

# AccessVUMC

## Identity Management tool

Resource Account Administration User Guide

VANDERBILT  UNIVERSITY  
MEDICAL CENTER

Information Technology

# AccessVUMC – What’s new for everyone?

1. **AccessVUMC is the new Identity Access Management tool for our workforce.**
  - [Check out the new AccessVUMC homepage](#)
2. **Enrollment in Multi-Factor Authentication is a requirement to protect and manage your resource accounts.**
  - If you are not already enrolled, visit the [Enterprise Cybersecurity MFA home page](#).
  - [See the new sign on experience](#)
3. **All current usernames and passwords will remain the same;** however, usernames are now called VUMC IDs.
  - VUMC no longer uses the term “ePassword”.
4. **Managing a VUMC account looks and feels different for our users.** See the [AccessVUMC User Guide](#) for information on how to change a password, how to set a display name, and how to reset a forgotten password.

Visit <https://www.vumc.org/it/vumc-it-identity-management-project-accessvumc> to see more about the AccessVUMC Identity Management Project.

# AccessVUMC – What's new for account administration?

**Administering a Resource Account is the same in most areas, but the workflow is new for the following functions:**

- [Change the password for a Resource Account](#)
- [To set a Resource Owner for a Resource Account – submit a Pegasus Ticket to https://pegasus.mc.vanderbilt.edu/request/start/5656/?s=](#)
- [To request a Resource Account, submit a Pegasus Ticket to https://pegasus.mc.vanderbilt.edu/request/start/5656/?s=](#)

All other Resource Account services will be provided by Vanderbilt University Partner Support until the next phase of the project.

Find out more about the AccessVUMC Identity Management Project at <https://www.vumc.org/it/vumc-it-identity-management-project-accessvumc>.

# The new AccessVUMC home page

New Sign On Experience 1 of 3

Find the new AccessVUMC home page at:

<https://www.vumc.org/it/accessvumc>.

This page will go live on January 31, 2020.

- Click on **Administrators**.
- From here you will authenticate using your VUMC ID and password.

Back to “What’s new for account administration?”

VANDERBILT UNIVERSITY  
MEDICAL CENTER

VUMC Information Technology

Home About Us Help & Support IT Services Software & Hardware Email & Connectivity **AccessVUMC** Cybersecurity

## AccessVUMC Identity Management

OVERVIEW  
If you need to cla ID and Password

New Users Existing Users **Administrators**

Contact the Help Desk

**Phone:**  
615-343-HELP (3-4357)  
(615-343-9999 for Phone Services)

**Online:**  
[Submit a help desk ticket](#) if you are experiencing an issue.  
[Submit a request](#) if you need access or an IT service performed.

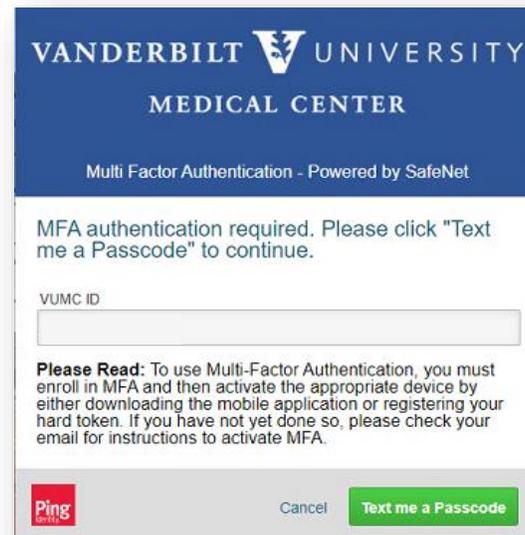
**Desktop Services Business Hours**  
Monday-Friday 7:00 a.m. - 6:00 p.m.

**After Hours Support**  
Call the Help Desk at 615-343-HELP (3-4357).  
If your issue impacts patient care, Desktop Engineering provides 24/7 after-hours desktop support for emergencies.

You will be prompted to authenticate using Multi-Factor Authentication. If you haven't enrolled already, visit [www.vumc.org/enterprisecybersecurity/mfa](http://www.vumc.org/enterprisecybersecurity/mfa).

