*E*nterprise *I*dentity *M*anagement

User Guide

Version 3.0

Prepared By:

Commonwealth Office of Technology
Office of the CISO

Kentucky
UNBRIDLED SPIRIT ™

TABLE OF CONTENTS

Welcome to the Enterprise Identity Management User Guide!

Purpose	Audience
Introduce and familiarize the reader with the Commonwealth Office of Technology's (COT) system for user identity management.	Any personnel, including Human Resource and Authorized Agency Contacts, that will be involved with requesting identities and other services from COT.

In this guide, you will learn about COT's identity management system:

Enterprise Identity Management

We will discuss how EIM operates, as well as how it affects Agency request procedures for creating, modifying, and removing basic user identities.

Section 1 will focus on introducing you to these new concepts.

Section 2 overviews how identity management operates.

Section 3 walks through the Enterprise Identity Management Portal.

Section 4 highlights the miscellaneous information related to COT's solution.

If you have any questions about anything listed in this document, please contact:

Commonwealth Service Desk
CommonwealthServiceDesk@ky.gov
502-564-7576 or 888-372-7434
Monday – Friday 6:30AM to 6:00PM EST
Saturday – 7:30AM to 1:00PM EST

Section 1: Introduction to EIM

Enterprise Identity Management (EIM for short) is the Commonwealth Office of Technology's (COT) solution for identity management for employees and other users in the Commonwealth.

In order to understand EIM and its benefits, let us first define a couple concepts.

EIM Definitions

Enterprise: A standardized and centralized solution for the Enterprise, particularly those in the Executive Branch of state government.

Identity: When this guide speaks of an identity, it is referring to an account or service that identified with a user. These are usually accounts that a user logs in with a username and password, such the Windows/Network account and email.

Management: Management refers to actions taken on identities, such as creating an account, modifying one, or removing it.

Putting these together, we can define EIM as a centralized system designed to standardize account creation, modification, and removal for users in the Commonwealth.

There are three core accounts that EIM will manage the Commonwealth's users:

- Active Directory (known as your Windows/Network login)
- Email
- Home Folder

These three identities are the most common to users among the Commonwealth.

EIM will have impact into other systems as well. These include email billing, and telephone numbers. We will address this more in depth in a later section.

Benefits of EIM

Now that we understand that EIM is a method of managing these common user accounts, let us look at the benefits of EIM management by starting with the current method.

Before the implementation of EIM, when an Agency had a new user begin, requesting the necessary accounts and services was a manual process. It usually began by emailing the Commonwealth Service Desk with a description of the request, including any necessary forms and authorizations. The Service Desk would then open a ticket and assign it to any relevant COT groups who would manually create any accounts requested. This time and resource intensive process was repeated for existing users, as well that needed additional services from COT.

EIM has centralized the majority of this process into one system. Perhaps EIM's biggest benefit is the capacity for *automatic* account management. Let us look at how it works.

Organizational Structure

When a user starts, they will align to some level in the Commonwealth's organizational structure. EIM recognizes seven levels of structure:

- Org level 1: Cabinet
- Org level 2: Agency
- Org level 3: Office
- Org level 4: Division
- Org level 5: Branch
- Org level 6: Section
- Org level 7: Unit

Each Cabinet will designate two things on every level of their organizational structure, both of which are critical to EIM account management.

1 – EIM uses organizational structure to determine which accounts to manage.
EIM uses the lowest org level a user receives to determine which types of accounts they should have. Cabinet leadership representatives are able to specify which of the three accounts EIM will manage on every organization level in their Cabinet.

For example, one Branch may have EIM set to manage all three of the core identities. However, another Branch may determine the users in that org level only need a Windows/Network account and email. Due to this EIM will manage those two identities, but not Home Folder.

It is important to keep in mind that if a Cabinet opts out of EIM management for any of the core accounts, the option to create it will not exist through EIM. The Agency can request EIM begin

managing these accounts, but until then any requests for these accounts would have to start with the Commonwealth Service Desk per the current method.

<u>2 - To determine whether to automatically create the specified accounts.</u>
EIM also looks at organizational structure to determine whether it should *automatically* create identities for users.

For example, say an Agency has a Section that selected all three-core identities to manage and opted <u>into</u> EIM's automated account creation. When a user starts with this particular Section as their lowest organizational unit, EIM will automatically create this user's three core identities.

If another Agency has a Section that has all three-core identities managed but has opted <u>out</u> of EIM's automated creation, an Agency Authorized Contact or Agency HR Administrator within that Cabinet would manually decide which identities for EIM to create. This manual decision is done through a webpage called the **EIM Portal**, an important aspect of EIM that we will address shortly.

Sources of User Information

Now let us take a closer look at the different types of users that come into the Commonwealth and more specifically the main source of information that EIM reads.

Main Source: KHRIS

The EIM system reads (synchronizes) user information from KHRIS, the Kentucky Human Resource Information System.

EIM synchronizes with KHRIS and reads in all relevant employee data (excludes sensitive *personal* data). This sets up a database of user records in EIM, known as EIM portal profiles, which is searchable via the Portal. EIM synchronizes several times a day with KHRIS and reads in information for additions and changes to user records.

These additions and changes could come in many forms. When EIM sees user information in KHRIS that is different from the information in that user's EIM portal record, it will take appropriate action on the user's accounts. Here are a couple examples.

- A new user in KHRIS that is not currently in EIM:
  - EIM Portal profile is created for new user based on information read in from KHRIS.
  - EIM will look at the user's lowest organizational level to determine managed accounts and whether or not automatically create them.

- Information modified for a user in KHRIS does not match EIM, such as work address or name.

- EIM will update the user's portal record with the KHRIS information, and push that information out to any managed accounts that use it.
  - Organizational changes.
    - Transfers are considered organizational changes; EIM has very specific rules set up to accommodate the many facets. We go into greater depth below.
  - User exits such as separations and retirements.
    - If EIM manages accounts for a user who exits, it will disable their accounts and set them for deletion according to COT's account retention practices.

