

AccessVUMC

Identity Management tool

User Guide

[Change a Password](#)

[Set your Display Name](#)

[Reset a Forgotten Password](#)

VANDERBILT  UNIVERSITY
MEDICAL CENTER

Information Technology

AccessVUMC Utilization Requirements

Please note:

To utilize the AccessVUMC Identity Management tool, enrollment in Multi-Factor Authentication is required. This extra layer of security ensures that your personal identifiable information (PII) is protected.

If you are not already enrolled, visit the Enterprise Cybersecurity website at:
<https://www.vumc.org/enterprisecybersecurity/multi-factor-authentication-mfa>

AccessVUMC – What's new?

- **AccessVUMC is the new Identity Access Management tool for our workforce.**
 - [Check out the new AccessVUMC homepage](#)
- **Enrollment in Multi-Factor Authentication is a requirement** to protect and manage your VUMC ID information.
 - [See the MFA sign on experience](#)
- **All current usernames and passwords will remain the same**, however usernames are now called VUMC IDs.
- **Managing your VUMC account looks and feels different** on the AccessVUMC dashboard.
 - [How to Change your Password](#)
 - [How to Set your Display Name](#)
 - [Forget your password? See how to Reset your Password](#)

Visit the [AccessVUMC Identity Management Project home page](#) for more information.

AccessVUMC – What's the same?

- **Most processes are the same** within AccessVUMC, they just look and feel different on the new dashboard
 - Claiming a new account is the same
 - Claiming an invitation is the same
 - Claiming a MAC Account is the same
 - Entering Personal Identifiable Information (PII) is the same
 - Claiming a Resource Account is the same
 - Claiming a Test Account is the same
- **Your username and password will remain the same; however, they will now be called a VUMC ID.**

Visit the [AccessVUMC Identity Management Project home page](#) for more information.

The new AccessVUMC home page

If you have a valid VUMC ID and password, and are enrolled in Multi-Factor Authentication, you can use AccessVUMC to manage your identity.

Find the new AccessVUMC home page at:

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

Return to "What's New" Menu

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 change your 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).

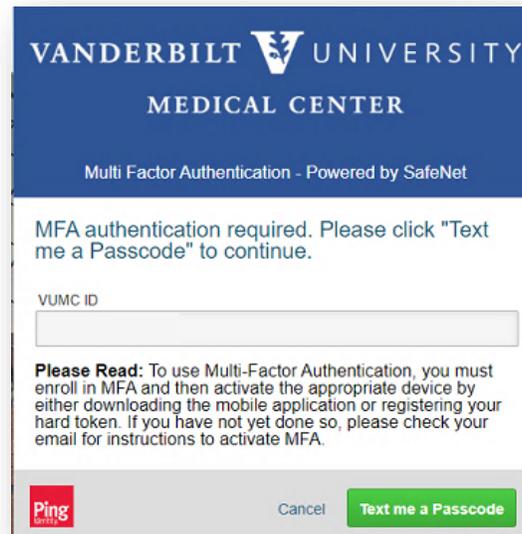
If your issue impacts patient care, Desktop Engineering provides 24/7 after-hours desktop support for emergencies.

Sign-On using Multi-Factor Authentication

When you sign on, you will be prompted to authenticate using Multi-Factor Authentication. If you haven't enrolled already, visit 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

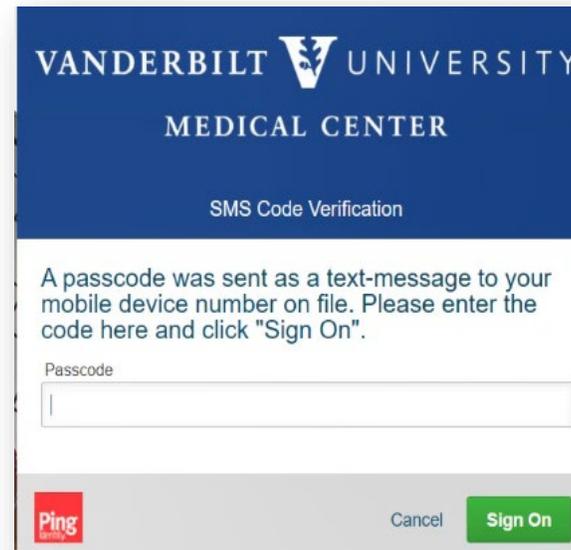
MFA authentication required. Please click "Text me a Passcode" to continue.

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.



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



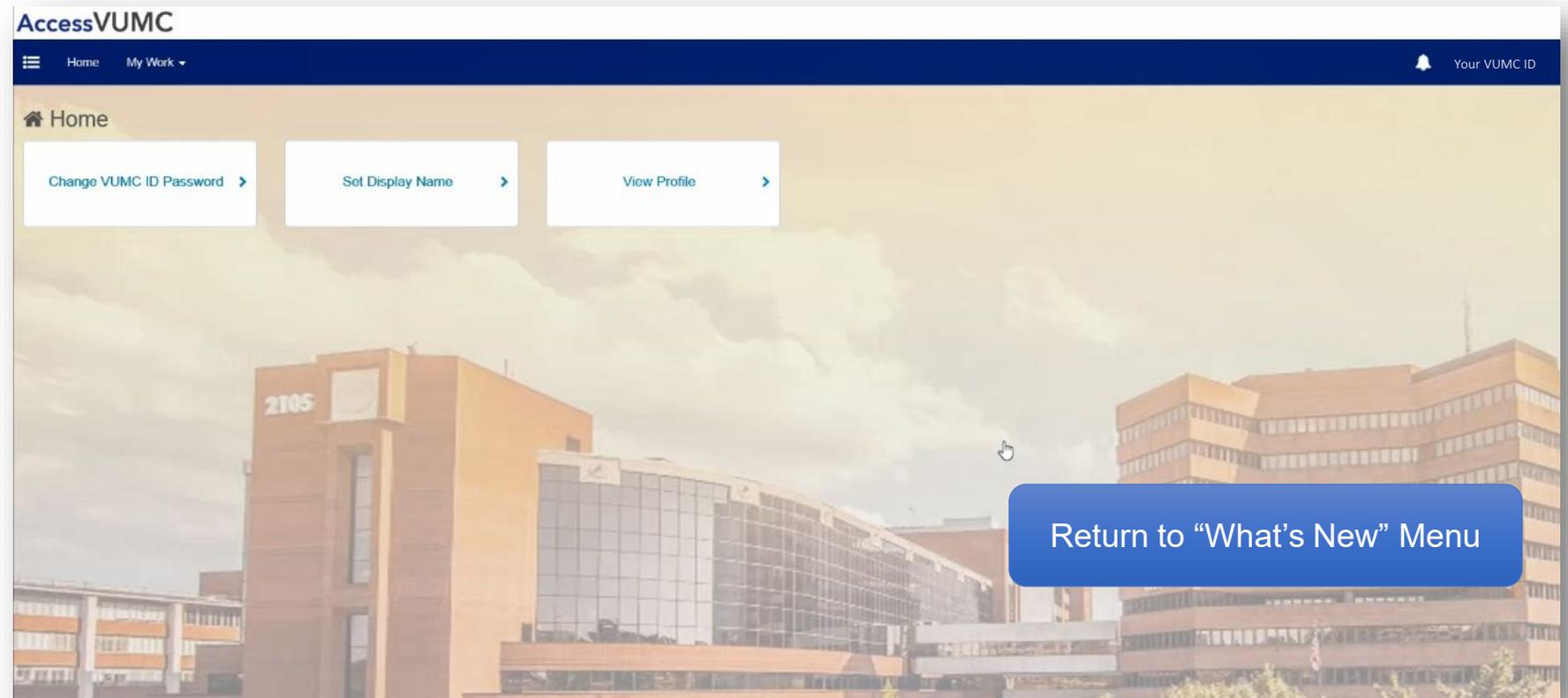
Return to "What's New" Menu

AccessVUMC Identity Management

The new AccessVUMC Identity Management dashboard

Once you authenticate, the new AccessVUMC dashboard will appear. From here you can:

