordinator (KCC) 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: New Concepts

Whether you are new to KMS or 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 discuss some of the core functionality that was not present in the original KMS releases. The information is presented in the context of relevance to the KCC role and is intended to give users of the original system a quick glance at important new features.

The following is strictly intended to introduce you to the concepts; later in the document we will explore more in-depth how you will be best leverage or will be affected by these features.

1.1 Profiles

Unless you are new to KMS and key management in general, profiles are unlikely to be a new concept to you. However, the importance of the concept, especially as it relates to KCCs, is such that we feel the topic warrants some discussion so we all know what we mean when we talk about a KMS v2 profile.

Profiles are essentially the blue print from which we can instantiate a cut physical key. You could think of the profile as a recipe that tells us how to perform that cut. Additionally, profiles can be related to one another through a parent-child relationship with each child able to operate on a subset of its parent’s locks. In KMS v2, 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)

As a KCC, your interaction with profiles will be fairly limited; however it is likely that you will be granted access to a sizable pool of profiles from which all of the keys you are responsible for are based. In fact, it is common for a KCC to have access to a profile tree that is much larger than the pool of profiles that are actually in current use.

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. The hierarchy of these titles, as currently supported within KMSv2, is as follows:

- Control
- Great Grandmaster
- Grandmaster
- Master
1.2 Profile Groups
Being introduced for the first time in KMS v2, profile groups are an organizational structure utilized by Implementers\(^1\) in grouping profiles together into authorization-oriented configurations. KCCs are then granted access to one or more groups of profiles; essentially granting them managerial rights to any keys instantiated from those profiles.

As stated above, profile groups are a tool for Implementers to leverage. However, as a KCC, you will be made a member of at least one profile group. There is no limit to the number of groups you can be assigned to, but note that there is a policy-driven authorization requirement that exists outside of the domain of the KMS v2 software. Once you have completed the KCC authorization process defined in policy 8.4, you can be authorized by the KMS v2 administrators; at which point you should have full access to all profiles contained in your assigned groups.

Under this new authorization model, there is also no limit to the number of KCCs that can be assigned to a single profile group. Thus, it is possible for multiple KCCs to be authorized and responsible for the same set of profiles. For those familiar with KMS v1, the profile group concept deprecates the need for the notion of the Back-Up KCC.

1.3 Community Tools
KMS v2 was developed as an enterprise-scoped solution; it supports a number of roles which when taken together, support a vast array of stakes across the enterprise. From Implementers that cut the keys to key-holders that utilize them, we provide the tools that enable the community to work together. Currently these concepts are limited to defining data and fulfilling various auditing needs, but future efforts are slated to expand upon this functionality.

Facility Objects (FO) are a core element of KMS v2 that allows the working community\(^2\) to populate the enterprise with data relevant to defining and tracking access locations and key storage areas. Anyone with a business need in KMS v2 has access to define and edit these objects. New objects you create 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.

For the first time ever, KMS offers functionality for the entire enterprise via the View My Keys interface which provides a general user with an inventory of all assigned keys and key rings.

\(^1\) Implementer is the name of KMS v2 role that is filled by lock shop or other staff members whose primary task is the management of profiles and the cutting of physical key instances.

\(^2\) The working community is defined as: Administrators, Implementers, KCCs, & AKCCs.
2. 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 KCCs 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 leverage them to achieve desired goals.

2.1 General Concepts

KMS v2 is a fairly substantial offering. Before getting into the various KCC 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 system you are currently working in.

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 1. 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 and if the KMS administrators feel the need to communicate with the community.

Figure 1: KMS v2 main interface
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 presented.

**Filters...**
Each of these displays contains a filter along the top edge of the interface area (see FIGURE 3). The filters are relevant key data points that will allow you to tunnel down into the data display. The data points are often cascading; meaning they are dependent on the data point selected to the left. As you make selections, starting from the left, the menus along the filter to the right will populate as they are able to.

![Figure 4: KMS data filter flow](image)

**Dialogues...**
While the manager displays provide you with a fair picture of the data to review, the majority of the operable functionality will be found in the small dialogues that pop-up when you first, select one or more rows in the display, and then click on one of the command buttons along the bottom of the interface.

As with the main user interfaces, while there are exceptions, the vast majority of the dialogues will flow and operate the same. Gaining some experience with one will grant your insight into most of the others as well.

![*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*](image)

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 (see FIGURE 5).
Figure 5: Hovering your pointer over the key ring name in the key manager interface results in a small reference list of member keys being displayed.

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.
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 Net Id solicited.
When you type a Cornell Net Id 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, his 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.