KHRIS is the Gold Source of information for state employees and contractors established in KHRIS. KHRIS becomes the Gold Source of information for their accounts. Any information changes needed for these users must be entered in KHRIS. Once information in KHRIS changes, EIM will read the information in the next sync and update their accounts accordingly.

A couple notes about EIM and KHRIS integration:

- Two main pieces of user information will never come from KHRIS are telephone number and email addresses. If EIM receives an email address for a user who is in KHRIS, an outbound file that contains a user's state email address goes to KHRIS. The email address is the only information that EIM will send back to KHRIS.

Secondary Source: EIM Portal

The other source of users will be the EIM Portal.

COT accounts and services who are not established in KHRIS, such as contractors, vendors, temporary workers and unpaid interns. In these cases, an EIM Agency Authorized Contact or Agency HR Administrator must log into the EIM Portal and create the user profile directly in the portal and provision accounts. This will allow them to choose their name, employee type, work information, contact information, and Report to Manager they report to. Regarding manager, EIM will take the org structure of the manager and apply it to the user.

Much like those that come from KHRIS, when a non-KHRIS user is created in the Portal, assigned their org structure, EIM will look to see if the lowest level present is set to automatically create. If so, it will go ahead and create all accounts the Cabinet has designated for that org level.

- Vendors are an exception to automatic creation, and will never have their accounts automatically created. An Agency Authorized Contact or Agency HR Administrator must choose vendor identities accounts manually through the EIM Portal after their profile is created.

EIM Portal

We have talked a bit about the EIM Portal, and will be going over it in depth in a coming section. For now, let us do a brief recap.

- Each cabinet leadership will select certain individuals, known as Agency Authorized Contacts, who can log in and access the EIM Portal.
  - Agency Authorized Contacts will only be able to see users within the Cabinet they align too.
  - General Government Cabinet is the exception to this, as they will only be able to see users in their Agency.
- Agency Authorized Contacts can view the EIM Portal profile for users and contractors that came from KHRIS.
  - Most information is read only since information changes for users in KHRIS must begin in the KHRIS system.
    - Office phone, mobile phone, and fax can be entered via the EIM Portal since this information will not come from KHRIS. This information will then flow down to their accounts.
    - Accounts can be added or removed as required by the Agency.
- Agency Authorized Contacts can create/modify/remove Portal accounts for users who **are not** in KHRIS.
  - This includes adding or removing accounts.
- Agency Authorized Contacts can view EIM profiles for users who **are** in KHRIS.
  - User information read in from KHRIS is READ only. Since the source of information for state employees and contractors established in KHRIS. Changes are made in KHRIS, and read in by EIM. Work Telephone Number, Fax Telephone Number and Mobile Telephone is the only information that can be entered on a user's portal profile via EIM, if user is coming from KHRIS.
  - Accounts can be added and removed as well.

Section 2: How EIM works

In this section, we will walk through EIM account management for both users in KHRIS and those added through the Portal. This will help us get an understanding of how EIM works in each scenario.

Now let us take a closer look at the different types of users that come into the Commonwealth, and more specifically the sources that EIM will read them from.

Overview of Management for Users in KHRIS

Since the majority of users who utilize COT accounts and services will be loaded into KHRIS, let us dive deeper in the KHRIS/EIM connection first. We will look at each of the four types of management: creations, modifications, transfers, and removals.

EIM finds a new user in KHRIS

An Agency hires a new State Employee and enters them into KHRIS. The next time EIM syncs will KHRIS, it will see that this user did not exist in EIM previously, and will begin the steps to evaluate what it needs to do.

1. EIM will read all relevant user information from KHRIS and create this user a profile in the EIM Portal. This means that even if an account is not created, this user will still be searchable in the Portal.
2. EIM will create the user's unique account name that their Network account and email will use and Home Folder. More on the account name creation below.
3. EIM will then evaluate the user's lowest organizational level to determine what it needs to do about the user's identities.
    a. It will first look to see if COT (and therefore EIM) manages the accounts for this org level.
        i. If EIM does **not** manage this org level, the user is considered non-managed and any accounts needed from COT must be requested outside of EIM. More on this in the section below concerning non-managed agencies.
        ii. If EIM **does** manage this org level, EIM will then look to see if this org level has been opted into automatic creation.
            1. If **no**, then an EIM Agency Authorized Contact will need to open the user's Portal Profile and manually check which account they will need. When selected and submitted, EIM will create the accounts.

2. If **yes**, EIM will automatically create any managed account for that org level. The account is created up to 10 days prior to the Start Date.

EIM finds modified user data in KHRIS

For this scenario, let us say a user requires a modification to their work information in KHRIS. Once information is modified, EIM will notice that the information in KHRIS for this user is now different from the information in the Portal. The Portal profile for the user will updated, and EIM will push any relevant changes to the user accounts.

This includes any data change except for organizational data. Organizational data changes are considered transfers and covered below.

It is important to note that name changes are especially sensitive since a name change will change the account name a user logs into their computer with, as well as their email address and home folder. More on this in the section on User Naming.

Finally, the only information that can be updated via the EIM Portal for a user in KHRIS is office phone, mobile, and fax number.

EIM finds a user with different organization in KHRIS

When EIM finds a user's organization has changed, it processes as a transfer. EIM recognizes two types of transfers: External (Cabinet to Cabinet) and Internal (agency to agency within same Cabinet).

- External transfer - A transfer that is considered "external" by EIM when the employee moves to a different Cabinet.
    - The user's network account from the previous Cabinet will be deleted. If necessary, it can be recovered within the 90-day timeframe.
    - While this frees up the employee's email **address** to use at their new job, it will disconnect the **content of their mailbox**.

    If the losing agency needs the email content, the Email Review request service offering must be submitted through Service Now.
- Internal transfer - A transfer is considered "internal" by EIM when the employee moves within the same Cabinet (Agency level or lower).
    - An employee that transfers internally will keep whatever accounts and permissions they had previously, including their email address. The employees work information updates to reflect their current position since EIM will see the information in KHRIS.

o It is extremely important to note that agencies will need to be cognizant that if any access and permissions, such as Network Shares, AD Group Permissions that the account has will move with the employee. If access and permissions should not move with the employee during an internal agency to agency transfer within the same Cabinet, an agency will need to send in a IT Service Request to the Commonwealth Service Desk to remove any access and permissions the employee no longer needs prior to the internal agency to agency transfer within the same Cabinet.