- Change your VUMC ID Password
- Set your Display Name
- View Your Profile
- Click on the ☰ menu button to access other options



AccessVUMC Identity Management Tool

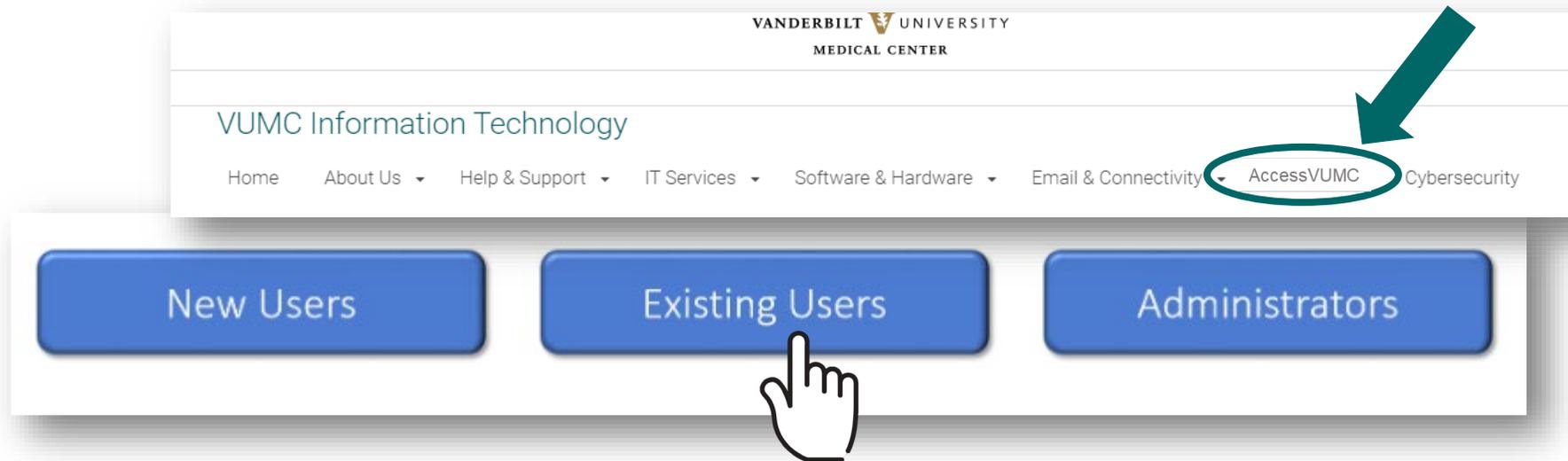
How to Change a Password

AccessVUMC Identity Management

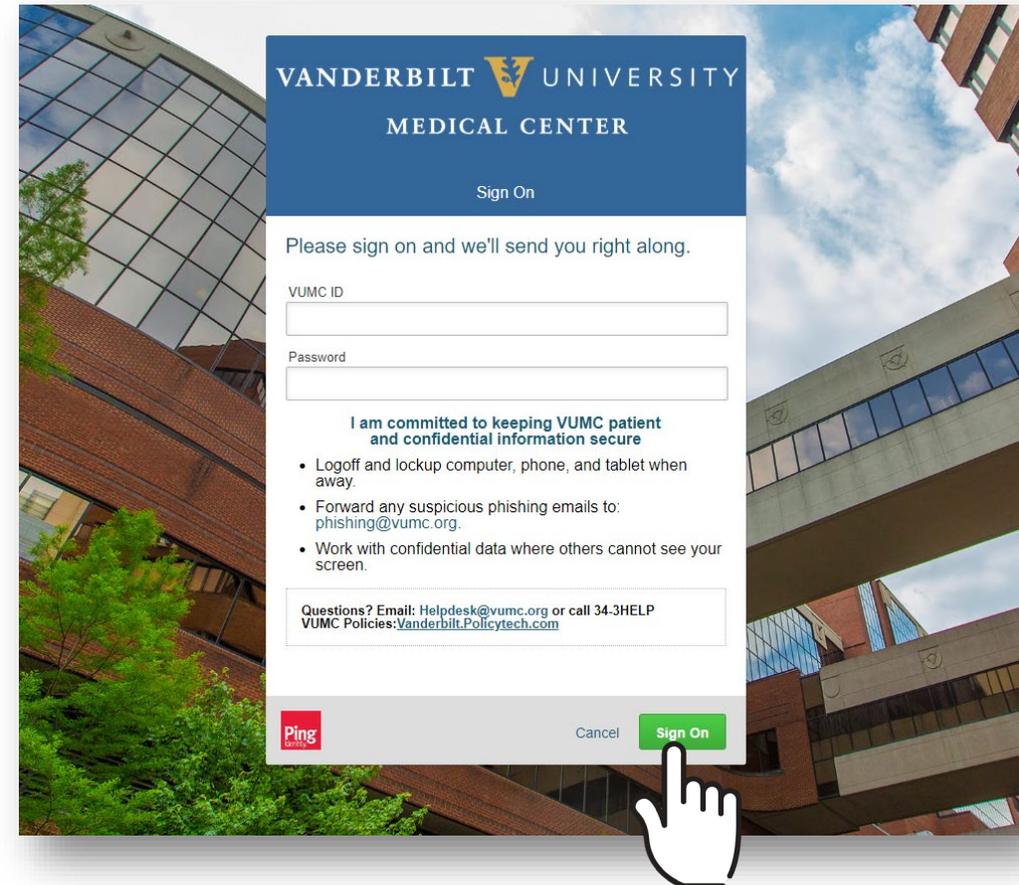
[Return to "What's New" Menu](#)

Users with a valid VUMC ID **AND** enrolled in Multi-Factor Authentication (MFA) can use AccessVUMC to change/reset a password.

- Click **Existing Users** from the AccessVUMC home page
<https://www.vumc.org/it/accessvumc>.

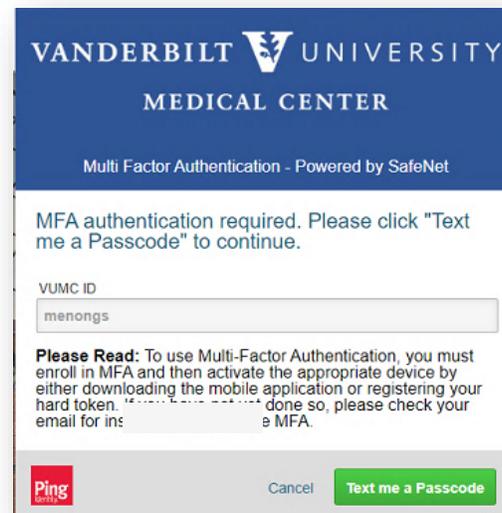


- From the AccessVUMC home page, you will be prompted to authenticate using your VUMC ID and password.
- Click **Sign On**.



- You will then be prompted to enter a Multi-Factor Authentication passcode.
NOTE: Your MFA sign on experience will vary based upon your MFA enrollment status (e.g. token, SMS texting, etc.).
- Click **Sign On** once you have entered your passcode.