*Be aware that security validation does not end with simple role checks for functionality; each and every element of data is scrutinized to determine whether or not you are allowed to manipulate it. Thus it is entirely possible that you may be able to load a dialogue due to your role as Implementer, but find you are not allowed to manipulate certain data due to a lack of KCC rights to that specific data.*

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 a KCC and also as a community member. Your position as a KCC will largely drive the options you will see on your menu. These will include:

- **Profile Manager**, viewing profiles and managing their access locations.
- **Key Manager**, review, edit, and manage the key instances instantiated from your assigned profiles.
- **Key Group Manager**, create and manage key groups and their AKCC memberships.
- **Key Ring Manager**, create and manage physical groupings of keys.
- **Key Searches**, a more elaborate filter set for tunneling into the key 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. Key Control Coordinator Tools

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

The following sections are provided in the order that we anticipate a KCC 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 Key Groups

Key Groups serve as the KCCs primary organizational unit for managing keys. If you manage multiple facilities, you might create one group per building or perhaps another logical grouping based on areas of responsibility; you are free to structure this organization in any way that makes sense for your needs.

The important thing to be mindful of when creating your key groups is that they also serve as the authorization tool for Associate Key Control Coordinators (AKCC). When you add an AKCC to a key group, they receive full managerial rights to any key instance that has also been assigned to the group.

*Note that key groups are actually owned by the profile group under which they are created. When a profile group is created, it spawns a single default key group, thus when you log into KMS for the first time as a KCC, you will already have at least one key group to work with.*

To begin working with key groups, Enter the Key Group Manager by locating the link Manage Key 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 key groups owned by the profile groups of which you are a member.
3.1.1 Creating Key Groups

Once you have entered the Key Group Manager, look to the bottom of the list; there, aligned right should be a series of command buttons. Locate the button labeled, Add Key Group and click it. This will launch the Create New Key Group dialogue.

At a glance...

As a data element, key groups are simple constructs, consisting of only three fields: Name, parent profile groups, a flag indicating whether or not this new group will serve as its parent’s default key group. To create the group, be mindful of the following limitations:

- **Names** must be unique across the scope of the parent 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: `- _ : /`
- **Default Key Groups** have a system-wide default name: New Keys. You can edit this name if you so choose.

To create a new group:

1. **Launch** the dialogue as described above.
2. **Type** a Name for the key group.
3. **Select** the parent Profile Group from the provided menu.
4. Optionally, **check** the Default Group checkbox if you would like your new key group to act as its parent profile group’s default container.
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 8: Creating a new key group](image-url)
3.1.2 Editing Key Groups
Editing an existing key group is as easy as defining a new one. To edit an existing group, enter the Key Group Manager to view the list of available groups. Once you have identified the group you wish to edit, SELECT the appropriate checkbox located in the far-left column of the main display. Having selected the group, locate the button labeled Edit Key Group and CLICK it.

You should now be faced with a dialogue similar to the one in FIGURE 9. 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 key 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 Group option is a flag that when selected, instructs this group to take over the role of default key group for its parent profile group.

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 the Default Group checkbox if you would like this group to become the new default.
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 AKCC Memberships

KCCs have the ability to freely add KMS users to assist in the managing of keys and their assignments; No university authorization is required. You may add as many Associate Key Control Coordinators (AKCC) as you deem necessary to get the job done. AKCCs are added to the system on a key group basis and will be granted authorization to manage key assignments and storage for all keys you have placed in the group. AKCCs may belong to multiple groups but you’ll need to add them to each individually. In this section we’ll discuss how to manage the users you wish to add to or remove from key groups.

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 AKCCs menu lists all AKCCs 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 Cornell Net Id.
2. **CLICK** Commit, you should see the user moved up to the KCCs menu.

**To remove a user from the group:**

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

*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 Keys
The physical cut keys and their management are the primary reason you are reading this manual and preparing to work with KMS. Tracking each key, who has it or where it is currently stored is the task you have been charged with and what all of the tools described in this manual are meant to help you accomplish successfully.

While it isn’t strictly necessary, we’ll suggest that you have put some thought into your organizational structure and have key groups created and waiting to be used prior to beginning work with key records for the first time.

To get started with keys, locate and click the link Manage Keys located on the left-hand navigation menu. On the right of the KMS interface, you should now be faced with a list-based managerial display similar to that in FIGURE 11 below.

When entering the key manager, you should be able to see and work with every key ever cut from a profile that was placed in your profile group. For example, if your profile group managed two (2) profiles: Best-L-A and Best-L-AA, and each had been cut five (5) times, you should see ten (10) keys in the key manager interface.

Figure 11: Launching the Key Manager interface
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 keys. We’ll discuss the options in detail in the following sections, but at a glance, you will be able to:

- View key details and vital statistics
- Edit existing keys
- Manage key group affiliations
- Place keys onto and remove from key rings
- Manage and track key assignments to key holders
- Manage key storage
- And more!