EIM finds a user in KHRIS that is leaving employment

When an employee leaves employment with the Commonwealth, EIM will take specific action when it sees these in KHRIS. The below also applies if a user is completely removed from KHRIS.

Once the end/effective date for the employee exit has come, EIM will disable any of their accounts and set them for deletion.

- The user's network account will be disabled for 90 days, at which time it will be removed.
- This action will disconnect the **content of their mailbox** 48 hours after the exit effective date. If the Agency needs the email content, the Email Review request service offering must be submitted through Service Now.

Overview of Management for Users Not in KHRIS

Now let us look over the four management scenarios for those users who are not in KHRIS.

A new user created in the EIM Portal

When an Agency has a non-KHRIS user start with the Commonwealth, the EIM Agency Authorized Contacts or Agency HR Administrator will need to create them manually through the Portal.

1. The Authorized Contact will begin the New User creation steps within the Portal's User section.
2. They will fill in relevant information including information that EIM requires, such as name, employee type, and manager.
   a. The report to manager is important, as the new user will copy the selected manager's organization structure. Much like those in KHRIS, this is how EIM determines which accounts EIM manages and automatically creates.
3. Once the new user has been submitted in the Portal, EIM will take a few moments to create the user's profile.

a. This include determining the unique account name that their Network account and email will use. More on the account name creation below.

4. EIM will then evaluate the user's lowest organizational level to determine what it needs to do about the user's identities.

a. EIM will first look to see which accounts the Cabinet requested be managed on the user's lowest organization level.

b. EIM will then look to see if this org level has been opted into automatic creation.

    i. If **no**, then an EIM Authorized Contact will need to open the employee's Portal Profile and manually check which account they will need. Once selected and submitted, EIM will create the accounts.

    ii. If **yes**, EIM will automatically create any managed account for that org level. The account will be created up to 10 days prior to the Start Date.

An existing user is modified in the EIM Portal

Modifying a user, who is not in KHRIS, is done completely through the EIM Portal. Simply search for the user and open their profile. From here, you will be able to change most information about this user.

- Please be aware that once submitted these changes are pushed down to the user accounts.
- Changing any part of the user's organization structure is considered a transfer, which is covered next.
- While most information can be modified for a non-KHRIS user through the Portal, some data cannot be modified directly. We will address these fields in the next section on the EIM Portal.

An existing user transferred in the EIM Portal

Transfers mostly work the same for KHRIS and Non-KHRIS users. There are unique aspects to consider:

- Transferring a Non-KHRIS user means manually modifying Organization Structure in the Portal.
  - Organizational level is visible in the Global Address Book (if the user has email).
  - Organizational levels can be left blank if necessary.
  - When you search a particular level, please make sure you are selecting the correct organization for the level you are modifying. For example, we do not want to put an Agency in the Section level.
  - Keep in mind that once you submit the organizational changes, EIM will evaluate based on two criteria:
    - External vs Internal transfer. This behaves exactly as described earlier.

- Will create accounts based on the lowest organizational level if necessary.
- A Non-KHRIS user transferring to a different Cabinet.
  - When created through the EIM Portal, a user will be tied to their Cabinet and that organizational level it will not be able to be modified directly. If they transfer to a new Cabinet, their current profile will need to be deprovisioned (by adding an end date in their current profile) and then a new profile will need to be created. The new profile will need to choose a manager in the new Cabinet so the user will copy their org structure.
- However, there is a special consideration when transferring a non-KHRIS user since it must be done through the Portal.

<u>A user is exiting the Commonwealth</u>

In order to exit a non-KHRIS user, you will need to open their EIM profile and set an END DATE. Once the end date for the employee has come, EIM will disable any of their accounts and set them for deletion per COT retention policy.

- The user's network account will is disabled for 90 days, at which time it will be removed. This action will disconnect the **content of their mailbox** 48 hours after the end date. If the Agency needs the email content, the Email Review request service offering must be submitted through Service Now.

User Account Naming and Display

Let's briefly look over how EIM handles usernames, starting with how they are created.

- EIM will calculate the username for a user when their profile is created. This username will be used if the user receives any accounts, including their email address.
- EIM looks at all network accounts to make sure the account it creates a unique username.
  - Note for Active Directory accounts, the username chosen will be unique across all of Active Directory, and not just the user's domain.
- The users email address will also use this account name.
- Display name is calculated based on these names.
  - Last Name, Preferred/First Name (Agency Acronym)

Let us look at an example user: Anthony "Tony" Franklin Doe:

Legal First Name	Preferred First Name	Middle Name	Last Name
Anthony	Tony	Franklin	Doe

PreferredFirstName.LastName	Tony.Doe
PreferredFirstNameMiddleInitial.LastName	TonyF.Doe
LegalFirstName.LastName	Anthony.Doe
LegalFirstNameMiddleInitial.LastName	AnthonyF.Doe
PreferredFirstInitialLastName	TDoe
LegalFirstInitialLastName	ADoe
PreferredFirstInitialMiddleInitial.LastName	TFDoe
LegalFirstInitialMiddleInitial.LastName	AFDoe
PreferredFirstNameLastInitial	TonyD
LegalFirstNameLastInitial	AnthonyD

For this employee, EIM will go down the list until it finds a username combination that is not already in use. If "Tony.Doe" and "TonyF.Doe" are already in use, this employee will receive "Anthony.Doe" as his Network account/email. Note that not all employees will have a Middle Name or a different Legal/Preferred name, so steps including those would be omitted for those users.

In the unlikely scenario that EIM goes through all available steps and is still unable to find a unique username, COT will be notified to investigate.

Name Changes

If a user's name changes, whether from KHRIS or through the Portal, it will have a great impact to their accounts.

Whenever EIM detects a name has changed, it first will recalculate their account name following the above naming standards. EIM will then update the EIM Portal with their new name, account name, and display name.

From here, it will update any of their accounts, including their Network Account and email (and therefore Global Address Listing). This means the account they log into their computer with

will now be different. If a name change goes through in the middle of the day, it could easily disrupt their business.