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
menongs

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 already done so, please check your email for instructions on how to activate MFA.

Ping Identity Cancel Text me a Passcode

MFA Sign on for Token users



VANDERBILT UNIVERSITY
MEDICAL CENTER

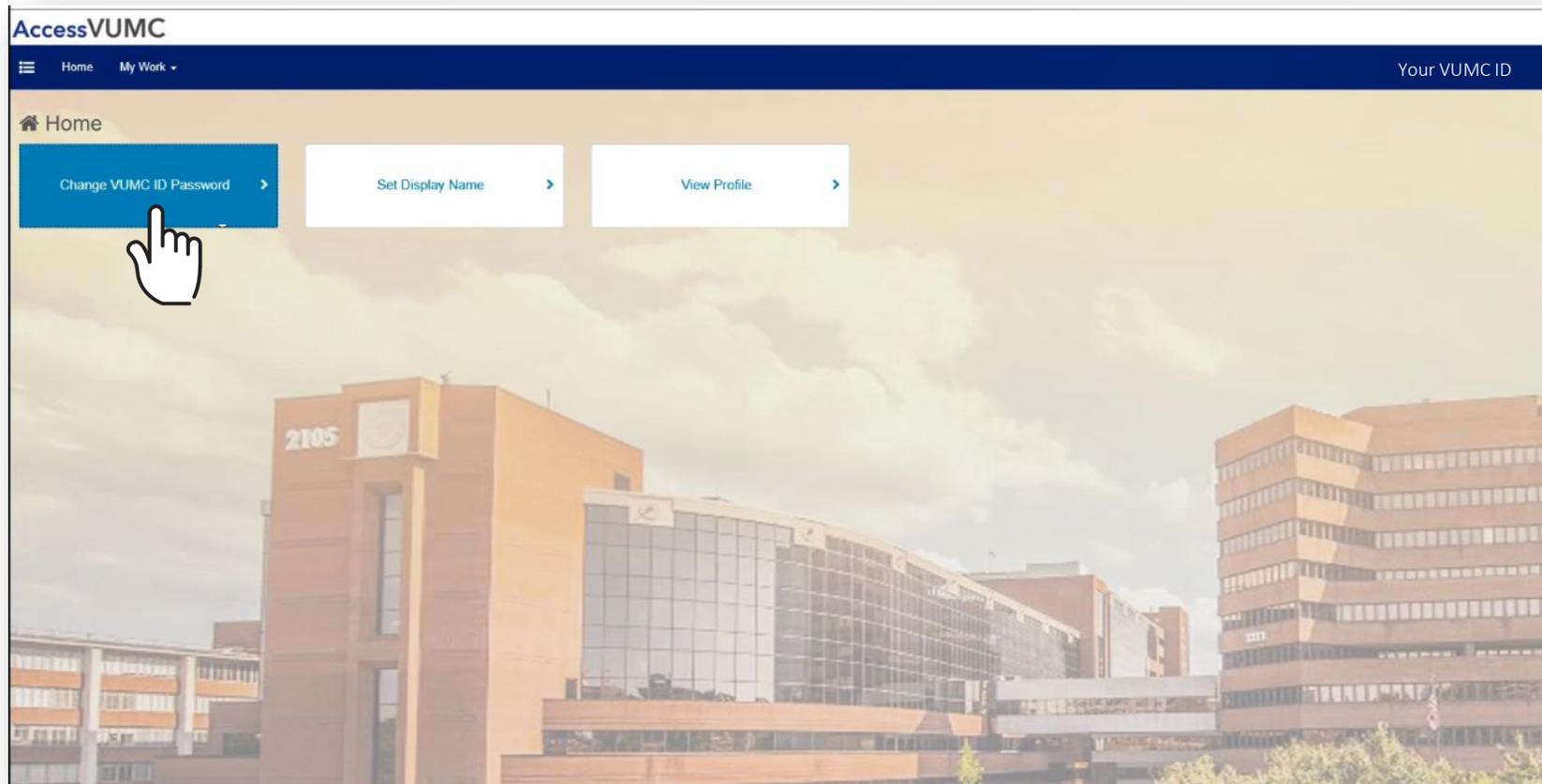
SMS Code Verification

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

Ping Identity Cancel Sign On

Click the **Change VUMC ID Password** button from the AccessVUMC dashboard.



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

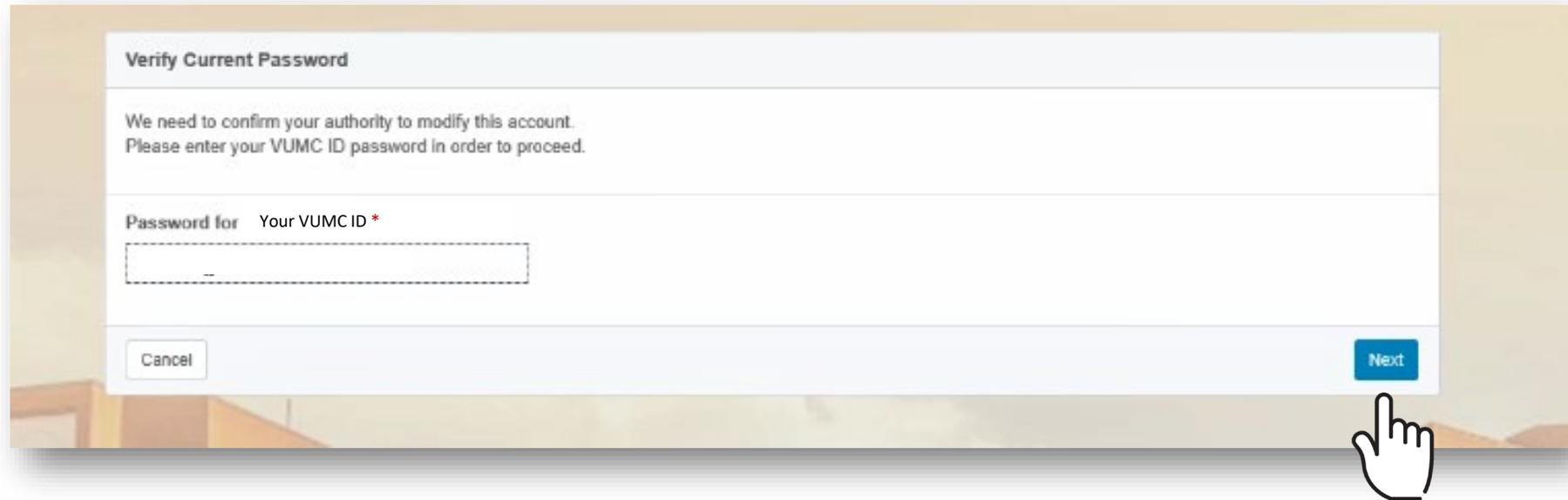
- A.** All members of the VUMC Workforce Members are given notice of this policy by virtue of its publication and are subject to it on the same basis. Ignorance of this policy does not relieve any user of his or her responsibilities under the policy. All Workforce Members are expected to familiarize 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 your current password.
- Click **Next**.



The screenshot shows a web form titled "Verify Current Password". The form contains the following text: "We need to confirm your authority to modify this account. Please enter your VUMC ID password in order to proceed." Below this is a label "Password for Your VUMC ID*" followed by a password input field. At the bottom of the form, there are two buttons: "Cancel" on the left and "Next" on the right. A hand cursor is pointing at the "Next" button.