While discouraged, you also have the ability to create new key records. However, this is somewhat of a special case which we’ll talk about in SECTION 3.4 Profiles.
3.2.1 Viewing Keys
There exists quite a bit of information as relates to keys. KMS v2 provides a dialogue which brings all this data together in one place in a read-only state; The View Key dialogue in the Key Manager interface provides you with a static view into all key-related data.

Once you have entered the Key Manager, 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 12 below.

![Figure 12: Static key view](image)

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 3.3.1), 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*
### 3.2.2 Editing Keys

One of the primary features to evolve in KMS v2 is redundancy of functionality; there is rarely only a single way to access certain information or to accomplish a given task. The KCC’s key editor is a good example of this design paradigm where you can not only edit the values that define the key, but you can also alter the key’s status, change its group membership, and even move it onto or off of a key ring.

To edit a key instance:

1. Enter the *Key Manager* interface as described in [SECTION 3.2](#).
2. Locate the key record you wish to edit and **select** it by setting the appropriate checkbox on the far-left of the interface.
3. **Locate** & **click** the button labeled *Edit Key*; this will launch the *Edit Key* dialogue.
4. Optionally, **select** a new *Key Status* if applicable.
5. Optionally, **select** a new *Key Group* to become a member of. The *Profile Group* menu is provided to help you filter *Key Groups*.
6. Optionally, **select** a new *Key Ring* to be placed on, or, if already on one and you wish to be removed, set the *Key Ring* menu to unassign.
7. 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 interrupted; see [CREATING A DUPLICATE KEY](#) below.
8. 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.
9. **Type** any *Note* you would like to add to the profile.
10. Optionally, **check** the *Restricted Note* checkbox if you would like the note to be viewable by only you.
11. **Click** *Continue*, this will bring you to a confirmation of the changes you have made.
12. Optionally, **click** *Previous*, if you’d like to change any values.
13. **Click** *Submit* when done.
3.2.2.1 Creating a Duplicate Key

Strictly speaking, the creation of duplicate keys is against university standards, will typically be blocked by KMS, and should simply be avoided. With that said, the reality of things is that duplicates do exist and need to be documented and tracked just as any other key... maybe even more so.

*Note if a key’s status is ever set to Destroyed then KMS v2 will allow you to create a duplicate key without much fuss at all. However, only an Implementer is allowed to destroy a key.

If in the process of editing a key, your changes would create a duplicate, a warning will appear at the top of the dialogue and a new field will appear in the body:

![Figure 14: Key editor duplication override flag](image)

You may set this check box to override KMS’ duplicate protection processes. Your decision will be noted in the key’s history and the key’s data will always be presented with a Duplicate flag displayed.
3.2.3 Managing Key Group Membership

All key instances must belong to a key group, and only a single key group. When a new key is cut and first recorded, it is placed into a group as part of its instantiation process. If the desired group is unknown at that time, then the key instance is placed into the profile group’s default key group.

You may at any time elect to change the key’s group membership via the KMS Key Groups Membership Editor located on the Key Manager interface.

To change a key’s group affiliation:

1. Enter the Key Manager interface as described in SECTION 3.2.
2. Locate one or more key records that you wish to edit and select them by setting the appropriate checkbox on the far-left of the main interface.
3. Locate & click the button labeled Add to Group; this will launch the KMS Key Groups Membership Editor dialogue.
4. Select a new Key Group from the provided menu.
5. Optionally, type any Note you would like to add to the profile.
6. Optionally, check the Restricted Note checkbox if you would like the note to be viewable by only you.
7. Click Continue, this will bring you to a confirmation of the changes you have made.
8. Optionally, click Previous, if you’d like to change any values.
9. Click Submit when done.
3.2.4 Adding Keys to a Key Ring

In the real world, keys are often grouped together on a key ring and assigned or stored as a single unit. KMS v2 has the ability to reflect this sort of organization (see section 3.3) by creating a KMS Key Ring and assigning key records to be members. The keys are then collectively managed as a ring rather than individually.

To add keys to a key ring:

1. Enter the Key Manager interface as described in SECTION 3.2.
2. Locate one or more key records that you wish to move onto a key ring and SELECT them by setting the appropriate checkbox on the far-left of the main interface.
3. LOCATE & CLICK the button labeled Add to Key Ring; this will launch the KMS Key Ring Membership Editor dialogue.
4. SELECT a new Key Ring from the provided menu.
5. OPTIONALLY, TYPE any Note you would like to add to the profile.
6. Optionally, CHECK the Restricted Note checkbox if you would like the note to be viewable by only you.
7. CLICK Continue, this will bring you to a confirmation of the changes you have made.
8. Optionally, CLICK Previous, if you’d like to change any values.
9. CLICK Submit when done.

