Guide to Identity Warehouse in AccessVUMC 2.0

Recommended Reading:

- VUMC ID Status-Based Troubleshooting Reference
- Guide to the Profile View in AccessVUMC 2.0

See the end of this document for additional references.

Table of Contents

Page no.

1. INTRODUCTION ……………………………………………………………… 1

2. SECTION 1: IDENTITY VIEW…………………………………………………. 3

   - Attributes tab 3
   - Entitlements and Application Accounts tab 7
   - Status Column, Policy, History, Risk, and Activity tabs 12
   - User Rights, Events tab 13

3. SECTION 2: DATA REPRESENTATION AND INTERPRETATION ……………. 14

   - Attributes tab 14
   - Entitlements and Application Accounts tab 17
   - Events tab 20

4. SECTION 3: CUBES ………………………………………………………. 21

   - Cubes Structure 21

5. SECTION 4: SUPPORT DIRECTIVES …………………………………………… 23

   - Support Directive by Type 23
   - Support Directives by Field 23
   - Support Directives by Team 27

6. ADDITIONAL REFERENCES ……………………………………………….. 29

7. **INDEX** 30

Definitions

- “Identity Cube” --7, 26
- “LDAP” ---20
- “PII” --- 13
- “Resource Account” ---16
- “Test Account” ---16
- “SIP” ---4

INTRODUCTION

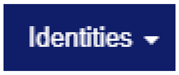
AccessVUMC 2.0 is accessed at the following link: https://vumcidentity.app.vumc.org/identityiq/

This document attempts to familiarize the reader with an understanding of the Identity Warehouse within AccessVUMC 2.0 (**AVU 2**) at Vanderbilt University Medical Center. You will need to be a VUMC Services Administrator to access the section of the application described in this documentation.

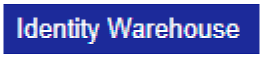
SailPoint Technologies™ is a tech company that provides Identity and Access Management. This documentation is describing the use of the "Identity Warehouse", which is a part of the VUMC tool named AccessVUMC 2.0 which uses the **SailPoint IdentityIQ** application architecture.

If you need access to this tool as part of the duties of your role, please see How do I become a VUMC Services Administrator (VSA).

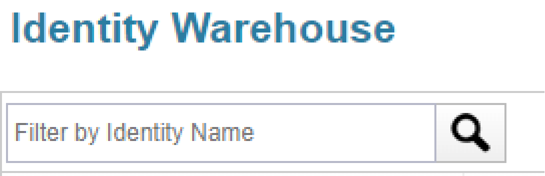
The Identities table accessed through Identity Warehouse contains basic user information for every identity discovered during the latest aggregation process. Identities can include non-human identities, such as service accounts and bot identities, as well as users.



At the top of the screen in **AVU 2**, if the menu item "**Identities**" is visible, as shown above, then you have the access to make use of this documentation.

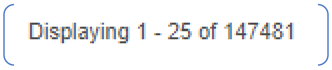


Select Identities and then from the pop-out menu that appears, select Identity Warehouse. This brings up the Search filter as shown here.



You may enter the VUMCID, the 7-digit Employee ID with leading zeros, or the [last name] + [comma] + [space] + [first name], or partial name. You may also simply include just the first or last name if the name is rare to unique. If you leave it blank, the first page of all accounts of all types will display. Depending on specifics entered, the results could include multiple cubes. With numerous results that may include multiple pages you can even click on any column header to sort that column.

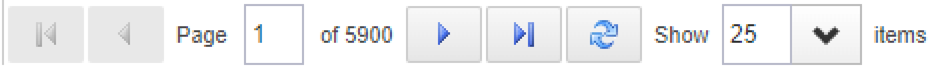
Leaving the field blank and waiting several seconds, the system will display all Identities in the Identity System, giving you a count of those accounts in the lower right of the screen. It changes often, but today the current count looks like this:



Displaying 1 - 25 of 147481

This is referencing 1-25 items on this page (Page 1), of a total number of 147,481 accounts of all types.

If you choose, you may also expand the number of results per page using the selectors on the lower left, as shown here:

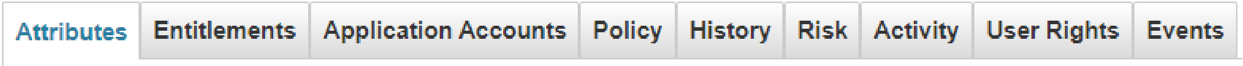


Choosing the down-chevron to the right of "Show [25]", you can select up to "100" per page. For the record, if selecting one hundred per page, the page-count will adjust accordingly. You may also select a specific page number, if you find the opportunity or need to do so.

However, this section is best used for a single account. If you are interested in working with large data-sets, or pulling a report, please see AccessVUMC 2.0 Reporting and Advanced Analytics.

SECTION 1: IDENTITY VIEW

Clicking on the relevant result will display the View Identity screen. This page will include tabs across the top, the Attributes tab is selected by default, as shown here:



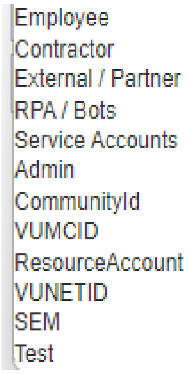
Attributes | Entitlements | Application Accounts | Policy | History | Risk | Activity | User Rights | Events

We will cover all the tabs seen here with the detail necessary to provide the most relevant information.

- ### Attributes tab

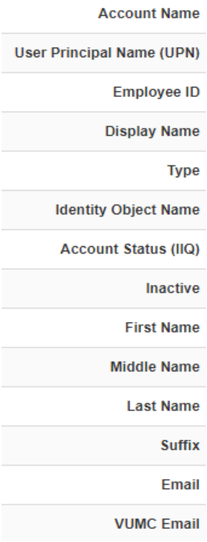
The Attributes tab shows similar information to what is found in the Profile View in some sense, but it is essentially a representation of the Identity itself. Multiple **types** of identities exist in the Identity system (not everything is a VUMCID, and not every VUMCID belongs to a human). A more complete treatment of this section will follow further down in this documentation.

You will see **VUMCID** accounts, but also **CommunityID**, **ResourceAccount**, **Admin**, **SEM**, and **Test**. The full list of account types includes account types that do not exist yet in our Identity System; but may at some point in the future. See graphic to the left for a list of all account-types.



Employee
Contractor
External / Partner
RPA / Bots
Service Accounts
Admin
CommunityId
VUMCID
ResourceAccount
VUNETID
SEM
Test

Each type of account will include to varying degrees different information on each tab. The fields displayed, whether populated or blank, will remain consistent throughout. The Attributes tab includes, for example, a set of data-fields that do not change. These fields may include data, or they may be blank depending on the type of account and what that account ought to show when active or disabled.



Account Name
User Principal Name (UPN)
Employee ID
Display Name
Type
Identity Object Name
Account Status (IIQ)
Inactive
First Name
Middle Name
Last Name
Suffix
Email
VUMC Email

An "**Account Name**" on the Attributes tab and throughout SailPoint *is* the VUMCID. The **Identity Object Name**, (ION), is not the VUMCID *but may have been in the past*. You will see the ION may match the Account Name, or it may be a different spelling (an old VUMCID), or it may only be a number, which is the Employee ID. Column headers in some places in AVU 2.0 may label the Identity Object Name with the simple term "***Name***".