When a name change is processed by EIM, a notification will be sent to the manager and alternate contact for this user to inform them of the new account name. It will be important to coordinate with the user so they know their new account name to log into.

If possible, it is preferred to change user names later in the day to help keep business disruptions to a minimum.

Global Address Listing

If a KHRIS or non-KHRIS user receives email, then a portion of their work information will show up in the Global Address Book.

(Example continued on next page)

Doe, Tony F (COT)

Doe, Tony F (COT)

Network Analyst

| General | Organization | Phone/Notes | Member Of | E-mail Addresses |

Cabinet:
Finance and Administration Cabinet

Agency:
Commonwealth Office of Technology

Office:
Office of Chief Info Security Officer

Division:

Branch:
Security Administration Branch

Section: **Unit:**

Manager:

Direct reports:

[Add to Contacts] [Actions]

[OK] [Cancel] [Apply]

Doe, Tony F (COT)

Doe, Tony F (COT)

Network Analyst

| General | Organization | Phone/Notes | Member Of | E-mail Addresses |

Phone numbers

Business:	502-555-5555	Home:	
Business 2:		Home 2:	
Fax:	502-555-5555	Mobile:	502-555-5555
Assistant:		Pager:	

Notes:

[Add to Contacts] [Actions]

[OK] [Cancel] [Apply]

Section 3: Using the EIM Portal

The EIM Portal is an important part of Enterprise Identity Management, and the main resource Agency Authorized Users and Agency HR Administrators will utilize. You can add the following link to Favorites.

EIM IAM Portal link: https://iamportal.ky.gov/IdentityManagement/default.aspx

Currently, the EIM Portal will need to be accessed using **Internet Explorer.** Using other browsers will result in a subpar experience.

- EIM will require pop-up windows, so Internet Explorer Pop-Up Blocker needs to be turned off.
    - This is accomplished by going to Tools, choosing Pop-Up Blocker, and turning it off.
- EIM will also require the Portal be added to Trusted Sites in order to function properly.
    - This accomplished by going Tools and then Internet Options. From the Internet Options window that opens, click the Security tab, choose Local Intranet and then click the Sites button. This opens the Local Intranet window where you should click Advanced. Finally, the last window will allow you to type the site address to add it.

Now let us walk through the Portal and how to use it.

EIM Portal Home Page

The EIM Portal Home Page is very simple, with only a few options you will need to be learn.

- You can immediately search for a user in the upper right corner 'search for:' box.
- Left side menu:
    - You can look at your own EIM Profile.

- You can visit the User Page from the menu on the left.
  - Note the number next to it indicating the user profiles EIM has for your Cabinet.
- Middle options:
  - The options that are also on the left side menu.

From here, let us look at the User Page by clicking Users in left side menu.

Creating a User

From here, we can create a user or search for users in EIM. Remember, you can only look for users in the same Cabinet as you (or in the case of the General Government Cabinet, only those in the same Agency).

Let us start by creating a user so we can search for them later.

Reminder: Only users who <u>are not in KHRIS</u> will need to be created through the EIM Portal.

Note: You will never want to use the Delete option here to remove EIM Portal profiles. There are specific ways to exit users.

Once you click **New**, the Create User window will open to the Employee Information tab.

Employee Information

You will want to fill out all the relevant information for the user you are creating, however only First Name, Last Name, and Manager are required. ***Please note the recommendation, if an employee has a middle name and is known, the middle initial of the employees middle name, should be entered into the Middle Name Field.*** Remember, the user you are creating will copy the selected Manager's organization structure. This determines the accounts EIM will manage for this user and whether or not to automatically create them.

Click Next to move to the next tab.

Work Information

From here, you will need to set their start date and employee type. End date should be left blank.

Click Next to move to the next tab.

Contact Information

This tab lets you specify any contact information for the user. Take note of the required fields*, standard formats, maximum limits and the syntax reminder.

Create User ✕

| Employee Information | Work Information | Contact Information | Summary |

More information

S Y N T A X … R E M I N D E R   No Leading or trailing spaces are allowed on fields below

Work Number

Format as 555-555-5555 or 555-555-5555 Ext 1234 (Case Sensitive)

Fax Number

Format as 555-555-5555

Mobile Number

Format as 555-555-5555

PO Box

Address
*
Maxlimit 128 characters

Work County
[▼]

City
*
Maxlimit 128 characters

State
[Kentucky ▼]

Zip Code
*
Format as 5 Digit 12345 or 9 Digit 12345-6789

Once completed, scroll down to click Next or Finish to review your submission.

Summary

Click Submit to finalize the creation of this user. If something needs to be modified, click Back to return to the previous tabs.

Create User

| Employee Information | Work Information | Contact Information | **Summary** |

Attribute	Value
Address	123 Test Avenue
City	Test City
Employee Start Date	6/1/2016 12:00:00 AM
Employee Type	Temporary
Fax Number	502-555-5555
First Name	Anthony
Job Title	Network Analyst
Last Name	Doe
Manager	Lemay, Katrina L
Middle Name	Franklin
Mobile Number	502-555-5555
Preferred First Name	Tony
Resource Type	User
State	KY
Work Number	502-555-5555
Zip Code	12345

Once submitted, EIM will begin the process of creating the account. Here is a recap of that process from Section 2.

1. EIM will create the user's EIM portal profile.
    a. This include determining the unique account name that their Network account and email will use. More on the account name creation below.
2. EIM will determine which accounts to create.
    a. EIM will first look to see which accounts are managed on the user's org structure.
    b. EIM will then look to see if this org level has been opted into automatic creation.
        i. If **yes**, EIM will automatically create any managed account for that org level. The account will be created up to 10 days prior to the Start Date.
        ii. If **no**, the accounts will need to be manually created by visiting the user's profile Entitlement tab. More on this below.

Now that we have created a user, let us return to the User Page and search for them.

Searching for a User

To start a search, type what you are looking for in the search box on the right hand side.