To reiterate the statements above; when you add a key to a key ring, the key loses its own identity and instead inherits its status, and all that encompasses such as assignments and storage, from the key ring it is attached to. The key itself will show a new status of Ring, but management activities, such as storage and assignments, will need to be handled via the Key Ring Manager.

There is no limit to the number of keys that may be placed on a key ring; however, keys must meet a few criteria before being considered eligible to be added to a key ring:

- The keys must be in the same key group as the key ring.
- The keys must not already be on a key ring.
- The keys must not be currently assigned to a key holder.
- The keys current status must not be one of: broken, lost, or destroyed.

*Note that key rings do not generate a history such as keys do. Activities performed on key rings instead propagate that information down to the individual keys and need to be viewed in the key’s individual historical record.
3.2.5 Assigning Keys to Key Holders

Keys will likely spend the vast majority of their existence in one of two primary states: assigned and in a key holder's possession or in storage awaiting assignment; we will address the former.

For a key to be considered eligible to be assigned, the key must not currently be:

- assigned to a key holder
- a member of a key ring
- in one of the following states: broken, lost, or destroyed

To assign a key to a key holder:

1. Enter the Key Manager interface as described in SECTION 3.2.
2. Locate one or more key records that you wish to assign to a key holder and select them by setting the appropriate checkbox on the far-left of the main interface.
3. Locate & click the button labeled Assign Key; this will launch the KMS Key Assignment dialogue.
4. Type a Cornell Net Id into the Key Holder field. The user you enter does not need to be a current KMS user, but he must possess a Cornell Net Id. As you type, a menu may appear offering suggestions; simply click on any value that might complete your selection.
5. Type a date into the Assignment Expiry field in the format: mm/dd/yyyy. The date must be at least twenty-four (24) hours in advance of your current time. Optionally, a date-picker is available by clicking the small calendar icon located at the end of the date field.
6. Optionally, enable the Responsible Party flag if the assignment is being made to a Cornell employee that will in turn disburse the key as temporary access to third parties.
7. Optionally, 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 only by you.
9. Click Continue, this will bring you to a confirmation of the changes you have made.
10. Optionally, click Previous, if you'd like to change any values.
11. Click Submit when done.

Figure 15: Key assignment dialogue.
3.2.6 Renewing and Purging Key Assignments
KMS v2 runs a background process known as TaskMon which monitors the system for various state changes and then reports on them. One such process is a daily check for assignment expirations, which if any would affect you, will result in a report being delivered to your e-mail. In many cases, it may be desirable to simply renew the assignment.

In other cases, it is plausible for one reason or another that you wish to just purge an assignment without much ado or fanfare. This section will talk about a couple less obvious tools that will help you in both events.

To renew a key assignment:

When you initially assign a key, its record will complete on the main interface. That is, the Assigned To and the Expiry fields will both populate. The Expiry is shown as a date and adopts a color. So long as the assignment is valid, the date will be green in color and if you hover your mouse over the date, a tooltip will appear informing you of how many days are left to the assignment.

When the assignment expires, the color will turn red and the value will become a clickable link which will launch a small dialogue for renewing the assignment, such as you can see in figure 16.

1. Enter the Key Manager interface as described in SECTION 3.2.
2. LOCATE the key record with the expired assignment; CLICK on the red date in the Expiry field.
3. ENTER a new date that is at least twenty-four (24) hours ahead of the current date.
4. Optionally, ENABLE the notify key holder flag which will e-mail a notice to the assigned key holder.
5. CLICK, Continue
6. REVIEW your changes
7. CLICK, Submit

To purge a key assignment:

There are a couple of different approaches you can take to end an assignment; in fact, the key holder can end the assignment by reporting the key as lost or broken (see SECTION 4.2 View My Keys). More directly, you can open the key editor and change the status to lost or broken. This will purge the assignment and leave an appropriate comment in the key’s historical record.
In a more direct approach, the Status field of the Key Manager interface will become a link if the status is one of: assigned, stored, or transit. You can click this link and a small dialogue will appear that will allow you to force an immediate change to the key’s state.

The change is immediate and an appropriate entry will be made against the key’s historical record. Note that in the above example, we changed the state to Transit; this is not meant to be a long term state, the key should now be assigned or placed into storage. If keys are left in Transit for too long, a TaskMon process will begin to harass you.
3.2.7 Recovering Lost Keys
As we discussed briefly and indirectly in Section 3.2.6, keys can be set to a *Lost* state via a couple different approaches. However, should that key later be found again, there is only one way to reclaim it. As with forcing a state change, if the key’s current *Status* value is *Lost*, the status value becomes a link; clicking this link will launch a small dialogue which will allow you to reclaim the key.