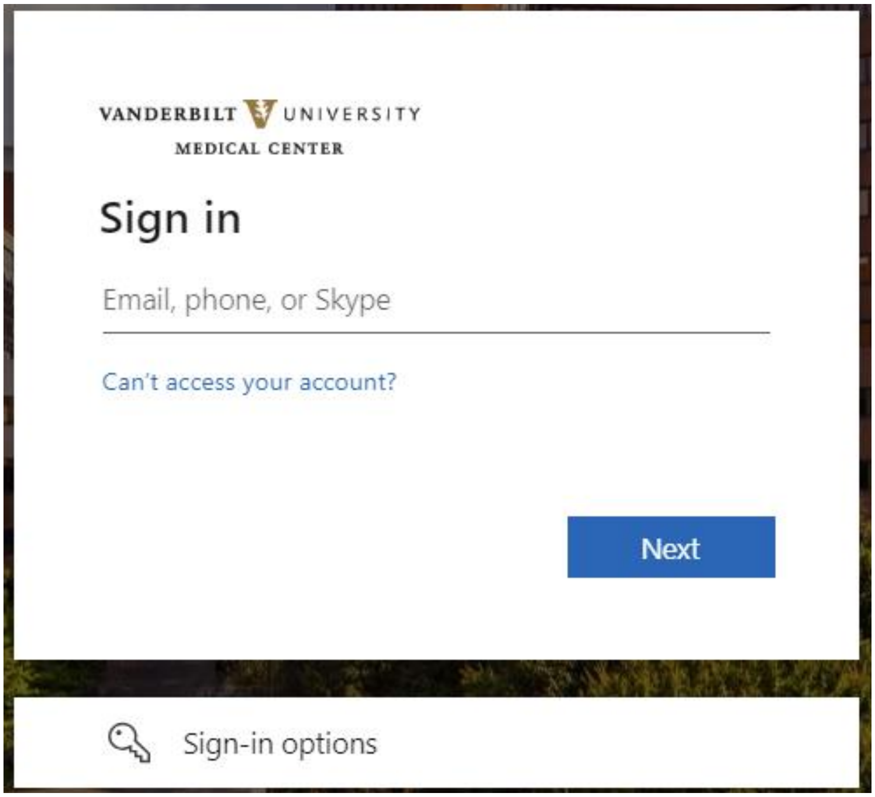
The "**User Principal Name**" (UPN) is a username and VUMC domain in an email address format. It is provided to an account for use when logging into accounts and applications that use the Microsoft Login. Every account, regardless of type will include a UPN and it must be a consistently formatted email address, also known as a Primary Email Address, and though these fields are separate fields in the data, our system is designed to have these formalized as identical, along with the **SIP address**. If these three fields do not match each other this is an error condition and can be addressed by sending a Pegasus incident to **VUMC IT PARTNER SUPPORT**.

DEFINITION**: "SIP"**

SIP *stands for "Session Initiation Protocol" and is an Internet Protocol (IP) used to facilitate live communication sessions such as those utilized within Skype or Teams.*

The UPN for VUMC will always include a VUMC domain. No other domains will work. If someone attempts to login to a VUMC resource using a Gmail email address, for example, it will fail. The username will not be found.

To summarize, the User Principal Name (**UPN**) is used as the "username" when logging into a resource. See graphic at right.



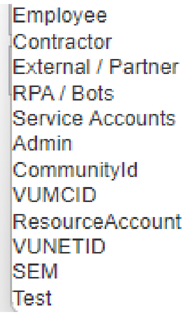
Some resources require the VUMCID instead. The **Primary email address** is used for email communications. The **SIP address** is used in Teams, primarily for communications within Teams. At VUMC these should all match each other.

Accounts that do not have a presence in Teams will lack a SIP address.

An **"Employee ID"** is an identifier WorkDay uses. It is a 7-digit number presently with a leading zero. It is essential for user accounts because they are instantiated first in the WorkDay system. There is no VUMCID for someone new, at this stage. For accounts in AVU that are missing an employee ID, there is nothing in WorkDay. Resource and Test accounts, as well as Admin, SEM and other types of accounts have no presence in WorkDay and thus the Employee ID field will be blank. The term Employee ID is a misnomer because it is also used in WorkDay to identify *non-employee*s.

The “**Display Name**” is the name visible in Pegasus, and the Global Address List (GAL). The display name is defined as the “Preferred Name” in the WorkDay environment and *is configured from within WorkDay*. See KM0014847 for more about the Preferred Name and how that is edited by the end-user.

“Type”: Multiple **types** of identities exist in the Identity system (not everything is a VUMCID, and not every VUMCID belongs to a human). To the right is a list of possible types.



Employee
Contractor
External / Partner
RPA / Bots
Service Accounts
Admin
CommunityId
VUMCID
ResourceAccount
VUNETID
SEM
Test

The **“Identity Object Name”**:

- Will match the VUMCID if the VUMCID has been in use without a break since before the new AVU 2 application began (before January 2024).

- It will reflect the old VUMCID if the original VUMCID was created before AVU 2 but became disabled and remained so for more than 30-days. (See KM0016050 for a discussion of this under EPassDeleted header). Or,

- The field will have a 7-digit Employee ID if the VUMCID was created *after* AVU 2 was released; and the new VUMCID has not yet been disabled for more than 30-days.

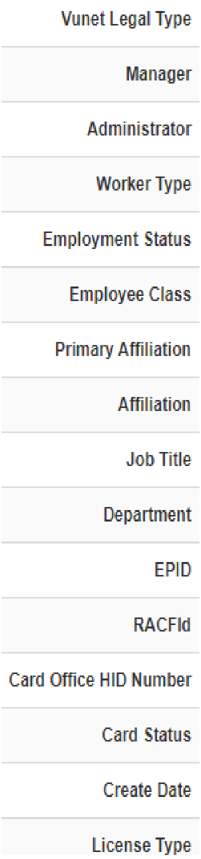
The “**Account Status (IIQ)**” is the status of the account itself in the Identity system. Although it follows the Employee Status for user accounts in general, this field is managed independently within the Identity system for accounts that are not user accounts. See VUMC ID Status-Based Troubleshooting Reference for more information about this field and how to interpret its values.

Each of the **name** fields, including the **suffix**, is self-explanatory. Resource Accounts will always have “Resourceid” as its last name. Test accounts will always have “Testid” as its last name; and other diverse types of accounts have conventions regarding the last name field. For users, the last-name field *must be the legal name*; and this field is determined by the entry for the employee record in WorkDay.

Upon initial provisioning of a UPN (and the Email account itself), the name: first, middle, and last, is used to build-out a *unique* email spelling not currently or historically used here at VUMC, nor at VU. For this reason, it is common for email addresses to include a numeral (*.1, .2, etc.)* appended to the local part of the address so problems are prevented.

“Email” and **“VUMC Email”** fields: The email field *is* the notification email address used by the Identity system when an account notification needs to be sent to the accountholder. It will be an external email address when the Microsoft License is at an F1 level. Microsoft 365 F1 is the default level of license for non-employees. At this level, the individual cannot use their Primary email address for email purposes. The external email address originates from WorkDay and was entered originally by a hiring manager or agent of HR who populated the Home Address for the pre-hire. The account holder can also edit it. For staff who receive the MS 365 E3 level license by default, or those who have received an upgrade to F3 or E3 from the Software Store, the notification email address will be updated to match the Primary Email Address, though the Home Address in WorkDay will not affect the notification address at this level.

The “**VUMC Email**” field is the Primary email address. It should match the UPN and SIP addresses where the SIP address is applicable.



Vunet Legal Type
Manager
Administrator
Worker Type
Employment Status
Employee Class
Primary Affiliation
Affiliation
Job Title
Department
EPID
RACFId
Card Office HID Number
Card Status
Create Date
License Type

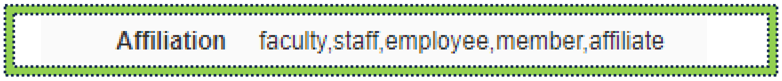
“**VUNet Legal Type**” was brought over from the previous version of AVU, or from the original “AccessVU” system. This field was added shortly after the initial Organizational split which occurred in April 2016. At that time, the identity system included both VU and VUMC accounts. This dual-presence in the Identity system persisted until the Identity system split, which occurred in mid-2019. In that sense, this field is a carry-over.

“**Manager**” is the manager of the account-holder. For users, this is that person’s organizational manager. A manager will not be listed for Resource, Test, Associated Admin (TLA), or Community accounts.

The “**Administrator**” is an account-owner for a non-user account (Resource or Test), or for an Associated Admin account. User accounts of any type do not have an administrator assigned.

The “**Worker Type**” field will be “Non-Employee” for Contingent Workers, or “Employee” for regular staff. More detail is provided in the following fields below this one, including “**Employee Class**”, “**Primary Affiliation**”, and “**Affiliation**” (this field contains what is called the “affiliation string”). These fields share commonalities.