- Enter and confirm your **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 ***

Confirm new password *

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



AccessVUMC Identity Management Tool

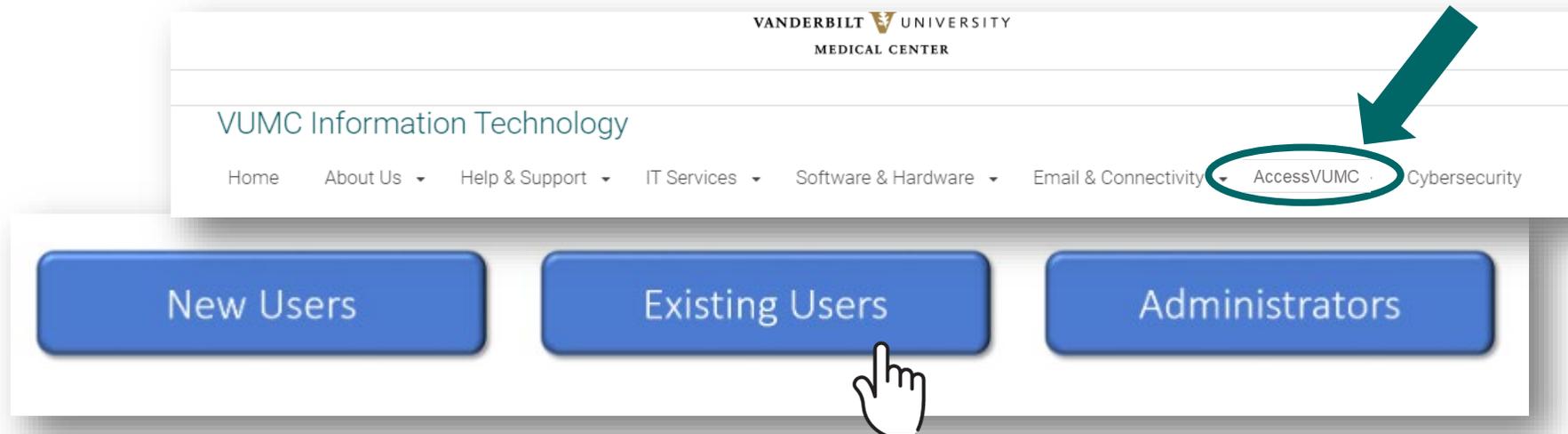
How to Set a Display Name

AccessVUMC Identity Management

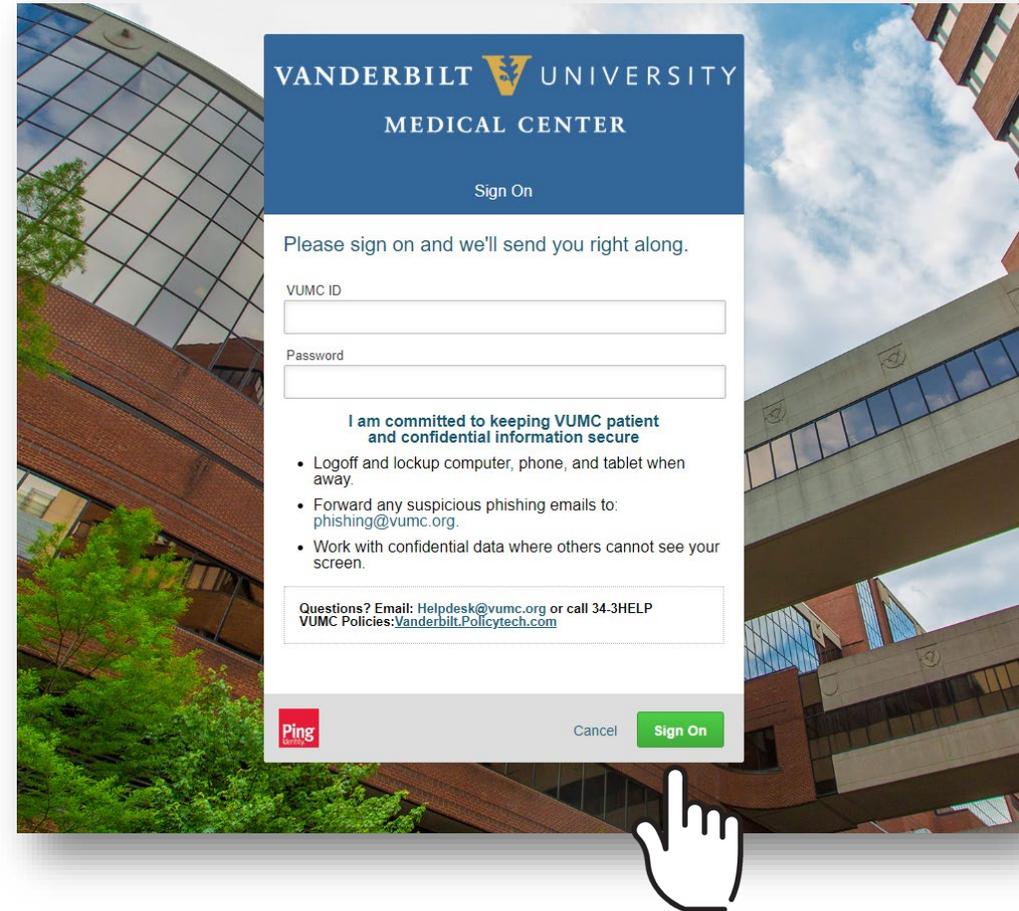
[Return to "What's New" Menu](#)

VUMC employees enrolled in multi-factor authentication AND with a valid VUMC ID can use AccessVUMC to Set a Display Name.

- Click **Existing Users** from the AccessVUMC website <https://www.vumc.org/it/accessvumc>.



From the AccessVUMC homepage, you will need to authenticate using your VUMC ID and password and **Sign On**.



- You will then be prompted to enter a Multi-Factor Authentication passcode.
NOTE: Your MFA sign on experience will vary based upon your MFA enrollment status (e.g. token, SMS texting, etc.).
- Click **Sign On**.