When you search, below are the fields EIM will look for and return any results that are found:

- Name (Preferred First, First, Middle, and Last Name)
- Display Name
- Account Name
- Email
- Cost Center
- Employee ID or Personnel Number
- Job Title
- Organizational Structure (any of the seven levels)
- Employee Status (Active/Inactive)
- Employee Type (State Employee, Contractor etc.)

This means when you search, it looks in every one of these fields. This means that broad searches may return more results than expected. If you are looking for someone whose last name is Fisher and you only search "Fish", you will see users with the last name Fisher but also those who are in the Department of Fish and Wildlife (since Org is being searched). You want to make your searches as precise as possible.

You can also use % as a wildcard before your search term if you know the letters you are searching for can appear in the middle of a word.

Search term	Result
wa	Found results for first names like Walter and Warren, and last names like Ward and Warner.
%wa	Included the same results as above, but also included results where "wa" was in the middle of a name, such as Howard and Conway.

Enhanced Searching

The basic search will likely suffice for everyday use, however there are times when you need to pull up a specific set of users. Advanced Searching allows you to pinpoint what you are searching for with much greater precision.

When you first click Advanced Search, you may see parameters already in Advanced Search box. If so, simply click the X to the right of each row to remove them.

A blank Advanced Search looks like this (click Add Statement to add a new search):

From here you can define the specific things you want to search. You can specify three things here:

- Left side Attribute: This is the field you want to search, such as First Name or Employee ID.
- Right side Value: This is the text you want to search.
- Middle Operator: This is the criteria for the search, such as "is" or "contains". This lets EIM know how to search.

 Here are a few examples:

- _AgencyName contains Commonwealth
  - o   This searches for all user's whose Agency contains the word "Commonwealth".
- EmployeeID is ABC1234
  - o   This searches for the user whose Employee ID is example ABC1234.
- LastName starts with Robin

o   This search for users whose last name start with Robin, such as Robinson.

You can return to the Basic Search from the Enhanced Search by clicking it on the right.

Once we find the user we want to view (in this case, the user we just created), click their display name to open their profile.

Viewing and Editing a User Profile

Once you have found the user you are looking for, click their name to open their EIM profile. Remember that we can see EIM profiles for both users from KHRIS and those created through the Portal. The fields you are able to edit will be different depending on the user's source.

Employee Information

When a user profile is opened, EIM will default to the Employee Information tab.

- Name (Preferred First, First, Last, Middle): This will display the name information that came from KHRIS or the Portal user creation.
- Display Name: This is the display name calculated by EIM based on the user's name and organization. Display is always "Last Name, First Name (Agency Acronym)"
    - o   EIM will use Preferred First Name if present.
    - o   The Agency Acronym is defined by the organizational level. Each Cabinet can define their acronyms per org level.
- Employee ID and PERNR (Personnel Number): Both KHRIS and Portal users will have a unique employee ID assigned. Personnel Numbers are unique to KHRIS users only.
    - o   The EIM Portal will general a unique employee ID for Portal users when they are created.
- Account Name, Domain, E-mail: This is unique account name that EIM generates for the user. EIM also uses this unique name as the email address. The Domain relates to their Network Account.

- Job Title: If the user has a job title, it will display here. For users in KHRIS, EIM will display the user's position title. If the user has a working title present in KHRIS, it will be used instead.
- Manager: The manager listed for a user will receive notifications on the user's behalf (more on notifications below). Clicking the manager will display a non-editable view of their profile. When creating a Portal user, selecting a manager is especially important, as the user will copy the select manager's organizational structure.
- Alternate Contact: This field allows Agencies to use an alternate contact email for notifications, such as a new account notification. If this field has a valid email, then any notification that would go to the manager would also go to the alternate contact.

Work Information

This tab details information relevant work information.

- Employee Start Date: This is the date and time the employee started.
- Employee End Date: EIM will default a phony far future date for the user's profile. If a non-KHRIS user leaves, this field will have to be manually filled in to properly exit the user.
- Validate Account: This is only used (checked) when an account gets flagged for deletion due to inactivity, and needs to be validated as active by manager or the agency HR authorized contact. More on this in the section concerning Stale Accounts.
- Stale Account: This is only check marked by EIM when an account status is stale greater than 90 days without a log on and disabled per EIM policy.
- On Leave: When this box is checked, EIM is receiving an "On Leave" status from KHRIS for the user.
- Email Forwarding Enabled: When checked mail addressed to the user's mailbox is being forwarded.
- Short Term Disable: Checking this box will also disable a user's access, but will also prevent their account from being flagged for deletion due to inactivity. This is to be used in short-term situations where access needs to be restricted, such as FMLA or Military Leave.
- *Held Disabled: When checked, user network access is held disabled for the reason specified below by the Security Administrator. *Restricted use by COT IAM Security.
- *Reason Held Disabled: The reason the account is being held disabled. Reasons are:

Phishing Responder
Management Directed
Duplicate Account

*Restricted use by COT IAM Security.

- Immediate Termination: Checking this box will disable the user's Network access and Disable (remove) the email account to prevent a user from logging in with their AD\Network account. ***This should only be used when an existing employee needs access revoked immediately***. A termination from KHRIS/Portal will still need to follow to deprovision them. ***Please note that if an Agency Authorized Contact or Agency HR Administrator inadvertently uses this, the employees email account will disconnect (be removed), a separate request to the Commonwealth Service Desk would have to be sent in order for the employees' mailbox to be reconnected.*** Caution and due diligence must be used to ensure this is not used unless an employee's access needs to be revoked immediately.
- Employee Type: This simply displays the employee type, such as State Employee, KHRIS Contractor, Contractor, Intern, Temporary, or Vendor.

- Contracting Company: Authorized Contacts will have the ability to specify a company for contractors they add through the EIM Portal.