Example: ***Affiliation String***



Affiliation faculty,staff,employee,member,affiliate

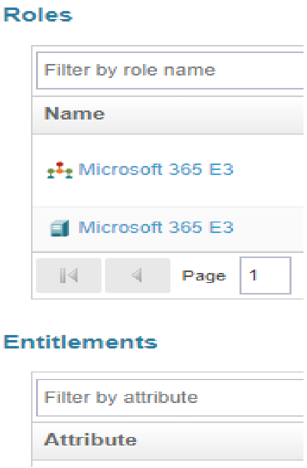
The “**Employment Status**” field will show either **ACTIVE**, or **INACTIVE**. If it is inactive, then the classifications beginning at Worker Type and its related fields will be blank. It is important to note the system may not clear these fields until after 30-days from the date the employment terminated.

Active accounts will also include the “**Job Title**” and “**Department**” information. The “**EPID**” is a pointer to the *actual record* where this Identity record exists in the AccessVUMC system. Specific details below this detail are mostly administrative in nature and self-explanatory.

You may see **RACFId** information; and **Card Office**, which is discussed further down.

- ## Entitlements tab

Roles



Active Accounts for users will have listed on the Entitlements tab, under ***Roles***, the Microsoft License applied to the account. Employees are provided by default the Microsoft 365 E3 license, and non-employees are, by default, provided the F1 license. Other information for some VUMCIDs will include privileges designed to give access to some of the tools available within the AccessVUMC application environment. For example, a VUMC Services Administrator (VSA) will have other roles listed here.

Entitlements

Group memberships in Active Directory, both VUMC (ds.vumc.io) and Common (ds. vanderbilt.edu) will be listed under ***Entitlements***.

- ## Application Accounts tab

This tab is critically important with respect to understanding more about the status of an Identity and its component parts. On this tab, you will see various “applications”. Each application can be called a “card”, which is a term of convenience to describe the component parts of a full Identity. The cards in this section represents an ***Identity Cube*** in AVU 2.

DEFINITION: "**IDENTITY CUBE**"

An "Identity Cube", or simply "cube" in AVU 2 is a full set of records for any one entity or individual. It is defined by SailPoint as “a multi-dimensional view of each identity and their associated access and attributes”.

This section covering **Application Accounts** will address each *card* in a *cube* and help you to interpret details within a card. In the columns displayed, it will include an "Account Name" column (which is not necessarily the VUMCID but rather the account-name associated with the card itself).

Account Name

Also included is a "Status" column (Active or Disabled) and a "Last Refresh" column, which is the date the AVU system registered an update. Both are discussed further down.

Each card in a cube can be affected by other cards in that cube. What this means in practice, is a VUMCID will function to provide access to WorkDay if there is a Workday card in that cube. If there is no WorkDay card the VUMCID cannot access WorkDay.

- **VUMC-Application-AccessVUMC**
    - **NOTICE:** If this is present in the cube, it represents the *legacy* VUMCID card. This is not used with *new* accounts, so if it is missing this is considered normal. You will always find the detail for a VUMCID instead under the Attributes tab, described above. Because of this, this card can be considered archival information and not necessarily current, or relevant.
        - This data is, and was, created within AVU itself. In the case of this part of a cube if it is present at all: it was created before AVU 2.0.
- **VUMC-Application-CCO**
    - The CCO card is the record-holder of the Card Office Access Card; the ID badge. The status will show disabled for cards which are disabled, but also for cards *enabled* but not used for higher-access actions. In other words, an Identity card *only*, and not used for access to buildings, doors, or magnetic stripe use. Therefore, the "Disabled" status associated with a CCO card is a non-issue and more nuanced than what appears. If more information is required, you may inquire of the Card Office directly.
        - This data is created in AVU when triggered soon after a WorkDay card is received, and then transmitted to Card Services, which in turn will update the information after instantiation in that system, as a writeback is received by AVU to synchronize. This type of update occurs very quickly (3-15 minutes).
- **VUMC-Application-CommonAD**

    - This card is a record of what exists in the *Common* Active Directory system. The word “common” in this context means shared between VU and VUMC, and specifically on the ds.vanderbilt.edu domain. Separation of the Active Directory system for the original single organization began about June 2017. This transition is still underway, which began in April 2016. This is why both CommonAD and VUMCAD (ds.vumc.io) exist as a separate card.

        - Common AD on ds.vanderbilt.edu domain is first created, as is VUMCAD, once a WorkDay feed and CCO is instantiated in the AVU system. Other types of accounts which are not hosted in WorkDay (Resource, Test, Admin, *et cetera*) will generate a new Active Directory account once a VUMCID is created. Certain account types never trigger the creation of this card (Example: CommunityID).

- **VUMC-Application-EIR**

    - This card will hold a record from the previous Enterprise Identity system (AccessVUMC 1.0) for a particular cube. This card will not be present on every record you encounter; but only those with a record which would have existed in the previous system. This card can be skimmed past, as it is not particularly relevant other than being data-storage for old, and sometimes outdated information.

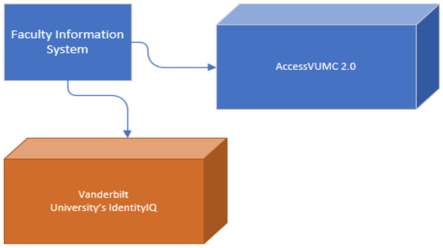
- **VUMC-Application-FIS**

    - **FIS** stands for **Faculty Information System**. It provides information about a faculty member’s status in *that* system. It is a separate, external system to any other VUMC system. It co-exists in Vanderbilt University’s EPI (Enterprise Person Index) system.

    - The start and end-dates, if present, do not pertain to employment but to an appointment from the Provost at Vanderbilt University under the auspices of the Office of Faculty Affairs. Being faculty is not relevant to whether an individual is a full-time-employee or a contingent worker. These are separate considerations.

    - If a start-date exists with no end-date, and shows active, this individual is tenured.

    - The data here comes from the Faculty Information System. Updates are not possible from AVU directly – the data moves only one-way, from FIS to AVU, and from FIS to VUIIQ.


Faculty Information System
AccessVUMC 2.0
Vanderbilt University's IdentityIQ

- There are three status flags within the FIS card: Teaching Status, FIS Status, and Faculty Status. To understand the FIS information, the only status that is considered relevant would be the FIS status itself. The other statuses can indicate one or more appointments and whether the individual carries on teaching at the university. You can be certain that any faculty will have a VUnetID (University Identity Account); whether active or inactive.

- **VUMC-Application-RACFID**
  - RACFId stands for *Resource Access Control Facility ID* and is being phased out. At present, older systems still use this for authentication. It includes PII details. Inquiries regarding a RACFID can be directed to VEC Access Systems team.

- **VUMC-Application-IIQ-Loopback**
  - This card will not be present in most cubes. A card that represents this individual has administrative roles related to certain upper-Tier privilege-settings to facilitate troubleshooting and administration within the AVU system and other systems tied to it.

- **VUMC-Application-IIQ-P1**
  - This is imported information from the previous AccessVUMC version and will not be present on newer accounts created after the upgrade. It contains information but, like the EIR card, it includes nothing which cannot be also found in other cards.

- **VUMC-Application-SPOK**
  - AMCOM and USA Mobility merged into SPOK (see https://spok.com). If the account has a phone number assigned to them, this is where that information is found.
  - This is updated by any user by editing the **Work Contact Information** in WorkDay.
    - Within WorkDay > Left Menu > Personal Information > **Contact Information**.
    - Click **Edit** at top > **Change My Work Contact Information.**
    - From this data, you may expect to see Active Directory updated with this information as well. From Active Directory, it will populate the Global Address List in the Microsoft Exchange profile information where it will show up in all Microsoft applications upon that individual logging in. This includes Outlook, Teams, Excel, Word, and so on.

- **VUMC-Application-VMCHR**
    - VMCHR refers to the legacy PeopleSoft system. Not every cube will have this card. It will not reflect current state of employment and may be set aside when troubleshooting. These "carry-over" cards will be less common as time moves forward. These provide a glimpse into the past, as it includes a certain history attached to an individual's presence in the Identity system.