MFA Sign on for SMS Text users

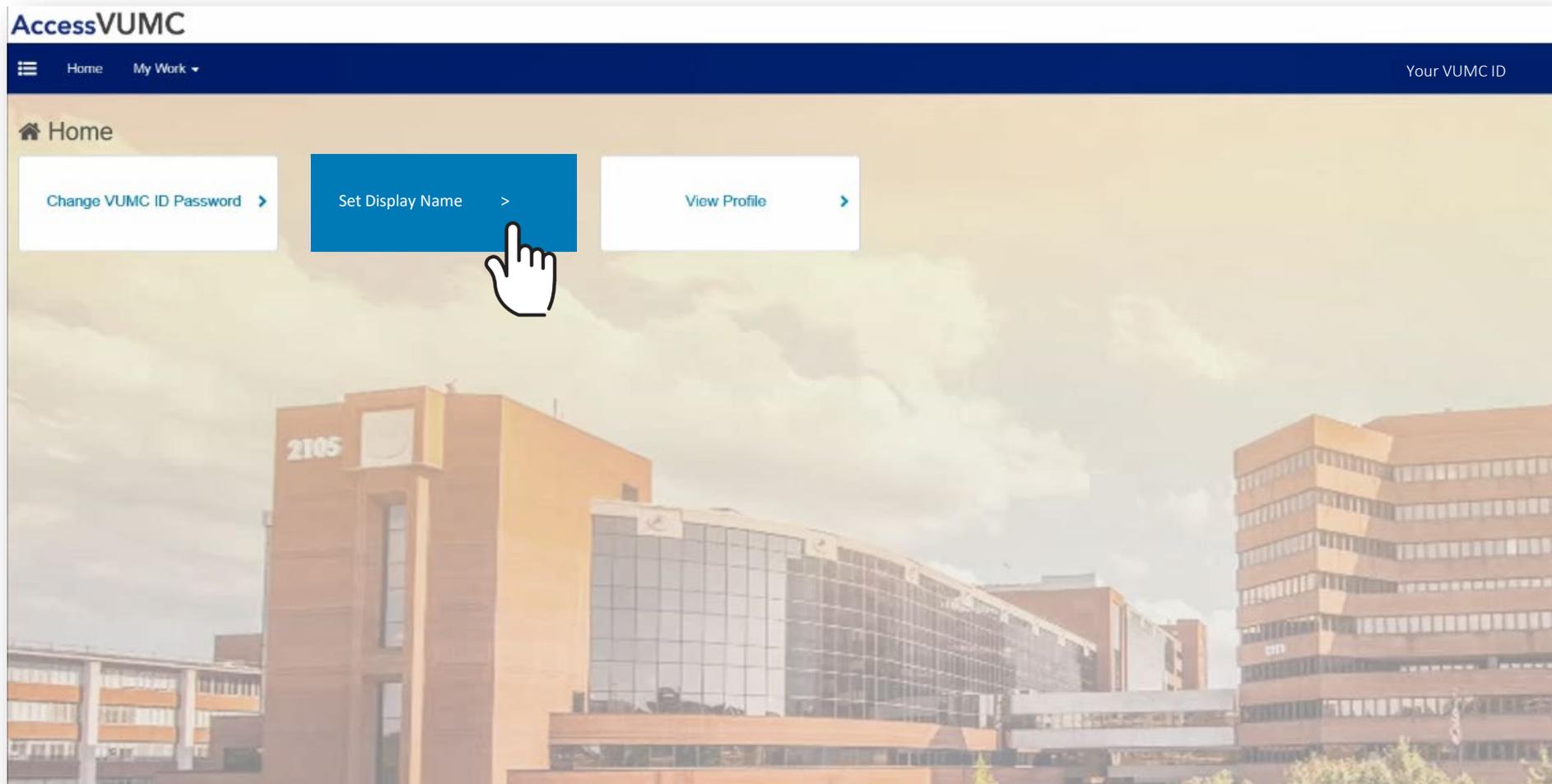
The screenshot shows the MFA authentication interface for SMS text users. At the top, it displays the Vanderbilt University Medical Center logo and the text "Multi Factor Authentication - Powered by SafeNet". Below this, a message states: "MFA authentication required. Please click 'Text me a Passcode' to continue." There is a text input field for "VUMC ID" containing the value "menongs". A "Please Read" section provides instructions on how to activate MFA. At the bottom, there are three buttons: a red "Ping" logo, a grey "Cancel" button, and a green "Text me a Passcode" button.

MFA Sign on for Token users

The screenshot shows the MFA authentication interface for token users. At the top, it displays the Vanderbilt University Medical Center logo and the text "SMS Code Verification". Below this, a message states: "A passcode was sent as a text-message to your mobile device number on file. Please enter the code here and click 'Sign On'." There is a text input field for "Passcode". At the bottom, there are three buttons: a red "Ping" logo, a grey "Cancel" button, and a green "Sign On" button.

Set your Display Name

Click **Set Display Name** from your AccessVUMC Dashboard.



- The Account's **Current Display Name**, **Last Name**, **First Name** and **Middle Name** will automatically appear.
- Enter the **New Display Name**.
- Click **Next**.

Set Display Name

Display Name is the name shown in the VUMC Corporate Outlook and Skype address list. You may customize First Name and Middle Name to your preference. Last Name cannot be modified. When you are ready to review your changes, click 'Submit'.

Account

Current Display Name
Doe, Jon

Last Name: Doe
First Name *: Timothy
Middle Name: Johnathon

New Display Name
TimothyDoe

Cancel Next



- Confirm the new display name on your account.
- Click **Submit**.

Set Display Name

Please confirm your new Display Name is correct. Click 'Back' to make changes or cancel. Click 'Submit' to update your display name.

Account

Current Display Name

Last Name	First Name *	Middle Name
<input type="text" value="Doe"/>	<input type="text" value="Timothy"/>	<input type="text" value="Johnathon"/>

New Display Name

AccessVUMC Identity Management Tool

How to reset a forgotten password

Forgot your password? Select your status:

1. [VUMC employees enrolled in Multi-Factor Authentication](#)
2. [Active VUMC ID holders enrolled in Multi-Factor Authentication](#)
3. [VUMC employees or active VUMC ID holders not enrolled in Multi-Factor Authentication](#)

[Return to “What’s New” Menu](#)

Reset a Password

For VUMC EMPLOYEES enrolled in Multi-Factor Authentication

Access VUMC Identity Management

[Return to "Reset Password" Menu](#)

VUMC employees enrolled in Multi-Factor Authentication AND with a valid VUMC ID can use AccessVUMC to Reset a Password.

Click **Existing Users** and **Forgot Password** from the AccessVUMC home page.

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

The image shows a screenshot of the AccessVUMC website. At the top, the Vanderbilt University Medical Center logo is visible. Below it, the text 'VUMC Information Technology' is displayed. A navigation menu includes links for Home, About Us, Help & Support, IT Services, Software & Hardware, Email & Connectivity, AccessVUMC (circled in green), and Cybersecurity. A green arrow points to the AccessVUMC link. Below the navigation menu, there are two large blue buttons: 'Existing Users' and 'Administrators'. A hand icon is pointing to the 'Existing Users' button. To the left of these buttons is a white box titled 'AccessVUMC - Existing Users'. This box contains an overview section and a section titled 'TO MANAGE YOUR VUMC ACCOUNT' which includes a 'Forgot Password' button. A hand icon is pointing to the 'Forgot Password' button. The bottom left corner of the image shows the Vanderbilt University Medical Center Information Technology logo.

- From the AccessVUMC home page, enter your VUMC ID.
- Click **Sign On**.

VANDERBILT UNIVERSITY
MEDICAL CENTER

Sign On

Please sign on and we'll send you right along.

VUMC ID

I am committed to keeping VUMC patient and confidential information secure

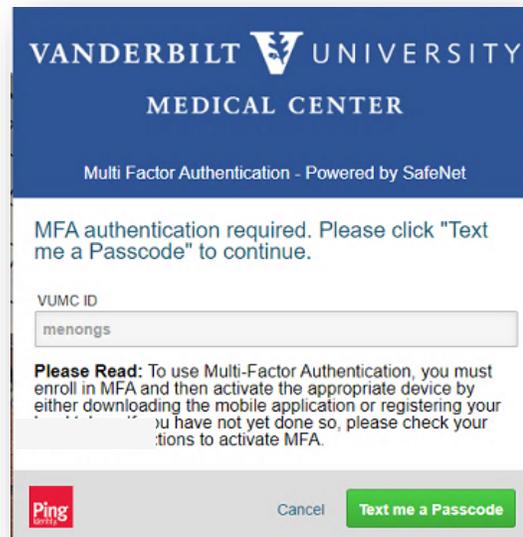
- Logoff and lockup computer, phone, and tablet when away.
- Forward any suspicious phishing emails to: phishing@vumc.org.
- Work with confidential data where others cannot see your screen.

Questions? Email: Helpdesk@vumc.org or call 34.3HELP
VUMC Policies: Vanderbilt.Policytech.com

Ping Identity Cancel Sign On

- You will then be prompted to enter a Multi-Factor Authentication passcode.
NOTE: Your MFA sign on experience will vary based upon your MFA enrollment status (e.g. token, SMS texting, etc.).
- Click **Sign On**.