![Recovering a lost key](image)

When you restore the key, an appropriate entry will be inserted into the key’s historical record. It will be restored to the key group that was last managing it, and its new status will be *Transit*; you will need to assign the key or place it into storage.
3.2.8 Storing Keys
Before you can store keys, you will need to have a Facilities Object created that is capable of acting as key storage. If you are not yet familiar with Facility Objects (FO) then please review SECTION 4.1 before proceeding with these instructions.

To place keys in storage:

1. Enter the Key Manager interface as described in SECTION 3.2.
2. Locate one or more key records that you wish to relocate to storage and select them by setting the appropriate checkbox on the far-left of the main interface.
3. Locate & click the button labeled Store Key; this will launch the KMS Key Storage Assignment dialogue.

At this point, you should see a very simple dialogue with little more than just a check box, such as:

![Default key storage dialogue](image)

If the key you are storing has previously been in storage, and you simply wish to put the key back where it was; do nothing. Click Continue and Submit the dialogue; the key will be returned to its last known storage location. A key’s last known storage location is viewable via the Key’s View Key report (see SECTION 3.2.1 for details). If however, the key has never been in storage or if you wish to place it in a new location, deselect the check box and continue:
4. Determine a sort ordering for the Building menu; sort by Code of Name.
5. Select the Building the key will be stored in.
6. Select the Room the key will be stored in.
7. Select the Object the key will be stored in.
8. Optionally, **check** the *Restricted Note* checkbox if you would like the note to be viewable by only you.
9. **Click** *Continue*, this will bring you to a confirmation of the changes you have made.
10. Optionally, **click** *Previous*, if you’d like to change any values.
11. **Click** *Submit* when done.

*Note* that you may store multiple keys at the same time; however they must all be going to the same storage location or all selected keys must be heading to their last known storage location.
3.3 Key Rings

Key rings are physical organizational units employed by many throughout the university. Multiple keys are grouped together onto a single ring and managed as a cohesive unit. When a key is placed onto a key ring that key essentially gives up its individual identity, electing instead to be managed via the key ring as a group. An assignment to key holders and placement into storage is all handled via the key ring mechanics available in the Key Ring Manager rather than the tools in the Key Manager. As such, the tools available to you in the Key Ring Manager are intentionally, very similar to the key ones.

As with keys, we'll suggest that you have put some thought into your organizational structure and have key groups created and waiting to be used prior to beginning work with key ring records for the first time.

To get started with key rings, locate and CLICK the link Manage Key Rings located on the left-hand navigation menu. On the right of the KMS interface, you should now be faced with a list-based managerial display similar to that in FIGURE 21 below.

![Figure 21: Launching the Key Ring Manager](image)
3.3.1 Viewing Key Rings

There exists quite a bit of information as relates to key rings. KMS v2 provides a dialogue which brings all this data together in one place in a read-only state; The View Key Ring dialogue in the Key Ring Manager interface provides you with a static view into all key ring-related data.

Once you have entered the Key Ring Manager, 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 Ring 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 ring. When the dialogue first loads, you will see a small display of the key ring’s vital statistics, such as in FIGURE 22 below.

![Figure 22: Key ring static view](image)

Following the initial key ring view, there are two collapsible data elements intended to provide you with information related to the key ring:

- **Member Keys**, a small tabular display, listing all of the keys that are current members of the key ring. The key’s profile may be viewed via this display by clicking on the small profile icon.
- **Notes attached to the key ring**, all notes related to this key ring 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.

*Note that key rings do not have a historical record per se. Rather, the individual keys continue to maintain the record of what happens to them. For example, if you have a ring with ten (10) keys on it, and you assign the key ring to a key holder, then all ten keys will contain the historical entry regarding the assignment.*
3.3.2 Creating Key Rings

Creating new key rings is a fairly straight forward process. The dialogue acts as somewhat of a wizard, guiding you through the required steps. Be aware that key ring names must be unique across the scope of the key group under which they are created. Also note that keys may only be placed on key rings that are members of the same key group; be conscious of this fact when creating the key ring so that the keys you need to manage will be able to see the key ring when you go to add them.

To create a key ring:

1. Enter the Key Ring Manager interface as described in SECTION 3.3.
2. Locate & click the button labeled Add Key Ring; this will launch the KMS Key Ring Editor dialogue.
3. Type a Name for your new key ring. Names must be between one (1) and thirty-two (32) characters in length and may only include alpha-numeric characters and the following symbols: - _ : . / \ 
4. Select a Profile Group so as to filter the available key groups.
5. Select a Key Group to make the new key ring a member of.
6. Optionally, type a Description of intended purpose for the key ring.
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.

When you click Continue, you will be brought to another display which will allow you to assign the key ring to a key holder. This step is optional, however if you do not assign the key ring, then the next step, storing the key ring, will be mandatory.

The key ring must be assigned or placed into storage during the creation process.