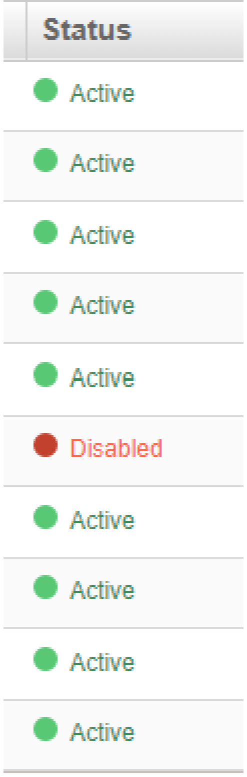
- **VUMC-Application-VUMCAD**
    - This is the VUMC Active Directory system. Only VUMC persons will be in this Active Directory system. If you notice that the VUMCID is active, but either AD card is *inactive*, check the password expiry, because typically this condition arises from the password having expired.

- **VUMC-Application-WorkDay**
    - The WorkDay card is the information in AVU which was obtained from WorkDay. This is valid for both employees and non-employees alike. It includes department information and position, status of the employee record in WorkDay, and other details, including hire date (or start date) and contract end-date for those who are on a contract term of known length.

- **VUMC-Application-cLDAP** and **VUMC-Application-MarketoWS**
    - The information from these cards, if you encounter them, pertain to **CommunityID** only. A Community ID while fully integrated with the VUMC Identity system, represents an individual service provider (Nurse or Doctor) unaffiliated with VUMC, but have nevertheless a connection with VUMC through the **HealthConnect** system to use the **EStar** system in a limited way to facilitate patient care and referrals. The Community ID system is supported by our VEC Directory Services and Access Systems teams.
    - There are going to be represented here on occasion a person who *also* has a VUMCID. This individual would have obtained a CommunityID first, but later became affiliated directly with VUMC and thus needed a VUMCID. The old CommunityID would thus fall into disuse; though it is not deleted.
    - **We will cover interpreting the data each card contains more fully in SECTION TWO.**

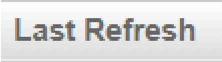
The Status Column: Active or Disabled

  - The status terms are non-intuitive. Oddly, the meaning of active and the meaning, especially, of disabled, in the context of *this column* does not mean, *necessarily*, that the VUMCID, or any functionality of a particular card is impacted.
  - A disabled CCO card may only mean that the card was printed on a plain plastic card without any technology, mag or contactless. In this case, the access is not disabled at all. Non-tech badges are left inactive in the badge system, so they don't take up a license.
  - Similarly, if a WorkDay card shows disabled, it may only mean that the account is in a working state *other* than active (but still not actually disabled). For example, a WorkDay card that is now functioning; has even triggered the provisioning of a new VUMCID for someone who starts in the future, the status within the WorkDay card will show "FUTURE" state. *This is not an active state*, and thus the status column shows "disabled". This is how it is outwardly seen and requires opening the hood to check directly before the actual status of the WorkDay record can be ascertained.



Status
● Active
● Active
● Active
● Active
● Active
● Disabled
● Active
● Active
● Active
● Active

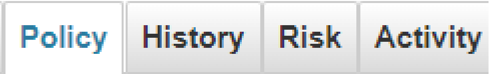
- **Last Refresh**



Last Refresh

  - The Last Refresh column is self-explanatory. If can be seen as an indicator whether a password-reset has fully propagated because updates to key cards occur as soon as a password reset is complete. If the relevant cards refresh is lagging behind then a password reset has not fully propagated. Some cards do not update when the password is updated, and this is normal.

- **Policy, History, Risk, and Activity tabs**

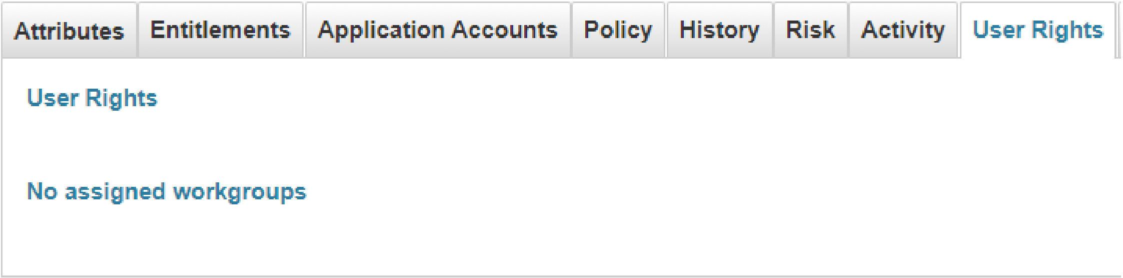


Policy | History | Risk | Activity

These four tabs are not often utilized at present. The Policy tab will only provide information that there have been no policy violations. The History tab similarly will contain no great insights into an Identity. Risk is not being measured. Activity monitoring is disabled. It is possible these will come into use later; however, these are built-in to the third-party SailPoint system. Parts of SailPoint exist but are not utilized because VUMC uses other systems to measure those things. It would be redundant to make use of these measuring systems in SailPoint also.

- ## User Rights tab

This tab is useful but limited to those who are in a support role in AVU 2 itself. In most cases, User Rights and Assigned Workgroups will be left unpopulated as shown below.



User Rights

No assigned workgroups

- ## Events tab

Unlike the previous few tabs, this tab of events will hold a cornucopia of information useful to determine what has been happening with this account and when it happened. It does not contain everything, however. It still provides a useful tapestry in the Past Identity Events, and occasionally, and especially for support personnel, relevant information in the Access Requests section below the event's log.

Typically, you will find modifications made from WorkDay which have subsequently updated other cards in the cube. Things such as birthdate or social security number changes, name changes, phone number changes, and other types of updates.

Definition "**PII**" : Personal Identifying Information, consists of legal name, U.S. Social Security number and date of birth.

SECTION 2: DATA REPRESENTATION AND INTERPRETATION

This section will attempt to cover the most relevant data provided in the cards. Because of this, cards are not included if only minimal information with little import is provided.

Data Flow Considerations:

An important consideration is the direction data flows. Information that is updated and what direction those updates flow is addressed inline. The following will expand on what was discussed in the last section and will go into more detail.

- ### Attributes tab
  - **This is the VUMCID data**. No other tab represents the *actual* data attached to a VUMCID. It will mirror somewhat what you find in the Profile View section of AVU.
    - **Employee ID**: this is the WorkDay card that is "managing" this VUMCID. This should match the WorkDay card in the same cube, and if it does not that is a problem that needs solving. One symptom is the inability to login to WorkDay.
    - **Display Name** is the Preferred Name in the WorkDay card. This is what shows up in the GAL (Office products), in Pegasus, and other places. It is only configurable from WorkDay. See Change Preferred Name (Display Name)
    - **Type**: there are twelve types of accounts (*See pg. 5*). Most accounts are of type VUMCID.
    - **Account Status (IIQ)** is the status of the VUMCID itself, and here it is limited to a specific set of values. Beginning with the Account Status is usually the best way to undertake *any* troubleshooting effort. An excellent resource is prepared for this: VUMC ID Status-Based Troubleshooting Reference
      - The Profile View in AVU 2 is also a useful reference.
    - Although PII details with respect to the SSN and DOB are only viewable from the Profile View, the legal name (**First Name**, **Middle Name**, and **Last Name**) is provided. This part of the card is visible in other places, and here you are only getting this information as "hearsay" data; meaning, the WorkDay card is the authority for the name. If a discrepancy exists, but the card is

historical in nature, it may not be a problem. Old names are retained in older data.

- **Email** and **VUMC Email.** *These are not the same*, nor will they always match each other. Email (alone) is the notification email address and is only used by the system to send notifications for password resets and other account activity. This address is what Pegasus will use for its notifications for this person. It might match the VUMC Email, and it will if that individual's account has a Microsoft License that permits use of the mailbox for communications. See *License Type*, below. Otherwise, it will be an external email address, and will match what is called the **EMAIL_ADDRESS_HOME** in the WorkDay card.