MFA Sign on for SMS Text users



VANDERBILT UNIVERSITY
MEDICAL CENTER

Multi Factor Authentication - Powered by SafeNet

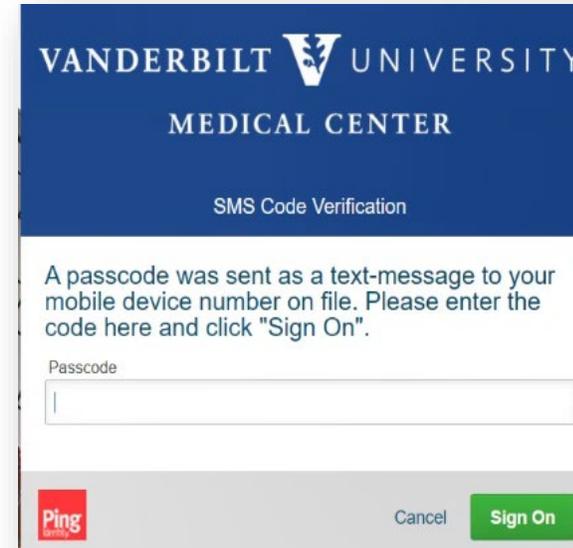
MFA authentication required. Please click "Text me a Passcode" to continue.

VUMC ID
menongs

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 device. If you have not yet done so, please check your enrollment options to activate MFA.

Ping Cancel Text me a Passcode

MFA Sign on for Token users



VANDERBILT UNIVERSITY
MEDICAL CENTER

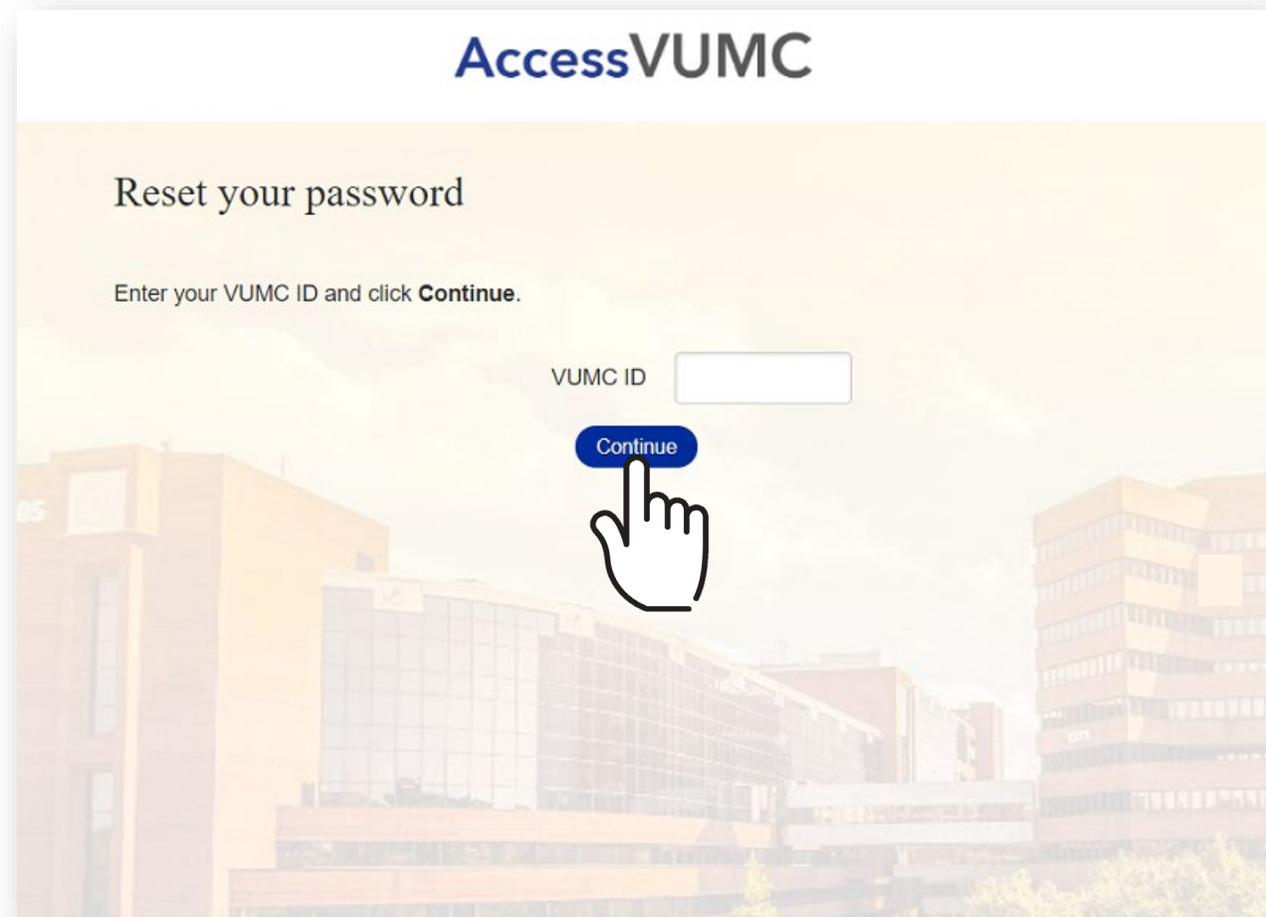
SMS Code Verification

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

Ping Cancel Sign On

- Confirm your identity by entering your VUMC ID again.
- Click **Continue**.



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



- Confirm your identity by entering your personal identifiable information (PII).
- Click **Continue**.

AccessVUMC

Confirm your identity

Enter the requested information below and click **Continue**.

First Name*

Last Name*

Last Five Digits of SSN (ex:99999)*

Confirm Last Five Digits of SSN (ex:99999)*

Date Of Birth*

Continue **Cancel**

- Enter your new password and confirm.
- Click **Submit**.

AccessVUMC

Reset your password

Enter your new password below, following the listed requirements.
Clicking **Submit** will complete the process of resetting your VUMC ID password.

VUMC ID: Your VUMC ID

New Password:*

Confirm New Password:*

The form may take a moment to process when submitted.

Submit **Cancel**

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

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



Reset a Password

For ACTIVE VUMC ID holders (not employees) enrolled in Multi-Factor Authentication

AccessVUMC Identity Management

[Return to "Reset Password" Menu](#)

Active VUMC ID holders who have forgotten their password and are enrolled in Multi-Factor Authentication can use AccessVUMC to reauthenticate.