Doe, Tony F (DOR)

| Employee Information | Work Information | Contact Information | Org Structure | Entitlements | Other Entitlements |

Employee Start Date

6/1/2015

Format as M/d/yyyy

Employee End Date

12/30/2500

Format as M/d/yyyy

Validate Account

If you received a notification stating this account is scheduled for deletion due to inactivity, validating the account will keep it enabled for 45 days. ☐

Stale Account

Stale >90 days w/o logon - when checked account is disabled ☐

On Leave

When checked, EIM is receiving an On Leave status from KHRIS ☐

Email Forwarding Enabled

When checked mail addressed to the user's mailbox is being forwarded. ☐

Short Term Disable

While checked, user network access will be disabled. ☐

*Held Disabled

When checked, user network access will be held disabled for reason specified below by Security Administrator ☐

*Reason Held Disabled

The reason the account is being held disabled. [dropdown ∨]

Immediate Disable

When checked, user network access will be disabled while the termination process is completed in either KHRIS or the Portal. This should only be used when an existing employee needs access revoked immediately. The employee's email account will disconnect (be removed). Please see User Guide for more information. ☐

Employee Type

Contractor

Contracting Company

Adecco

Contact Information

This tab lists any contact information for this user.

- Work Number: This is the employee main work telephone number. More on this topic in the section below on Pinnacle.
- Pinnacle: When this box is checked, EIM is receiving an assigned VoIP work phone number that has been assigned to a user. VoIP work phone numbers assigned are read into EIM, from Pinnacle once assigned.
- Fax and Mobile Number: These fields will be editable in the EIM Portal when necessary, and will update the users Network account and Global Address Book.
- PO BOX: If the user has been given a PO BOX, it will show up here. Note that some records from KHRIS have PO BOX in an address line and will therefore show there.
- Address: The other fields pertain to their work address, such as their street and city.

Org Structure

This tab shows the user's current organizational structure. The seven levels are listed, alongside the Cost Center, which displays the Cabinet/Agency's cost center code. Keep in mind due to the varying structure of each cabinet, users will not have all seven levels defined.

In this case, of our example Tony Doe, we can see he copied the Org Structure from his manager.

Doe, Tony F (DOR)

| Employee Information | Work Information | Contact Information | Org Structure | Entitlements | Other Entitlements |

Cost Center	39130
	5 Digit Number
Cabinet	Finance and Administration Cabinet
Agency	Department of Revenue
Office	Office of Income Taxation
Division	Division of Individual Income Tax
Branch	Individual Income Tax Branch
Section	Governmental Programs Section 2
Unit	

Viewing an Organizational Level in EIM

If you click on one of the organizational levels, you will open a window that has some detail on that level. Remember EIM looks at the *lowest* level a user has to determine which accounts to manage and automate.

Governmental Programs Section 2

General | Entitlements

Org Type 1	Section
Org Type 2	
Org Type 3	
Org ID	10102808
Cost Center	39130
Org AD Abbreviation	DOR
Enable Automatic Provisioning	✓
Default Domain	FIN.DS.KY.GOV
Default OU	OU=PEOPLE,DC=FIN,DC=ds,DC=ky,DC=gov
Default Groups	
Email Billing Code Reference	

Governmental Programs Section 2

General | Entitlements

Active Directory Managed	✓
Exchange Managed	✓
Home Folder Managed	✓
KOG Managed	☐

Entitlements

This tab lists the Entitlements for this user. Entitlement is EIM's word for identity, or the core accounts it can manage. Please reference the screenshot on the page following this overview.

- Unchecking a box for one of these accounts (and submitting) will cause EIM to remove that account for the user, and set them for future deletion. If the box is rechecked before the account is deleted, EIM will reconnect them.
  - o While individual accounts can be removed or added as needed, removing the Network Account will also remove their Email and Home Folder since they are connected to it.
  - o It is advised to use this option sparingly. This is not the proper way to exit a user.
- Once a user has been given Email, they will be assigned their default Email billing number. This can be changed if a user needs to have their Email billed differently. More on Email billing in Section 4 'Miscellaneous Info'.
- Rated Messaging Service Code: Displays the COT rated messaging service code associated with either Office 365 cloud services licensing and support or basic On-premise Email service support. One of two possible checked marked Exchange Mailbox items below indicates the messaging services type identifier.
- Exchange On Premises Mailbox: When checked the user has a basic On-Premises (local) Exchange Mailbox **not** in the cloud.
- Exchange Online O365 Mailbox: When checked the user has an Exchange Online Mailbox in the Office 365 cloud.
- O365 License Assignment: The identifier associated with the Office 365 license dynamically assigned by the Office 365 cloud service per the organizational level.
- Home Folder: will display the user's storage folder path and drive letter defined per the organizational level.

Important Notes:

- If an organizational level is set to **not** automate account creation, this screen will show each managed account type but with empty check boxes. An authorized contact will need to check the boxes for the accounts desired and submit to have them created.
- If "Request Mainframe/KYNET/RACF ID" has been submitted from the Other Entitlements tab, this tab will show "Mainframe/KYNET/RACF" options after Home Directory (Folder). More on this in the Mainframe topic in Section 4 below.

Doe, Tony F (DOR)

| Employee Information | Work Information | Contact Information | Org Structure | Entitlements | Other Entitlements | Audit |

Network Account/Active Directory
Choosing this gives the user an enabled Active Directory account

☑ Checkbox is greyed out if Active Directory is not managed in User's Organization

Outlook Mailbox
Choosing this gives the user an Exchange account for email capabilities

☑ Checkbox is greyed out if Exchange is not managed in User's Organization

Email Billing Code
*

KRC INFRASTRUCTURE

Email Billing Code

XXXXXXXX

Rated Messaging Service Code
Provides Office 365 cloud services licensing and support or On-premise email service support.

MB10

Exchange On Premises Mailbox
When checked user has an On-Premises (local) Exchange Mailbox not in the cloud.

☐

Exchange Online O365 Mailbox
When checked user has an Exchange Online Mailbox in the Office 365 cloud.

☑

O365 License Assignment

G3 DOR ⌄

Home Folder
Choosing this gives the user a Home Folder

☑ Checkbox is greyed out if Home Folder is not managed in User's Organization

Home Folder Share

XXXXXXXXXXXXXXXXXXXXXXXXXXX

Home Drive

U: ⌄

Home Directory

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

Other Entitlements

This final tab will allow Authorized Users to request Mainframe services and accesses for a user:

Doe, Tony F (DOR)

| Employee Information | Work Information | Contact Information | Org Structure | Entitlements | Other Entitlements | Audit |

Request Mainframe/KYNET/RACF ID
Check this box if this employee
requires a Mainframe/KYNET/RACF ID. ☐

- Optionally, <u>should an employee need Mainframe</u>, please check the Request Mainframe/KYNET/RACF ID checkbox. Checking the box will expand the selections to drop-down, while unchecking will cause it to collapse again for the following inputs including required fields*.
  - Mainframe Billing Number*
  - Preferred User ID
  - Mainframe Alternate Contact
  - Mainframe Groups/Comments

Important: Mainframe has its own topic 'Requesting Mainframe (KYNET/RACF) ID' later in Section 4 of this guide.