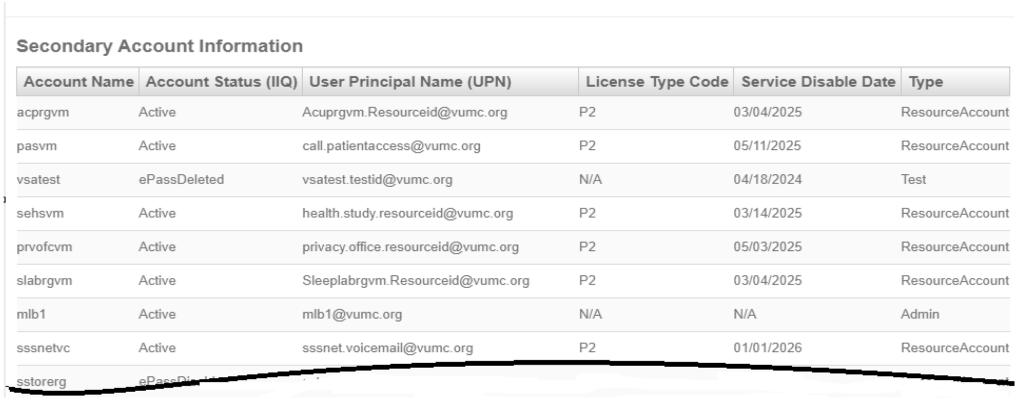
    - For Resource and Test accounts, the system will also send notifications to the notification email address to alert a team, or owner, about the impending disable-date for the account.

    - The VUMC Email is called the Primary email address and will be an email address on the VUMC domain. It will match the UPN and SIP address.

- **Manager** is self-explanatory; and it is this person to whom you would direct the account-holder for questions about their status and other issues which may arise with the WorkDay feed.

- **Administrator** is a field used to hold the owner's information for a TLA (Associated Admin Account), a Test account, or a Resource Account.

NOTE: It is possible to see all accounts for any given administrator by searching that individual at View Profile. The accounts administered by that individual will be listed at the bottom of the View Profile page under the heading Secondary Account Information, as shown here.



Secondary Account Information

Account Name	Account Status (IIQ)	User Principal Name (UPN)	License Type Code	Service Disable Date	Type
acprgvm	Active	Acuprgvm.Resourceid@vumc.org	P2	03/04/2025	ResourceAccount
pasvm	Active	call.patientaccess@vumc.org	P2	05/11/2025	ResourceAccount
vsatest	ePassDeleted	vsatest.testid@vumc.org	N/A	04/18/2024	Test
sehsvm	Active	health.study.resourceid@vumc.org	P2	03/14/2025	ResourceAccount
prvofcvm	Active	privacy.office.resourceid@vumc.org	P2	05/03/2025	ResourceAccount
slabrgvm	Active	Sleeplabrgvm.Resourceid@vumc.org	P2	03/04/2025	ResourceAccount
mlb1	Active	mlb1@vumc.org	N/A	N/A	Admin
sssnetvc	Active	sssnet.voicemail@vumc.org	P2	01/01/2026	ResourceAccount
sstorerg	ePassDi				

  - User accounts will not have an Administrator; therefore, this field will be blank for user accounts.

- **Worker Type** for user accounts will be **Employee** or **Non-employee.**
  - For non-*user* accounts this will be blank.
    - *"non-user" means an account that is not an identity for a human being, for example: test, resource, and shared mailboxes.*

Definition: **"RESOURCE" and "TEST" accounts**

A Resource Account is an account used for automatic logins for such things as printers, equipment, conference rooms, or administrative purposes which do not require a human presence.

A Test Account is an account intended to be used to mimic any type of account.

Both types of account are administered by an "owner", known in AVU as the "Administrator".

See Resource and Test Account: Ownership Model for more information.

- **Employment Status** is self-explanatory. It is unrelated to the Account IIQ Status but can be an important puzzle-piece to help understand why the Account Status is what it is.
- **Primary Affiliation** has more granularity than Worker Type.
- **Affiliation** is the full affiliation-string, which includes not just the Primary, but all other affiliations.
- **Job Title** and **Department** are filled in for active user accounts.
- **EPID** is the Enterprise Person Index record number – which is a pointer to where this record exists in the overall data. If you have this specific number you can look it up this way through Advanced Analytics.
- **RACFId** if one exists in this cube, and is attached to this VUMCID, it will also show here. This ties the RACFId to the VUMCID.
- **Create Date** is the date and time the record was created in the system.

        - **License Type** is specific to Microsoft. If F1, no access to the mailbox is permitted, but the individual still logs into VUMC resources that require an email address with the UPN and VUMCID password. You can find more information about Microsoft Licensing here: https://www.vumc.org/it/microsoft-licensing-nonemployee

        - **Last Password Change Date** is next, also on the View Profile screen. Included where applicable, the extension and date of password expiration extension will be visible.

- ## Entitlements tab

    - **Roles** Include the Microsoft License specifics and will show if additional roles are provided for VSA Administrators who have them.

        - A VUMC Services Administrator (VSA) is a critical position at VUMC that helps ensure workforce members in their area maintain secure access to resources using a VUMCID, UPN, and password. (See KM0015505)

    - **Entitlements** Memberships in various groups will be listed here, and listed under the respective Active Directory cards within the Application Accounts tab.

- ## Application Accounts tab

    - Each card within this tab includes information like what you see under the Attributes Tab for the VUMCID. In a real sense the VUMCID itself is also a card although its information is laid out under the Attributes tab. See Section One for a good introduction to the Attributes tab.

    - Here is covered only four cards, the others not being as critical: the **CCO card** for the Card Office Access card, the **Active Directory cards**; both of those together here, and the **WorkDay** card, which is relevant only to user accounts. These three types are the only “required” cards for a usable VUMCID Type “user” account.

        - **CCO Card** includes the name which matches the legal name and will be what shows on the physical card, and includes the EPID, which is also known as the PIK# on a Card Office Card. If enabled (ACTIVE = A) there will be a magstripe code included.

        - **CommonAD**, and **VUMCAD** Card

    - CommonAD is the Active Directory on ds.vanderbilt.edu (also referred to sometimes as “on-prem AD”). It includes fields present in Active Directory. The scope of this document is not such that all fields will be described. The same is true for the VUMCAD card, which represents the fields present in Active Directory on ds.vumc.io. Corresponding details here match what is found on the VUMCID and other cards.

- **WorkDay** Card

    - All users have a WorkDay card.

        - One of the things which has not been touched on often is the SSN and DOB hash details. SSN and DOB is encrypted. Please note that the hash will match each other across cards when a cube is consistent. Inconsistent cards can exist, however. When and if this happens, the cube is considered inconsistent. It is even possible to search for inconsistent cards using Advanced Analytics. Inconsistencies often do not impact the end-user nor functionality, but when it does cause problems it should be investigated further.

        - The labels for the fields in the WorkDay card match what data-structure looks like in WorkDay proper. You will see, for example, “CONTRACT_BEGIN_DATE”; and this is a typical naming convention used “under the hood”. In this documentation, this type of labeling of data will be minimally incorporated, and for example, in most cases where the contract begin date is referenced it will be presented simply as contract begin date.

        - Contract begin date is relevant only where contractors are concerned; non-employees are usually affiliated with VUMC for a specific duration. Full Time Employees in Workday will use a different term, “hiredate”, instead.

        - You will find the Company Code and Name is universal: VUMC, Vanderbilt University Medical Center.

        - You may see a contract end date. Employees do not have this since their term is non-specific. When it comes time to terminate, or for someone to retire or quit, then a date will show up at “termination date” once that has been entered in WorkDay.

- **What is missing**?
    - **The following are not covered in detail here in Section 2, because when troubleshooting access issues these seldom play a role**. See Section 1, pages 8 through 11, for overviews.
        - FIS
        - EIR
        - RACFId
        - IIQ-Loopback
        - IIQ-P1
        - SPOK
        - VMCHR
- How long data lives in the various tabs may become relevant.
    - For example: the WorkDay record keeps information in AVU for 30 days after termination. When an account has been disabled for more than 30-days, some information will be cleared away. For example, the email addresses are cleared away; because the mailbox is deleted.
    - The information is not lost entirely. The old information is locatable in various places such as event logs and other cards within the cube.
    - Employee Class and Employee Type disappear from the applications tab as no longer applicable after 30 days.