![Figure 23: Creating a new key ring.](image)
If you choose to assign the key ring:

9. **TYPE** a Cornell Net Id into the **Key Holder** field. The user you enter does not need to be a current KMS user, but he must possess a Cornell Net Id. As you type, a menu may appear offering suggestions; simply **CLICK** on any value that might complete your selection.

10. **TYPE** a date into the **Assignment Expiry** field in the format: mm/dd/yyyy. The date must be at least twenty-four (24) hours in advance of your current time. Optionally, a date-picker is available by **CLICKING** the small calendar icon located at the end of the date field.

11. Optionally, **ENABLE** the **Responsible Party** flag if the assignment is being made to a Cornell employee that will in turn disburse the key as temporary access to third parties.

12. **CLICK** Continue

13. **REVIEW** your settings

14. **CLICK** Previous to go back a step and make change or **CLICK** Submit to complete the process.

If you choose to store the key ring:

9. **SELECT** a **Building** from the provided menu.

10. **SELECT** a **Room** the key ring will be stored in.

11. **SELECT** an **Object** to store the key ring in.

12. **CLICK** Continue

13. **REVIEW** your settings

14. **CLICK** Previous to go back a step and make change or **CLICK** Submit to complete the process.
3.3.3 Editing Key Rings

Editing key rings is less of a process than creating them; the editor concerns itself only with the vital statistics of the key ring itself. There are two notable differences between the edit dialogue and the initial creation one: you are able to force the key rings status to Lost; and you can no longer select a profile group to filter the key groups. You can move the key ring to another group, but it has to be one that is owned by the same profile group.

To edit a key ring:

1. Enter the Key Ring Manager interface as described in SECTION 3.3.
2. LOCATE & SELECT the key ring record you wish to edit by enabling the check box located to the far-left of the main interface.
3. LOCATE & CLICK the button labeled Edit Key Ring; this will launch the KMS Key Ring Editor dialogue.
4. Optionally, EDIT the key ring Name being mindful of the limitations explained in section 3.3.2.
5. Optionally, you may declare the key ring as Lost; ENABLE the Key Status flag.
6. Optionally, you may change key group membership; SELECT a new Key Group.
7. Optionally, you may EDIT the Description text.
8. Optionally, CHECK the Restricted Note checkbox if you would like the note to be viewable by only you.
9. CLICK Continue, this will bring you to a confirmation of the changes you have made.
10. Optionally, CLICK Previous, if you’d like to change any values.
11. CLICK Submit when done.

Figure 25: Editing a Key Ring record
3.3.4 Managing Key Ring Group Membership
All key rings must belong to a key group, and only a single key group. When a new key ring is created and first recorded, it is placed into a group as part of its instantiation process. If for some reason you later need to change that affiliation, this dialogue will be of use to you.

You may at any time elect to change the key’s group membership via the KMS Key Ring Groups Membership Editor located on the Key Ring Manager interface.

To change a key rings group affiliation:

1. Enter the Key Ring Manager interface as described in SECTION 3.3.
2. Locate one or more key ring records that you wish to edit and select them by setting the appropriate checkbox on the far-left of the main interface.
3. Locate & click the button labeled Add to Group; this will launch the KMS Key Ring Groups Membership Editor dialogue.
4. Select a new Key Group from the provided menu.
5. Optionally, type any Note you would like to add to the profile.
6. Optionally, check the Restricted Note checkbox if you would like the note to be viewable by only you.
7. Click Continue, this will bring you to a confirmation of the changes you have made.
8. Optionally, click Previous, if you’d like to change any values.
9. Click Submit when done.
3.3.5 Managing Member Keys

As an alternative to assigning keys to rings from the Key Manager interface (see SECTION 3.2.4), you can use the member key manager to move keys onto and off of a key ring. The dialogue will provide you with lists of keys already on the key ring, or eligible to be added. Keys are considered to eligible to be added if they share a key group with the key ring. The keys are expressed as [key stamp] [sequence].

To manage a key ring’s member keys:

1. Enter the Key Ring Manager interface as described in SECTION 3.3.
2. LOCATE the key ring record that you wish to work with and SELECT it by setting the appropriate checkbox on the far-left of the main interface.
3. LOCATE & CLICK the button labeled Manage Keys; this will launch the Manage Member Keys dialogue (see FIGURE 26).
4. Member keys are those already on the ring. To remove keys from the ring, SELECT one or more from the member keys menu.
5. Eligible keys are those that share a common key group with the ring and may be added. SELECT one or more keys from the eligible keys menu to add them to the ring.
6. Optionally, you may filter the eligible keys menu by their relevance to a facility and room.
7. Optionally, CLICK add a note to the next commit to attach a note to the key ring during your next action. Selecting the checkbox will force a notes field to appear.
8. CLICK Commit to save your changes. Newly added keys should now appear in the member keys menu and removed keys should now be in the eligible keys menu.
9. As soon as you have made a change to the key ring, a second button labeled Finished will appear. CLICK Finished when you are done making changes.
10. CLICK Close Window to close the dialogue.