Please take the following steps to reset your password:

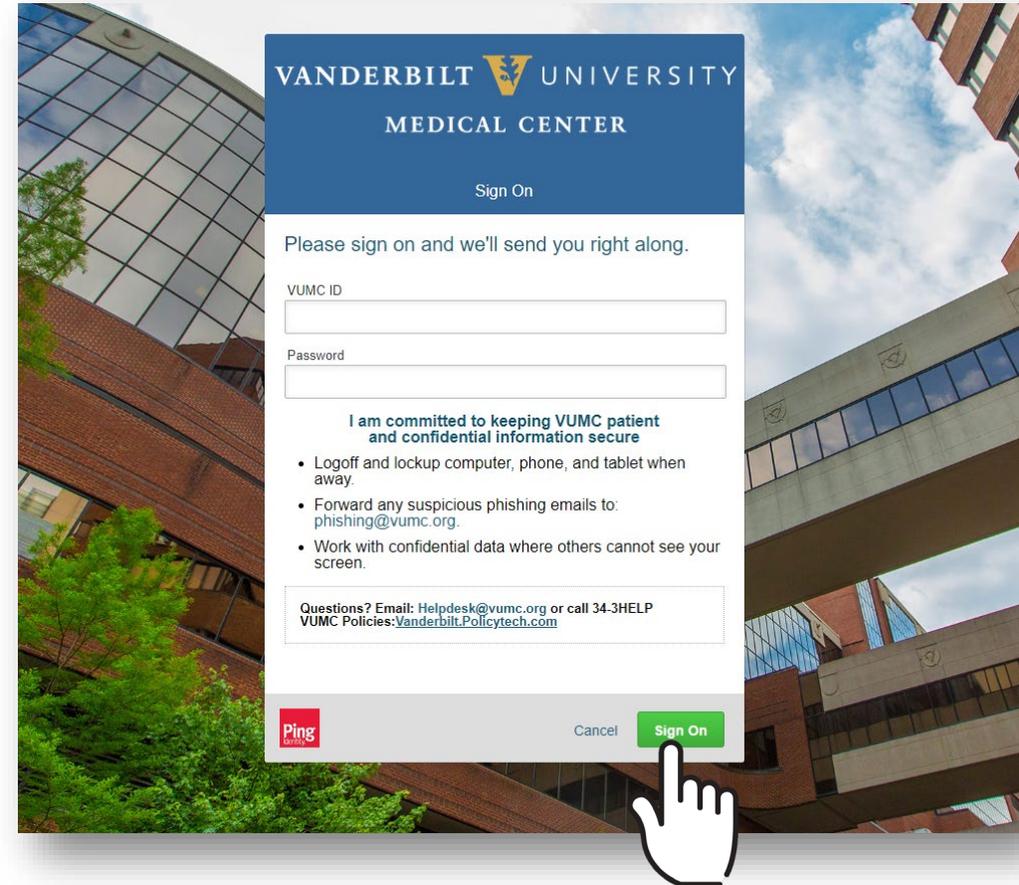
1. Contact the VUMC IT/NTT Help Desk at 615-343-HELP/3-4357 to start the Password Reset (reauthentication) Process.
2. When you receive your temporary login passcode, take the steps provided in the following slides.

Active VUMC ID holders include workforce members who are sponsored by departments including contractors, vendors, student employees, etc.

- After you have received your temporary MFA passcode, login to AccessVUMC at <https://www.vumc.org/it/accessvumc>.
- Click **Existing Users** and **Forgot Password**.

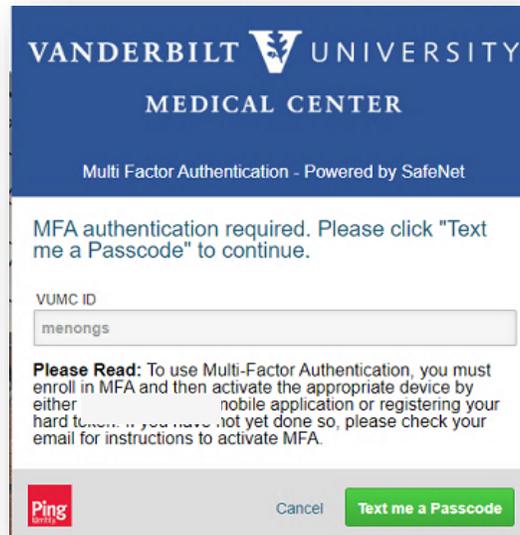
The screenshot shows the VUMC Information Technology website. At the top, it says "VANDERBILT UNIVERSITY MEDICAL CENTER". Below that is "VUMC Information Technology". A navigation menu includes "Home", "About Us", "Help & Support", "IT Services", "Software & Hardware", "Email & Connectivity", "AccessVUMC", and "Cybersecurity". The "AccessVUMC" link is circled in green, with a green arrow pointing to it from the top right. Below the navigation menu, there are two blue buttons: "Existing Users" and "Administrators". An inset window titled "AccessVUMC - Existing Users" is shown in the bottom left. It contains an "OVERVIEW" section with text about managing VUMC accounts and a "TO MANAGE YOUR VUMC ACCOUNT" section with a "Forgot Password" button. A hand cursor is pointing at the "Forgot Password" button.

- From the AccessVUMC homepage, you will need to authenticate.
- Use your VUMC ID and the temporary passcode you received from the Help Desk.
- Click **Sign On**.



- You will then be prompted to enter a Multi-Factor Authentication passcode.
NOTE: Your MFA sign on experience will vary based upon your MFA enrollment status (e.g. token, SMS texting, etc.).
- Click **Sign On**.

MFA Sign on for SMS Text users



VANDERBILT UNIVERSITY
MEDICAL CENTER

Multi Factor Authentication - Powered by SafeNet

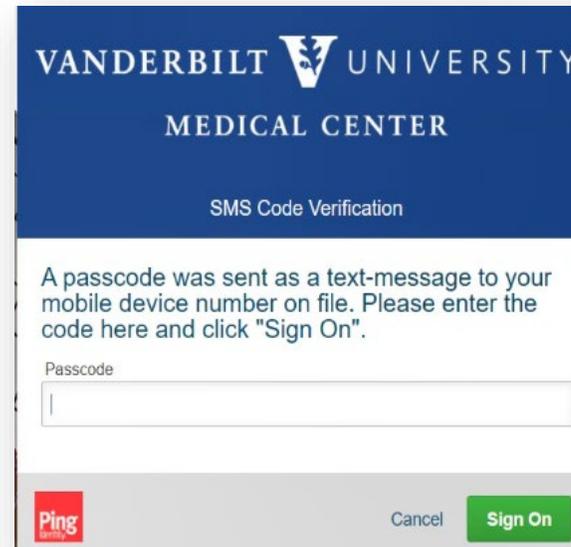
MFA authentication required. Please click "Text me a Passcode" to continue.