- Other account Types such as **Resource and Test** accounts:
    - The cards for a Test or Resource account cube will not include a WorkDay card. These will include Active Directory cards because if an account uses a password there must be an Active Directory account.
    - You will also see a CCO card account. A CCO card for non-user accounts is essential as a placeholder card. There will be no physical access card created nor needed in most circumstances;

though test accounts may sometimes need a card for testing purposes, depending on what the test parameters may include.

    - CommunityID accounts do not need a presence in Active Directory. There will be a cLDAP card which serves the same technical considerations.

- DEFINITION**: “LDAP”**

Lightweight directory access protocol (LDAP) is a protocol that makes it possible for applications to query user information rapidly.

LDAP is a protocol. Active Directory is a directory server. LDAP is a cross-platform open standard, but Active Directory is Microsoft’s proprietary software meant for Windows users and applications.

- ## Events tab

    - The Events tab is a log of things that have been going on behind the scenes for any given account. Sometimes this log will include little depending on the type of account; and a user account will have more happening than a resource or even a test account.

    - A comprehensive guide to everything which could be found in this log is outside the scope of this documentation.

    - Log entries under Past Identity Events include “Launched workflows” to show changes, updates, and merely auditing records. Note Source information in the column so designated. Notification email address changes, name changes, and things which may be relevant to troubleshooting may be found in the events log.

    - Access Requests is listed at the end of the Past Identity Events. If there are any log entries here, the individual account you are viewing will be an individual who has access to perform access requests in AVU. A VSA will have access for this.

SECTION 3: CUBES

- ### Cubes Structure

    - As previously discussed Cubes contain Cards.

    - Cards are a visible record of data which exists within other systems. The RACFId, FIS, WorkDay, and CCO cards are examples of cards which contain a set of data provided to AVU from external systems. Those systems may have received details from AVU initially – such as the CCO card as one example.

    - Each card in a cube may interact with other cards in that cube. No card can interact with other cubes or the cards within other cubes.

    - Interaction is best described by example. The WorkDay card "drives" the VUMCID, that is in the cube with it. The status of a feed from WorkDay affects the VUMCID. The action of a change in status to the WorkDay feed (which happens first in the WorkDay system itself) will trigger an action which in turn updates the status of a VUMCID in the same cube. The SailPoint IdentityIQ system facilitates this.

        - What this means in practical terms, is when an adjustment is made such as a termination-date applied in WorkDay, this causes a transaction to be transmitted to AVU, and AVU registers the update and then takes action to terminate the VUMC ID on that date. The same occurs with a change in role, or in department, and the date that change occurs; and the like.

        - Writeback occurs where information from a VUMCID record is written back to WorkDay. This two-way communication occurs to maintain WorkDay systems. Examples of this is the UPN and the VUMCID itself. When new data arrives from WorkDay which results in the creation of a new Identity account, which in turn provisions an email account, this data can only be updated in WorkDay *after* AVU is finished its work creating those attributes. So, it is up to AVU to upload the changes back to WorkDay and then WorkDay accepts that package of information and updates the WorkDay record for that employee ID.

        - A similar process will occur on writeback for other changes, including when a change in status of the existing VUMCID goes from ePassDisabled to ePassDeleted. At that point, the email account is deleted, and the email address is no longer useful. This data-clearance also must be conducted in WorkDay. This is when communications with the former affiliate shifts from using their vumc.org email address to their existing home email address to login to WorkDay.

- Other systems conduct actions externally and periodically update AVU with the changes made in those systems, and the same basic process occurs. This will happen with changes from AVU to Active Directory, where the Microsoft Exchange processes are affected.

- Similar action occasionally occurs between other cards.

- Password changes occur only in the AVU system and then propagate to other systems downstream. This change will be reflected immediately in the Last Refresh date. A password reset will not refresh the CCO card, or SPOK, nor some of the other cards, but it will refresh Active Directory cards.

SECTION 4: SUPPORT DIRECTIVES

This section is intended to assist with helping determine what team can help with the diverse information provided in each section. It will not be as comprehensive as we might like; and the primary reason for that is that processes are in a state of constant flux, and processes and options and support teams will change as time moves forward. Because of this, the information provided as of the time of this writing will be a useful guide to direct you to Knowledge Articles which by and large will continue to be updated to current state.

○ Support Directives by Type

- **Account Name** is a unique identifier created by the Identity System (AVU). It includes the following types along with the name of the team that provides Tier 2 level support *for most issues related to the* ***type***. Additional information regarding where to find more information and Tier 3 support teams is made available in this list.

    1. **VUMCID**: VUMC IT PARTNER SUPPORT - KM0011656
        - Tier 3: **VUMC IT IDENTITY**
    2. **CommunityID**: VEC ACCESS SYSTEMS - KM0013520
        - Tier 3: **VEC DIRECTORY SERVICES**, **VUMC IT IDENTITY**
    3. **ResourceAccount**: VUMC IT PARTNER SUPPORT - KM0015698
        - Ownership and Extensions: KM0000021
        - New Account: Pegasus Request
        - Tier 3: **VEC DIRECTORY SERVICES**, **VUMC IT IDENTITY**
    4. **Test**: VUMC IT PARTNER SUPPORT
        - Ownership and Extensions: KM0000021
        - New Account: Pegasus Request
        - Tier 3: **VEC DIRECTORY SERVICES**, **VUMC IT IDENTITY**
    5. **SEM** (Shared Email): VUMC IT COLLABORATION PLATFORMS
        - Created and managed through CollabHub
        - See also: KM0016141, or submit a Pegasus Request
        - Tier 3: VUMC IT PARTNER SUPPORT, **VUMC IT IDENTITY**
    6. **Admin** (TLA): VUMC IT PARTNER SUPPORT
        - New Account: KM0013463

○ Support Directives by Field

- **User Principal Name** (UPN) is created by the AVU system upon instantiation of the account which needs a UPN. All types except the SEM type will be assigned a UPN. Changes to the UPN is possible for *some* account types. Support and Questions to VUMC IT PARTNER SUPPORT. Tier 3 Support by **VUMC IT IDENTITY**. See also KM0010524.
- **Employee ID** is information provided by Human Resources' WorkDay system and recorded here in AVU. It is only populated if there is a WorkDay presence for the account. *Only user accounts (either non-employee or staff) will have a presence in WorkDay*.
    - Tier 2 Support: **VUMC IT PARTNER SUPPORT**
    - Tier 3 Support: **VUMC HR SYSTEMS**

- **Display Name** is information provided by WorkDay, where it is called the “Preferred Name”. It is managed in WorkDay, and if updated the changes propagate downstream to AVU and all other connected downstream systems. See Pegasus Article KM0014847 for more information.
- **Type**: This is the type of account currently in view and will be one of the following, and with the Tier 2 team noted as a primary source of assistance and information about that type:
  - VUMCID (VUMC IT PARTNER SUPPORT)
  - CommunityID (VEC ACCESS SYSTEMS)
  - ResourceAccount (VUMC IT PARTNER SUPPORT)
  - Test (VUMC IT PARTNER SUPPORT)
  - SEM (VUMC IT COLLABORATION PLATFORMS)
  - Admin (VUMC IT PARTNER SUPPORT)

- **Identity Object Name** is an identifier only insofar as troubleshooting current issues. However, it does have meaning for the VUMCID type account, as follows:
  - If it is another VUMCID it is an older one no longer in use because it advanced to ePassDeleted state before AVU 2.0 was released.
  - If it is the same as the VUMCID then this VUMCID was active before the new AVU 2.0 software was released, and it never experienced a disablement sufficient in duration to advance to ePassDeleted during the transition to AVU 2.0.
  - If it is a number that matches the Employee ID, then it is a new account created after AVU 2.0 was released. The ION for a VUMCID type account will consistently match the Employee ID of the WorkDay record that sourced the provisioning of the account.
- **Account Status (IIQ):** troubleshoot by status by following KM0016050
- **Inactive**: Will show disabled or blank. Blank indicates active.
- **LEGAL NAME**

  - **First Name** is from WorkDay and is the legal first name, not necessarily the preferred name.
    - *Accounts with no presence in WorkDay acquire the name from AVU itself upon account instantiation. This is true for all name fields.*
  - **Middle Name** from WorkDay and can be blank, a middle initial, or full name; it is the legal middle name.
  - **Last Name** is the legal surname in WorkDay.
  - **Suffix** is a usually the generational designation such as “Jr.”, or “IV”, etc. indicating a patriarchal succession (typically). This is also set in WorkDay.
- Note that the legal name is configured fully as part of a WorkDay record. Changes to it require changes in WorkDay. See KM0014847 for more detail.