NOTE: Your MFA sign on experience will vary based upon your MFA enrollment status (e.g. token, SMS texting, etc.).

MFA Sign on for SMS Text users



VANDERBILT UNIVERSITY  
MEDICAL CENTER

Multi Factor Authentication - Powered by SafeNet

MFA authentication required. Please click "Text me a Passcode" to continue.

VUMC ID

**Please Read:** To use Multi-Factor Authentication, you must enroll in MFA and then activate the appropriate device by either downloading the mobile application or registering your hard token. If you have not yet done so, please check your email for instructions to activate MFA.

 Cancel

MFA Sign on for Token users



VANDERBILT UNIVERSITY  
MEDICAL CENTER

SMS Code Verification

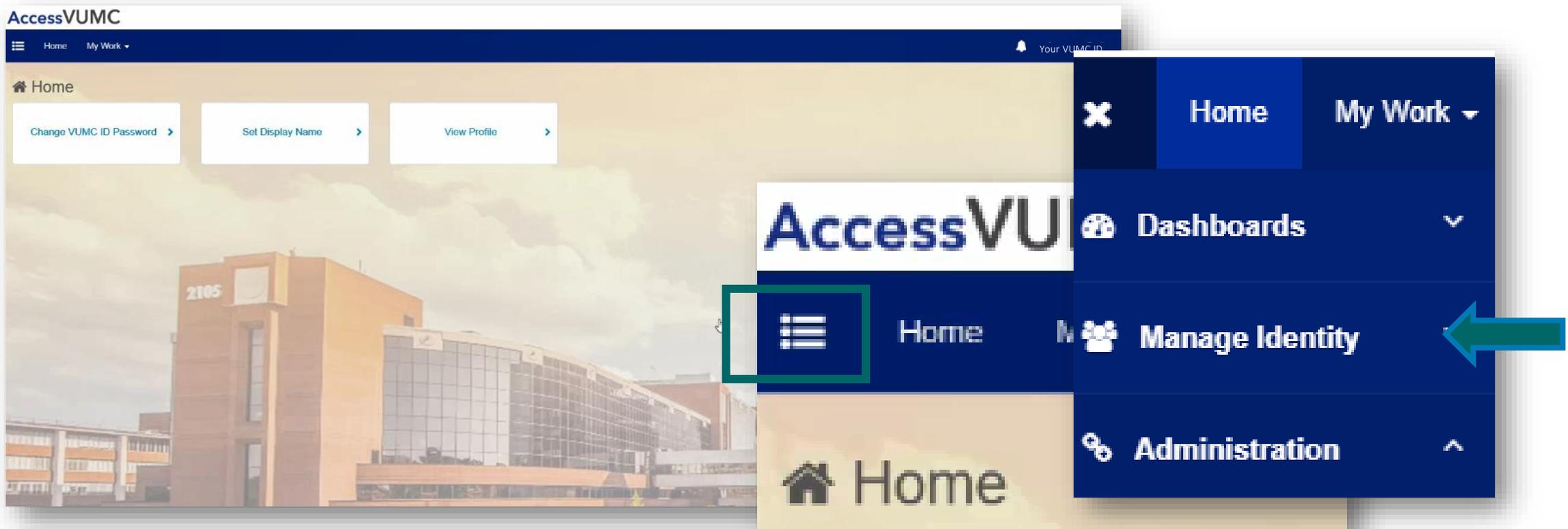
A passcode was sent as a text-message to your mobile device number on file. Please enter the code here and click "Sign On".

Passcode

 Cancel

Back to “What’s new for account administration?”

From the AccessVUMC dashboard you can manage your VUMC Resource Account password by clicking on the menu button ☰ and then **Manage Identity**.