Section 4: Miscellaneous Info

In this section, we will be reviewing the miscellaneous things that EIM will either affect or have influence on.

Email Billing

Since EIM will be managing the creation of email, it will also be working to make sure billing for this service is also started/ended appropriately.

- Each Cabinet will have default billing numbers aligned to their organizational structure. When a user is given a mailbox, EIM will assign them to a default number based on where they align in the Cabinet.
    - o For automatic email creations, EIM will only assign the billing number in the Portal when it confirms the mailbox has been created. This may take a few minutes.
    - o This number can be changed on users through the Portal.
    - o If default billing org alignments need to be modified, a request will need to be sent to the Commonwealth Service Desk with a description of the desired modifications.
- If an organizational level is not automatically creating accounts, the billing number will be required when the Agency Authorized Contacts or Agency HR Administrator requests the mailbox from the Entitlement tab manually.
- On a monthly basis, billing information will be retrieved to update the billing system.
- Any resource account or account that EIM does not manage will need to be requested outside of EIM.

Phone Number Assignment

Phone number assignments will still be done outside of EIM via a request to the Commonwealth Service Desk.

- If a user is assigned a VoIP (Voice-over-IP) number in Pinnacle, EIM will read that in and display it to the user's EIM profile as work number.
- If a user is assigned a number outside of Pinnacle, it will be updated directly into either EIM Portal or their Network (Active Directory) account.

- This number will display in the Global Address Listing if the user has email.
- If the phone number needs to be modified because it is wrong, it needs to be changed in the source. For example, if the wrong number was assigned in Pinnacle, a request needs to be sent to the Commonwealth Service Desk to have Pinnacle support correct it.
- An EIM Agency Authorized Contact or Agency HR Administrator can modify the Work Number directly from the Portal, if there is not a number available in Pinnacle for the user.

Stale Accounts Process

The stale account process monitors network accounts to detect the ones that are "stale" with no login over 45 days. Once EIM finds an account with no login over 45 days, it will send an initial notification E-mail to the user's manager and alternate contact in EIM.

Example Notification

Subject Service Request xxxxxxx Customer Notification regarding Stale account process

T**he 'automated stale process' is alerting of pending action to de-provision the account.** Accounts over 90 days in stale status are disabled, then after 120 days they are scheduled for automatic de-provisioning.

The IAM Portal allows the manager or alternate contact(s) to follow the link in the notification e-mail directly to the employee's Identity record to allow them to validate the account. **Alternately,** managers can go to the IAM Portal using the following link to see all of their direct reports=> https://iamportal.ky.gov/IdentityManagement/default.aspx

Once you are in the IAM Portal, please click the work information tab to view the 'Validate Account' selection, click the check box, then click OK button followed by clicking the submit button to process your request to extend the account for an employee who is off work and unable to login.

If the employee is on leave status in KHRIS, then the account would NOT have been selected for stale account processing. If an employee is off from work using their accumulated leave time, the safest thing to do is to set/check their 'Short Term Disable' to disable their AD account, which protects the account from being selected for stale, account processing. ****Important**** Once the employee returns to work, you must submit the 'Validate Account' request and before submitting a request to remove the 'Short Term Disable'.

Suggestion: All Users need to logon every month or before 45 days elapse of inactivity or their designated contacts (manager or alternate) in the notification e-mails need to validate the account to prevent it from entering stale account status. Accounts over 90 days in stale status are disabled, then after 120 days they are scheduled for de-provisioning.

This notification will let them know the account login will be blocked (disabled) after 45 more days if not logged into for a total of 90 days. If the manager/alternate contact determines they need to keep this account active, they can visit the profile for this user and check the "Validate Account" option on the Work Information tab. Once it has submitted, this will validate the account as active for 45 more days. If the account has not been logged into in the next 45 days, it will be once again be flagged as "stale" and a new notification will be sent alerting the account will be blocked from login (disabled) in 45 more days. The Active Directory account is

de-provisioned (deleted) after a total of 120 days of inactivity, along with all entitlements removed from the User's account.

Selecting the Validate Account option or the user logging in to a Network connected computer with their account credentials will reset the inactivity timer.

Notifications

EIM will send email notifications in certain scenarios. Below is a list of the notifications that will be going out, who it goes to, what triggered the notification, and its purpose.

- New Network Account
    - o Whenever a user has a new network account created, the manager and alternate contact will receive the account name and password in two emails.
    - o These are to be passed on to the user after they have started.
    - o Since accounts can be created up to 10 days prior to the user's start date, this can be received early.
- Stale Accounts
    - o Alerts the manager and alternate contact about a user account that will soon be deleted due to inactivity.
    - o The manager or an authorized contact will need to validate the user in the EIM Portal.
- Other Entitlements
    - o The requestor will be CC'd on the email when they request services and access through the Other Entitlement tab.
- Account Name Changed
    - o This notification will go to the manager and alternate contact alerting them a user's name has changed, and therefore modified the account name they log in with.
- Mainframe (KYNET/RACF) notification
    - o Mainframe ID and password will be sent in two separate emails to the user, their manager, and the RACF Alternate Contact (if specified).

Agencies EIM Doesn't Manage

Some Agencies will not use EIM to manage their accounts. These are primarily those who manage their own Network (Active Directory) accounts. If an Agency that manages its own Active Directory accounts needs services from COT (such as email), they will need to request that services from the Service Now catalog offerings.

If an Agency would like EIM (and therefore COT) to begin managing their accounts fully, they can opt into EIM management by contacting the COT Security Administration Branch.