- **Email** field is the “notification” email address, and for user accounts, comes from WorkDay, initially, as the “**Home Address**”. See this article, KM0014881, for more information. It will match the UPN when and if the Microsoft License is above F1. SEM, Test, ResourceAccount, and CommunityID accounts will always have an email address in this field. *This field will be blanked out for accounts which have attained the ePassDeleted state*.
  - Test accounts will have the owner’s email address here.
  - ResourceAccounts will typically have an SEM or Distribution List email address configured here.
- **VUMC Email**, also called the Primary email address is populated by the UPN for those accounts. The Primary email address is created by AVU. It is always created to be unique

from any other email address at either Vanderbilt University or Vanderbilt University Medical Center. At instantiation of the Identity Account in AVU, it will be created based on the name, first, middle, and last. The default domain is vumc.org.

> Please note, only the local-part of an email address (the section before the @) must be unique. In other words, it is not permitted for first.last@vanderbilt.edu to be used as first.last@vumc.org. The string before the @ must vary. The table that manages this "uniqueness" requirement is called the Collision Avoidable Table. The team that can assist and answer questions regarding it: **VUMC IT IDENTITY**.

  - Support for the mailbox begins at Tier 2 with VUMC IT PARTNER SUPPORT, Tier 3 is VUMC IT COLLABORATION PLATFORMS
  - Changes to the spelling of the UPN and thus the Primary email address can be requested by following the directions in KM0010524.
    - The format of an email address must follow a pattern which maintains consistency across the organization.
    - Users who need to know what their UPN is can reference KM0015724.
    - For information regarding Microsoft Licenses please refer to the following: KM0013846.

- **Vunet Legal Type** will always show VMC.
- **Manager** is the individual who manages the account-holder. Not all account types have a "manager". For most administrative purposes you would direct an individual to this person for assistance. This would be the individual who is best able to work directly with the user if there is a discrepancy with the Social Security Number, birthdate or other personal details, for example, and which may need attention in WorkDay.
  - Not all managers are staff members of VUMC. In WorkDay, this field is referred to frequently as the "one-up manager", meaning, the person who is first in line to create, sort, manage, approve and configure a user account in WorkDay.
- **Administrator** is responsible for the account. *User* accounts (that is accounts used solely for humans) do not have an administrator. If a VUMCID has an Associated Administrator account (Type: "Admin", also referred to as a "TLA"), then the administrator of the TLA *is* the VUMCID account holder associated with the admin account. ResourceAccounts and Test accounts will have an Administrator, also known as the "Owner". See KM0015698, Resource and Test Account: Ownership Model. Assistance for this subject is provided by VUMC IT PARTNER SUPPORT.
- **Worker Type** will be either employee or non-employee. In other places and contexts, a "non-employee" will be referred to as a Contingent Worker. This field applies to User Accounts *only* and is set by a field in WorkDay.

> Discrepancies for this field or any of the fields from Vunet Legal Type (underlined above) to here should be referred with an incident to **VUMC IT PARTNER SUPPORT**. Depending on specifics of any issue, Tier 3 may be **VUMC HR Systems**, or **VUMC IT Identity**.

- **Employment Status** is determined by WorkDay where applicable (user accounts only).
- **Employee Class** is also determined by WorkDay and will match Worker Type field ("Employee" and "Staff" being equivalent)
- **Primary Affiliation** is the one part of the affiliation string (next) that represents the primary relationship this account has with VUMC.
- **Affiliation** is the affiliation string. It includes all the various relationships this account has with VUMC. This string must be correct for access to certain applications and systems

within VUMC; and it both allows or restricts access as needed. As an example, those systems and resources to which faculty are provided access must include the faculty flag here in the affiliation before that account will be permitted access to that resource.

- **Job Title** is provided through WorkDay as part of the configuration on the employee* account.
    - *“Employee” in this context and in some other places, is in reference to an employee ID record, whether the account holder is staff or non-employee.*
- **Department** is configured in WorkDay as in Job Title above.
- **EPID** stands for **Enterprise Person Index Data** and is the number associated with the record (the Cube) you are looking at in the AVU tool at any given time. It is of note that it is possible to search for this number directly. Questions regarding this element should be directed to VUMC IT PARTNER SUPPORT.

> DEFINITION: "**IDENTITY CUBE**"
>
> An "Identity Cube", or simply "cube" in AVU 2 is a full set of records for any one entity or individual. It is defined by SailPoint as “a multi-dimensional view of each identity and their associated access and attributes”.

- **RACFId** – refers to Resource Access Control Facility Identifier. It is an older system no longer being used, and presently in the process of being retired. EStar has taken its place at VUMC. Information or questions regarding this field can be directed to VEC Access Systems.
- **Card Office HID Number,** managed by the Medical Center Card Services office, **HID** stands for **Hughes Identification Device**. This number is in reference to the card being carried by this individual for access to the various physical locations which are protected by the **HID** monitoring panels. Issues related to access and status of the card should be directed to the VUMC HR SYSTEMS team.
    - Detail of the card itself is in Identity Warehouse, Application Accounts tab, under VUMC-Application-CCO

- **Card Status** will show “I” for inactive, or “A” for active. The meaning is related to the capabilities of the card provided, whether it includes a magnetic stripe. No other meaning can be attributed to this status. Questions regarding the status of a particular card should be directed to the VUMC HR SYSTEMS team using CI=**CSGOLD-VUMC** or contact the Card Services Office directly.

- **Create Date** shows when the VUMC ID itself was instantiated.

- **License Type** configured in AVU by an administrator or provided by default by WorkDay for a user account. This will be F1 for non-employees by default or E3 or E5 for staff. Support for the Microsoft License can be addressed by VUMC IT COLLABORATION PLATFORMS.

- **Last Password Change Date, and Password extension in days and Password extension date** includes information which can be used by Helpdesk and other support teams to determine when the password was last updated.

- Support Directives by Team with common CIs
    - **VUMC HR SYSTEMS**
        - **Common Configuration Items (CI)**
            - WORKDAY-HUMAN_RESOURCES
            - CSGOLD-VUMC
        - Common issues pertaining to Employee ID, known discrepancies, and card office inquiries.
    - **VUMC IT PARTNER SUPPORT**
        - **Common Configuration Items (CI)**
            - PASSWORD VUMC-ID
            - EPI-MERGE
            - PARTNER SUPPORT
            - VUMC ID – NEW-RENEW
            - VOICEMAIL SYSTEM
            - M365-TEAMS-VOICE
        - Tier 2 team that assists with matters pertaining to a VUMC ID , including access problems, Email changes and configuration, Voice Services (Skype and Teams) server configuration, claim issues where a VUMC ID exists related to duplications, VSA Administration training and service lead, responsible for Resource, Test and TLA account creations, and password problems which require special handling.
        - Escalation path from Helpdesk is often through Partner Support who can triage to determine whether another team must be engaged such as HR Systems, WorkDay, Collaboration, Identity, or VEC.

    - **VUMC IT COLLABORATION PLATFORMS**
        - **Common Configuration Items (CI)**
            - M365-LICENSING
            - M365-TEAMS-VOICE
            - M365 – APP
        - Email, Group, Teams and Azure, Microsoft Licensing in cooperation with the Software Store, ListServ, Distribution List and Shared Mailbox assistance.

    - **VUMC IT IDENTITY**
        - **Common Configuration Items (CI)**
            - ACCESSVUMC
            - COLLISION AVOIDANCE
            - ACCESSVUMC SAILPOINT ADAPTER
        - Only Incidents are accepted.

        - Tier 3 team for all things AccessVUMC-related.

- **VEC ACCESS SYSTEMS**
    - **Common Configuration Items (CI)**
        - SYSTEMS APPLICATION ACCESS
        - VEC-ACCESS-SYSTEMS-VHC
    - Multi-factor authentication system assistance and support, emergency re-activation or emergency disablement of Identity accounts.