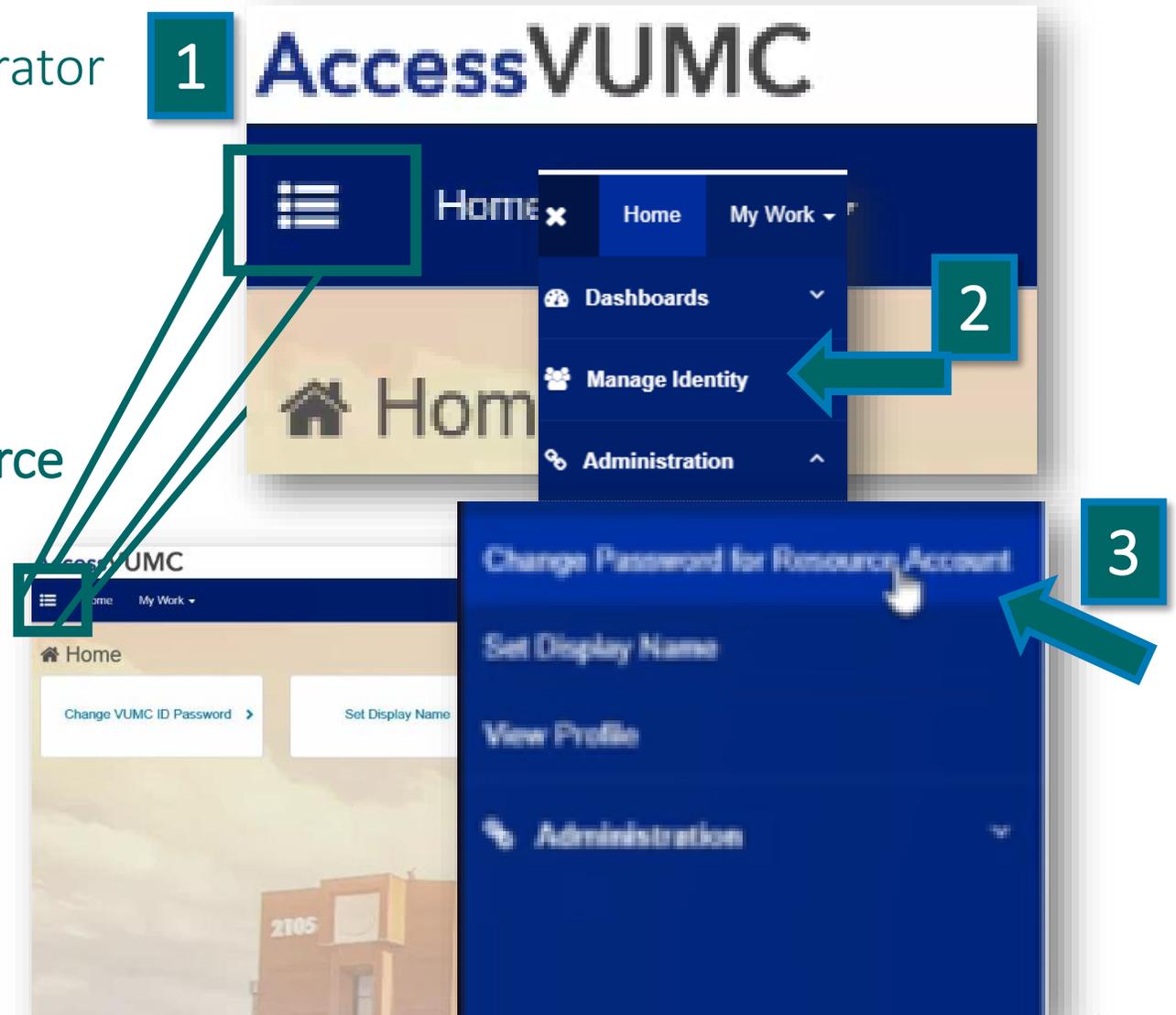
# AccessVUMC Identity Management Tool

## Change the password for a Resource Account

### AccessVUMC Identity Management

[Back to “What’s new for account administration?”](#)

- Login to the AccessVUMC Administrator dashboard. [See sign on slides.](#)
- Click the **menu** button ☰ from the AccessVUMC dashboard.
- Choose **Manage Identity**.
- Choose **Change Password for Resource Account**.