![Figure 26: Managing member keys](image)
3.3.6 Assigning Key Rings
Assigning key rings is pretty much the same process as assigning keys (see SECTION 3.2.5). In fact, all of the tools created to work with key assignments were specifically designed to work with both keys and key rings; if you become comfortable with the various processes for one, you will also gain an understanding of the other.

To assign a key to a key holder:

11. Enter the Key Ring Manager interface as described in SECTION 3.3.
12. LOCATE one or more key ring records that you wish to assign to a key holder and SELECT them by setting the appropriate checkbox on the far-left of the main interface.
13. LOCATE & CLICK the button labeled Assign Key Rings; this will launch the KMS Key Ring Assignment dialogue.
14. TYPE a Cornell Net Id into the Key Holder field. The user you enter does not need to be a current KMS user, but he must possess a Cornell Net Id. As you type, a menu may appear offering suggestions; simply CLICK on any value that might complete your selection.
15. TYPE a date into the Assignment Expiry field in the format: mm/dd/yyyy. The date must be at least twenty-four (24) hours in advance of your current time. Optionally, a date-picker is available by CLICKING the small calendar icon located at the end of the date field.
16. Optionally, ENABLE the Responsible Party flag if the assignment is being made to a Cornell employee that will in turn disburse the key as temporary access to third parties.
17. Optionally, ENABLE the override existing assignments flag. This will purge any pre-existing assignments prior to making the new one.
18. OPTIONALLY, TYPE any Note you would like to add to the profile.
19. Optionally, CHECK the Restricted Note checkbox if you would like the note to be viewable by only you.
20. CLICK Continue, this will bring you to a confirmation of the changes you have made.
21. Optionally, CLICK Previous, if you’d like to change any values.
22. CLICK Submit when done.

![Figure 27: Assigning a key ring to a key holder](image-url)
3.3.7 Storing Key Rings
Before you can store key rings, you will need to have a Facilities Object created that is capable of acting as key storage. If you are not yet familiar with Facility Objects (FO) then please review SECTION 4.1 before proceeding with these instructions.

To place key rings in storage:

1. Enter the Key Ring Manager interface as described in SECTION 3.3.
2. LOCATE one or more key ring records that you wish to relocate to storage and SELECT them by setting the appropriate checkbox on the far-left of the main interface.
3. LOCATE & CLICK the button labeled Store Key Rings; this will launch the KMS Key Ring Storage Assignment dialogue.

At this point, you should see a very simple dialogue with little more than just a check box, such as:

![Default key ring storage dialogue](image)

If the key ring you are storing has previously been in storage, and you simply wish to put the key ring back where it was; do nothing. CLICK Continue and Submit the dialogue; the key will be returned to its last known storage location. A key’s last known storage location is viewable via the Key ring’s View Key Ring report (see SECTION 3.3.1 for details). If however, the key ring has never been in storage or if you wish to place it in a new location, DESELECT the check box and continue:
4. Determine a sort ordering for the Building menu; sort by Code of Name.
5. Select the Building the ring will be stored in.
6. Select the Room the ring will be stored in.
7. Select the Object the ring will be stored in.
8. Optionally, check the Restricted Note checkbox if you would like the note to be viewable by only you.
9. Click Continue, this will bring you to a confirmation of the changes you have made.
10. Optionally, click Previous, if you'd like to change any values.
11. Click Submit when done.

*Note that you may store multiple key rings at the same time; however they must all be going to the same storage location OR all selected key rings must be heading to their last known storage location.
3.4 Profiles
As a KCC you will be granted limited access to the KMS v2 Profile Manager. The manager interface will give you access to the tools which will enable you to view profile records, manage access locations, and create key instances.

To get started with profiles, locate and **click** the link *Manage Profiles* located on the left-hand navigation menu. On the right of the KMS interface, you should now be faced with a list-based managerial display similar to that in **Figure 29** below.

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
- Manage profile access locations
- Create key instances & more!
3.4.1 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 30 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.*
3.4.2 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.
3.4.3 Deleting Access Locations

There are use cases under which you 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 32:

![Figure 32: 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 34: deleting an access location](image)
3.4.4 Creating Keys

We should start our key creation topic with the comment that it is not desirable for KCCs to create keys. These tools are provided to give you the ability to document pre-existing keys that you may or may not have had previous knowledge of. However, it is the rare case when a KCC would actually be cutting physical keys, and it is at that point in time that the key really must be entered into the system if we are to obtain and maintain a true chain of custody for the instance. With that said...

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 Key Manager interface (see **SECTION 3.2**).