- **VEC DIRECTORY SERVICES**
    - **Common Configuration Items (CI)**
        - SAFENET-SSS-PROD
        - MFA-SERVICE
        - ENTRA-MFA-VUMC365
    - Tier 3 for multi-factor authentication systems, verification of Resource and Test accounts, and Active Directory and Azure issues.

- **VUMC IT WORKDAY – APP SUPPORT**
    - **Common Configuration Items (CI)**
        - WORKDAY-SECURITY_ACCESS
        - MYWORKDAY-IMPLEMENTATION
    -
- **VUMC IT WORKDAY - INTEGRATIONS**
    - **Common Configuration Items (CI)**
        - WORKDAY-INTEGRATIONS
        - WORKDAY-DATABASE-LOADER
        - WALKME

- **VUMC IT WORKDAY - APP SECURITY**
    - **Common Configuration Items (CI)**
        - WORKDAY-SECURITY_ACCESS
    - Access problems with access to WorkDay by current workers (*not related to Password problems*)
    - In many cases it is best to engage with VUMC IT PARTNER SUPPORT before committing a ticket to this team.

- **VUMC IT NETWORK VOICE ENGINEERING AND OPERATIONS**
    - **Common Configuration Items (CI)**
        - ARM-APPLICATION
        - VOICE GENERIC

Additional References

The AccessVUMC tool: https://vumcidentity.app.vumc.org/identityiq/
Medical Center Card Services office
AccessVUMC 2.0 Reporting and Advanced Analytics.
KM0015505, How do I become a VUMC Services Administrator (VSA)
KM0016072, Profile View in AVU 2
KM0016050, VUMC ID Status-Based Troubleshooting Reference
KM0014847, Change Preferred Name (Display Name)
KM0014881, Change Notification Email Address
KM0015698, Resource and Test Account: Ownership Model
KM0010524, How to change your Primary Email Address (UPN)
KM0016044, How to Identify the current VUMC ID for a person
KM0000021, How to extend, or disable, a VUMC ID
KM0013358, VUMCID PASSWORD MANAGEMENT

INDEX

1. Access Requests 13, 20
2. Account Name 3, 8, 23
3. Account Status (IIQ) 5, 14, 24
4. Active Directory 19
5. Active Directory Card 17
6. Activity Tab 12
7. Additional References 30
8. Admin 3
9. Administrator 5, 15, 25
10. Affiliation 16, 25
11. Application Accounts Tab 6, 17
12. Associated Admin Account (See TLA)
13. Attributes 3, 14
14. Card 8, 21
15. Card Office 5
16. Card Office HID Number 26
17. Card Status 26
18. CCO Card 17
19. CI ACCESSVUMC 27
20. CI ACCESSVUMC SAILPOINT ADAPTER 27
21. CI ARM-APPLICATION 28
22. CI COLLISION AVOIDANCE 27
23. CI CSGOLD-VUMC 27
24. CI ENTRA-MFA-VUMC365 28
25. CI EPI-MERGE 27
26. CI M365 – APP 27
27. CI M365-LICENSING 27
28. CI M365-TEAMS-VOICE 27
29. CI MFA-SERVICE 28
30. CI MYWORKDAY-IMPLEMENTATION 28
31. CI PASSWORD VUMC-ID 27
32. CI SAFENET-SSS-PROD 28
33. CI SYSTEMS APPLICATION ACCESS 28
34. CI VEC-ACCESS-SYSTEMS-VHC 28
35. CI VOICE GENERIC 29
36. CI VOICEMAIL SYSTEM 27
37. CI VUMC ID – NEW-RENEW 27
38. CI WALKME 28
39. CI WORKDAY-DATABASE-LOADER 28
40. CI WORKDAY-HUMAN_RESOURCES 27
41. CI WORKDAY-INTEGRATIONS 28
42. CI WORKDAY-SECURITY_ACCESS 28
43. cLDAP 20
44. CommonAD 17, 18
45. Community ID 3
46. Configuration Items (CI) 27, 28

47. Contract End Date 18
48. CONTRACT_BEGIN_DATE 18
49. Create Date 16, 26
50. Cubes 21
51. Cubes Structure 21
52. Department 5, 16, 26
53. Display Name 5, 14, 24
54. Email 15
55. EMAIL_ADDRESS_HOME 15
56. Employee 16
57. Employee Class 19, 25
58. Employee ID 4, 14, 23
59. Employee Type 19
60. Employment Status 5, 16, 25
61. Enterprise Person Index Data 26
62. Entitlements 17
63. Entitlements Tab 6, 17
64. EPID 5, 16, 26
65. EStar 11
66. Events Tab 13, 20
67. First Name 24
68. HealthConnect 11
69. History Tab 12
70. Hughes Identification Device 26
71. Identity Cube 7, 26
72. IdentityIQ: See “*SailPoint IdentityIQ*”
73. Identity Object Name 3, 24
74. Identity Warehouse 1
75. Inactive 24
76. Job Title 5, 16, 26
77. Last Name 24
78. Last Password Change 26
79. Last Password Change Date 17
80. Last Refresh 12
81. LDAP 20
82. Legal Name 24
83. License Type 17, 26
84. Manager 5, 15, 25
85. Medical Center Card Services Office 26
86. Microsoft License 15
87. Middle Name 24
88. Non-Employee 16
89. Notification Email Address 24
90. Ownership Model 25
91. PARTNER SUPPORT 27
92. Password 22
93. Password Extension date 26
94. Password Extension in days 26

95. Past Identity Events 13, 20
96. PII 13, 14
97. Policy Tab 12
98. Primary Affiliation 16, 25
99. Primary Email Address 4, 15, 24
100. Profile View 3
101. RACFID 5, 16, 26
102. Resource Account 3, 16, 19
103. Risk Tab 12
104. Roles 6, 17
105. SailPoint IdentityIQ 1, 27
106. SEM 3, 4, 23, 24
107. SIP address 4, 6, 15
108. Status Column 12
109. Suffix 5, 24
110. Support Directives 23, 27
111. Termination date 19
112. Test 3, 4, 5, 6, 9, 15, 16, 19, 20, 24, 25, 27, 28, 29
113. Tier 2 25, 27
114. Tier 3 25
115. TLA 15
116. Type 5, 14, 24
117. User Principal Name (UPN) 3, 4, 23
118. User Rights Tab 13
119. VEC ACCESS SYSTEMS 23 , 28
120. VEC DIRECTORY SERVICES 23, 28
121. VUMC Email 5, 15, 24
122. VUMC HR SYSTEMS 23, 26, 27
123. VUMC IT COLLABORATION PLATFORMS 23, 27
124. VUMC IT IDENTITY 23, 27
125. VUMC IT NETWORK VOICE ENGINEERING AND OPERATIONS 28
126. VUMC IT PARTNER SUPPORT 23, 27
127. VUMC IT WORKDAY - APP SECURITY 28
128. VUMC IT WORKDAY – APP SUPPORT 28
129. VUMC IT WORKDAY - INTEGRATIONS 28
130. VUMCAD 17, 18
131. VUMC-Application-AccessVUMC 8
132. VUMC-Application-CCO 8, 26
133. VUMC-Application-cLDAP 11
134. VUMC-Application-CommonAD 8
135. VUMC-Application-EIR 9
136. VUMC-Application-FIS 9
137. VUMC-Application-IIQ-Loopback 10
138. VUMC-Application-IIQ-P1 10
139. VUMC-Application-MarketoWS 11
140. VUMC-Application-RACFID 10
141. VUMC-Application-SPOK 10
142. VUMC-Application-VMCHR 11

143. VUMC-Application-VUMCAD 11
144. VUMC-Application-WorkDay 11
145. VUMCID 1, 3, 4, 5, 7, 8, 9, 11, 12, 14, 16, **17**, 21, 23, 24, 25
146. Vunet Legal Type 25
147. Work Contact Information 10
148. WorkDay 5, 6
149. WorkDay Card 8, 11, 12, 14, 15, 17, 18, 19, 21
150. Worker Type 6, 16, 25
151. Writeback 8, 21

VUMC IT PARTNER SUPPORT
Mark L. Bloss
July 31, 2024