Click **Accept** once you have read the VUMC Acceptable Use Policy regarding your computer privileges and responsibilities.

#### **E. Publication or Distribution of Unauthorized Recordings, Photos, Images, Text or Video**

With the availability of low cost cameras, smart phones, and consumer electronics, it is possible for someone to acquire voice, video images, still images, multimedia, or text in non-public situations without the knowledge or consent of all parties. VUMC network computing assets must not be used by anyone in the organization to publish or distribute this type of material without the expressed consent of all involved parties.

#### **F. Right to Copy and Inspect for Legal, Regulatory, and VUMC Purposes**

VUMC is committed to protecting the privacy of faculty, students, staff, patients, and other users of its IT resources, and their electronic communications. However, because VUMC operates subject to compliance with various federal and state laws and regulations and must be able to enforce its own policies, VUMC must occasionally inspect, preserve and produce records to fulfill legal obligations and to carry out internal investigations. VUMC reserves the right to obtain, copy, and convey to outside persons any records or electronic transactions completed using VUMC information systems in the event it is required by law or institutional policy to do so. VUMC may also in its reasonable discretion, when circumstances require, obtain and review any records relevant to an internal investigation concerning compliance with VUMC rules or policies applicable to faculty, staff, or to all others granted use of VUMC's information technology resources. Users therefore should not expect that records created, stored or communicated with VUMC information technology or in the conduct of VUMC's business will necessarily be private. VUMC reserves its right to any work product generated in the conduct of its business.

#### **G. Locally Specific Policies**

Individual units within VUMC may create additional policies for information resources under their control. These policies may include additional detail, guidelines and further restrictions but must be consistent with principles stated in this policy document. Individual units adopting more specific policies are responsible for establishing, publicizing and enforcing such policies, as well as any rules governing the authorized and appropriate use of equipment for which those units are responsible.

### **IV. Disclosures**

**A.** All members of the VUMC Workforce Members are given notice of this policy by virtue of its publication and are subject to it on the same basis. Ignorance of this policy does not relieve any user of his or her responsibilities under the policy. All Workforce Members are expected to familiarize themselves with the contents of this policy and act in conformance with these principles regarding any use of VUMC's IT resources.

**B.** Due to the rapid nature of change in both information technologies and their applications, VUMC may amend this policy whenever deemed necessary or appropriate. Users are encouraged to periodically review this policy in order to understand their rights and responsibilities under it.

I Decline

Accept



- Verify the current password you use to manage your Resource Account (usually your personal password)
- Click **Next**.



**Verify Current Password**

We need to confirm your authority to modify this account.  
Please enter your VUMC ID password in order to proceed.

Password for **Your VUMC ID \***

- Enter and confirm the **NEW** password.
- Click **Submit**.

Keep these 3 password basics in mind when you create your VUMC Account password.

1. You cannot reuse your last 10 passwords
2. Passwords **MUST CONTAIN**:
  - At most 16 characters
  - At least 1 lowercase letter
  - At least 8 characters
  - At least 3 character types
  - At least 1 number
  - At least 1 uppercase letter
3. Passwords **CANNOT CONTAIN** your:
  - Email address
  - Account last name
  - Display name
  - Account names in reverse

**Set New Password**

Enter your new password below, following the listed requirements. Clicking "Submit" will change your password to the new value. You may exit at any time by clicking "Cancel".

**Identity Info**

Account Name: Your Account Name here

Full Name: Last Name, First Name

Account Type: Your VUMC ID

Email: Your @vumc.org email address

**Password**

New Password for: Your VUMC ID \*

ENTER

CONFIRM

- You will receive a confirmation screen that your password was successfully re-authenticated.
- You will also receive an email that your Resource Account password was changed.
- Click **OK**.



For all other Resource Account services, submit a Pegasus Ticket to

<https://pegasus.mc.vanderbilt.edu/request/start/5656/?s=>

VUMC Enterprise Cybersecurity (VEC) Directory Services will review your request and, if approved, forward your request to be finalized by Vanderbilt University Partner Support.

VEC Directory Services Resource Account Request

**FORM INSTRUCTIONS**