*Note that the Key set and Key cut values are supplied for reference only.*
Figure 35: 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:

![Diagram of key creation interface](image)

**Figure 36: Differences in creating multiple keys.**

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 35** 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**.
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 and 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 out of the box with more than 63,000 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 to 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 and managed 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.

![Facility 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 38: 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 38 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 41: 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 straight forward 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 straight forward 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>KMS v2 main interface</td>
<td>7</td>
</tr>
<tr>
<td>2</td>
<td>Navigation Details</td>
<td>8</td>
</tr>
<tr>
<td>3</td>
<td>Example of a KMS v2 managerial interface</td>
<td>8</td>
</tr>
<tr>
<td>4</td>
<td>KMS data filter flow</td>
<td>9</td>
</tr>
<tr>
<td>5</td>
<td>Hovering your pointer over the key ring name in the key manager interface</td>
<td>10</td>
</tr>
<tr>
<td>6</td>
<td>Key manager with notes menu expanded</td>
<td>11</td>
</tr>
<tr>
<td>7</td>
<td>Keys tab navigation</td>
<td>15</td>
</tr>
<tr>
<td>8</td>
<td>Creating a new key group</td>
<td>16</td>
</tr>
<tr>
<td>9</td>
<td>Editing a pre-existing key group</td>
<td>17</td>
</tr>
<tr>
<td>10</td>
<td>Managing key group access for AKCCs</td>
<td>18</td>
</tr>
<tr>
<td>11</td>
<td>Launching the Key Manager interface</td>
<td>19</td>
</tr>
<tr>
<td>12</td>
<td>Static key view</td>
<td>21</td>
</tr>
<tr>
<td>13</td>
<td>Key Editor Dialogue</td>
<td>22</td>
</tr>
<tr>
<td>14</td>
<td>Key editor duplication override flag</td>
<td>23</td>
</tr>
<tr>
<td>15</td>
<td>Key assignment dialogue</td>
<td>26</td>
</tr>
<tr>
<td>16</td>
<td>Renewing a key assignment</td>
<td>27</td>
</tr>
<tr>
<td>17</td>
<td>Forcing an assigned key to transit state</td>
<td>28</td>
</tr>
<tr>
<td>18</td>
<td>Recovering a lost key</td>
<td>29</td>
</tr>
<tr>
<td>19</td>
<td>Default key storage dialogue</td>
<td>30</td>
</tr>
<tr>
<td>20</td>
<td>Placing keys into storage</td>
<td>31</td>
</tr>
<tr>
<td>21</td>
<td>Launching the Key Ring Manager</td>
<td>32</td>
</tr>
<tr>
<td>22</td>
<td>Key ring static view</td>
<td>33</td>
</tr>
<tr>
<td>23</td>
<td>Creating a new key ring</td>
<td>34</td>
</tr>
<tr>
<td>24</td>
<td>Completing the key ring creation process</td>
<td>35</td>
</tr>
<tr>
<td>25</td>
<td>Editing a Key Ring record</td>
<td>36</td>
</tr>
<tr>
<td>26</td>
<td>Managing member keys</td>
<td>38</td>
</tr>
<tr>
<td>27</td>
<td>Assigning a key ring to a key holder</td>
<td>39</td>
</tr>
<tr>
<td>28</td>
<td>Default key ring storage dialogue</td>
<td>40</td>
</tr>
<tr>
<td>29</td>
<td>Placing key rings into storage</td>
<td>41</td>
</tr>
<tr>
<td>30</td>
<td>Launching the profile manager</td>
<td>42</td>
</tr>
<tr>
<td>31</td>
<td>Profile Static View</td>
<td>43</td>
</tr>
<tr>
<td>32</td>
<td>Adding a new access location</td>
<td>44</td>
</tr>
<tr>
<td>33</td>
<td>Example profile tree</td>
<td>45</td>
</tr>
<tr>
<td>34</td>
<td>deleting an access location</td>
<td>45</td>
</tr>
<tr>
<td>35</td>
<td>The key creation process for a single key</td>
<td>47</td>
</tr>
<tr>
<td>36</td>
<td>Differences in creating multiple keys</td>
<td>48</td>
</tr>
<tr>
<td>37</td>
<td>Navigating to the Facilities Object Manager</td>
<td>50</td>
</tr>
<tr>
<td>38</td>
<td>Facilities Object Manager</td>
<td>51</td>
</tr>
<tr>
<td>39</td>
<td>Creating a new object</td>
<td>53</td>
</tr>
<tr>
<td>40</td>
<td>Creating a new child object</td>
<td>53</td>
</tr>
<tr>
<td>41</td>
<td>Object batch creation</td>
<td>54</td>
</tr>
<tr>
<td>42</td>
<td>Editing a Facility Object</td>
<td>55</td>
</tr>
</tbody>
</table>
Figure 43: My Keys inventory interface; available to the entire KMS vested community. ............................... 58