EIM and HR Actions from KHRIS

When EIM reads user information from KHRIS, it mainly is looking for information. This could mean it sees a new appointment and creates the user in EIM, or it could see information change such as a name or a title.

However some specific HR Action "Z" codes will cause EIM to do specific things.

- ZA Suspension – Network Account will be disabled and excluded from the Stale Account process.
- ZB / ZC On Leave – Network Account will be excluded from the Stale Account process.
- ZD / ZE Return from Leave – Network Account will now be included in the Stale Account process.
- ZF Separation / ZG Retirement – User will begin them down the deprovision path.
  - Network Account will be disabled for 90 days, then deleted.
  - Mailbox disconnected 48 hours after the effective date of the HR action.
  - The Home Folder will be set for deletion in 90 days.
- ZJ Return from Suspension – Network Account will be enabled and included in the Stale Account process.

Non-KHRIS User Being Entered into KHRIS

When a non-KHRIS user becomes a state employee or contractor input into KHRIS, it is important to take care on how this transition is handled.

- If the non-KHRIS user is being hired in a different Cabinet, then the user will need to be exited through the Portal first. When they come through in KHRIS, EIM will create their new accounts accordingly.

- If the non-KHRIS user is transitioning (converting) from a non-KHRIS employee to a KHRIS employee (State Employee) within the same Cabinet. When EIM reads in the KHRIS action, EIM will provision new accounts. It is best practice to have a HR business process for employee on-boarding\Off-boarding in these situations. The employee should use the newly provisioned accounts. Then the user will need to be existed through the portal to remove their non-KHRIS accounts.
- If the user is staying within the same Agency, then the best practice is to not set the end date in EIM for that user until after the first pay cycle in KHRIS. This will confirm them in the system in case a void or data correction HR action is committed.

Retaining Mailbox or Home Folder Content

When a user leaves or transfers from a Cabinet, their mailbox will disconnect and home folder will be set to delete.

If the losing Agency needs to keep the content of the mailbox, the Email Review request service offering must be submitted through Service Now within 90 days from the date the employee leaves.

Requesting Mainframe (KYNET/RACF) ID

EIM has the ability to allow Authorized Users to request a Mainframe ID for a user (also known as a KYNET or RACF ID).

Requesting a Mainframe ID

Open the EIM profile for the user who you want to request a Mainframe ID for, and navigate to the Other Entitlements tab. Check the box next to "Request Mainframe/KYNET/RACF ID", and four options become available as shown in the following example.

Doe, Tony F (DOR) ✕

| Employee Information | Work Information | Contact Information | Org Structure | Entitlements | **Other Entitlements** | Audit | Set Me▸er❓ip |

Use the HEAT Self-Service Catalog for additional services.
Continue to use the mainframe section below for EIM managed mainframe agencies. You must be an authorized agency contact to use HEAT Self-Service Portal to request additional services.

HEAT Self-Service Catalog

Request Mainframe/KYNET/RACF ID
Check this box if this employee requires a Mainframe/KYNET/RACF ID.   ☑

Mainframe Billing Number
*
The Mainframe Billing Number is an 8-character code that will be associated with this account for mainframe billing. Billing is based on mainframe usage.

Must be 8 characters without spaces

Preferred User ID
The Preferred User ID is used to specify a prefix or full ID, from 2 to 7 characters, that should be assigned to the employee.

No leading or trailing spaces allowed (2 - 7 characters)

Mainframe Alternate Contact
The Mainframe Alternate Contact is the email address for someone other than the user or their manager that needs to be notified about the creation of the Mainframe ID and password.

Valid email address must contain the @ character.

Mainframe Groups/Comments
Enter Mainframe groups or special instructions if applicable.

* Requires input

- Mainframe Billing Number (required): The Mainframe Billing Number is the 8-character code that will be associated with this account for mainframe billing. The billing charges for Mainframe are based on Mainframe usage.
- Preferred User ID (optional): The Preferred User ID is used to specify a prefix or the full ID, from 2 to 7 characters, that should be assigned to the employee.
- Mainframe Alternate Contact (optional): The Mainframe Alternate Contact is the email address for someone other than the user or his or her manager that needs to be notified about the creation of the Mainframe ID and password.
- Mainframe Groups/Comments (optional): Enter Mainframe groups or special instructions if applicable.

From here, you will need to click the 'OK' button and 'Submit' the request. Once submitted, EIM sends an email to the Commonwealth Service Desk with the submitted information, and they will open a ticket to have the Mainframe ID established.

Once the ticket has been opened and the Mainframe ID is established, the EIM profile for this user will be updated. You can find this information on the **Entitlement tab** below Home Directory (Folder):

Doe, Tony F (DOR)

Mainframe/KYNET/RACF

If this box is checked and a Mainframe ID is present below, then the user has a Mainframe ID assigned. Unchecking this box will allow you to revoke the Mainframe account assigned to this employee.

☑

Mainframe ID

The Mainframe ID is the User ID assigned to the employee, to be used to log in with, and will only show here once it has been created.

ABC1234

No leading or trailing spaces allowed.

Display Mainframe Initial Password

Select this as an Administrator to show the Mainframe Initial Password field.

☐

Mainframe Billing Number

The Mainframe Billing Number is an 8-character code that will be associated with this account for mainframe billing. Billing is based on mainframe usage.

12345678

Must be 8 characters without spaces

Mainframe Alternate Contact

The Mainframe Alternate Contact is the email address for someone other than the user or their manager that needs to be notified about the creation of the Mainframe ID and password. This should be a valid email address.

John.Doe@ky.gov

Valid email address must contain the @ character.

At this time, EIM will send the Mainframe ID and password in two separate emails to the user, their manager, and the optional RACF Alternate Contact (if specified).

IMPORTANT Reminders to share with Mainframe Users:

This process only requests the initial ID and password for Mainframe to establish a credential without access to login. An authorized contact with your Agency will now need to request any Mainframe application access necessary for the user login following the standard application request procedure.

The user must refrain from login to mainframe until notified by COT they have been granted application login access permission. Otherwise, a user's login ID will automatically revoke (disable) after three failed attempts and require contacting the Commonwealth Service Desk once they have access for reset.