VUMC ID

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



MFA Sign on for Token users



VANDERBILT UNIVERSITY
MEDICAL CENTER

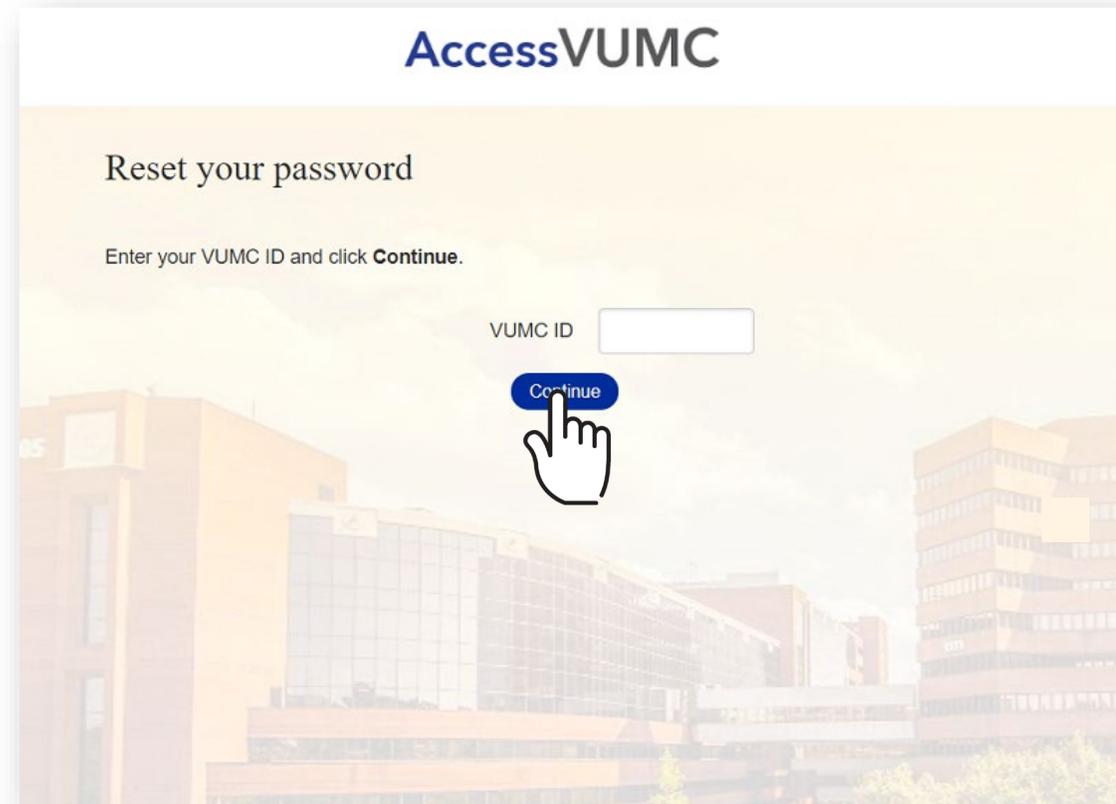
SMS Code Verification

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



- Verify your identity by entering your VUMC ID.
- Click **Continue**.



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.

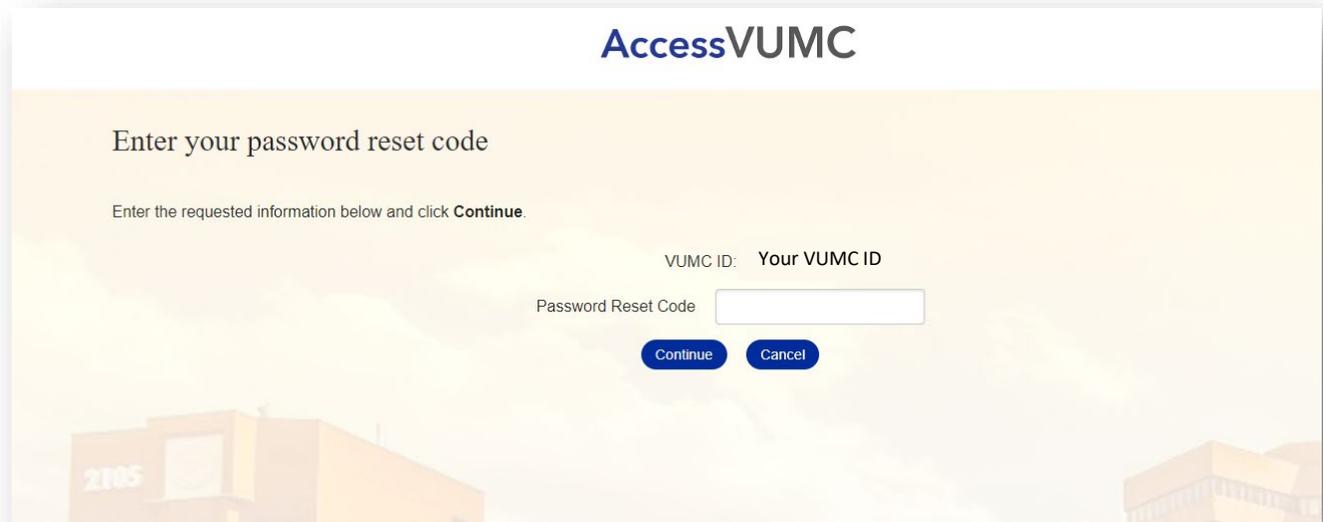
IV. Disclosures

- 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

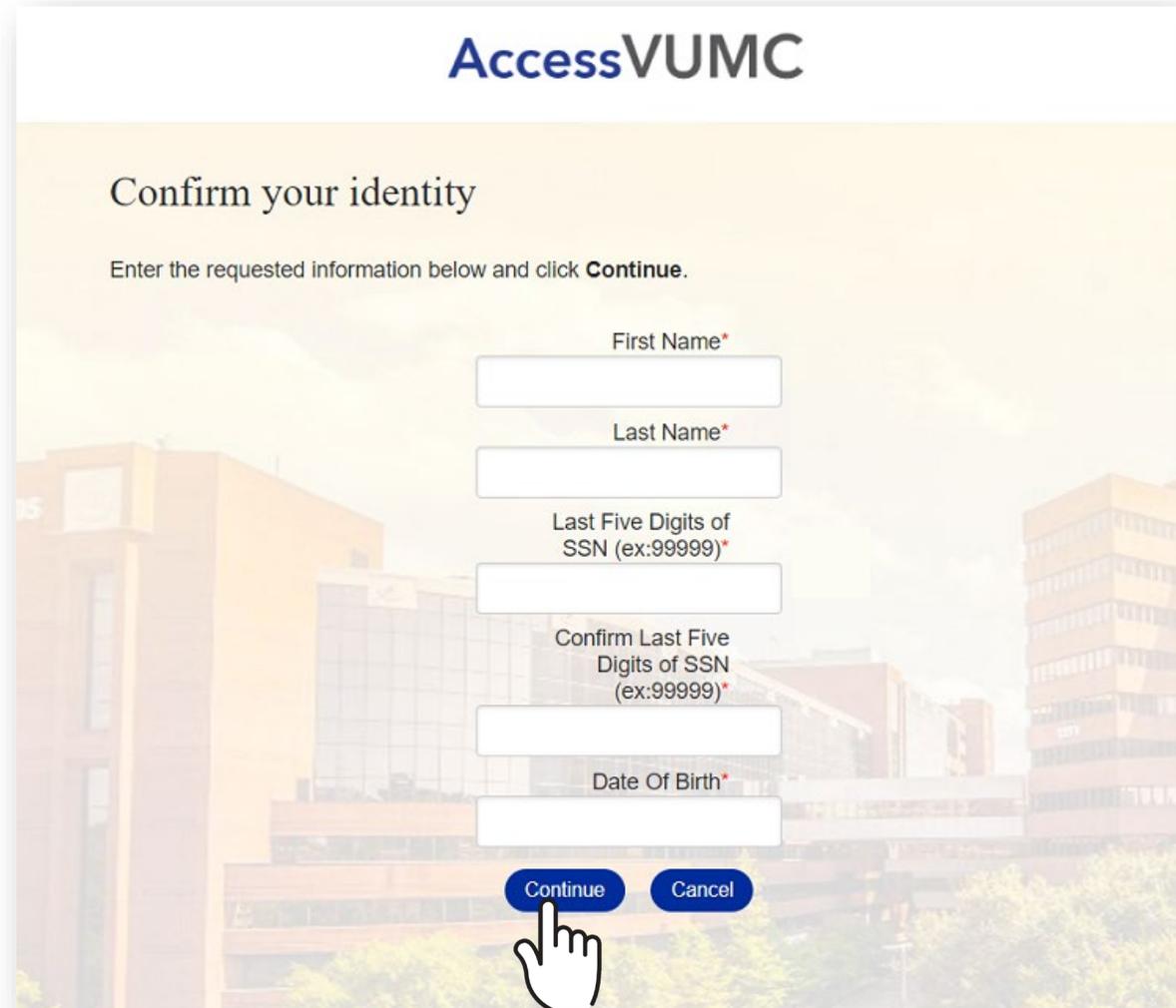


- If you receive the screen below, then you have not yet entered your Personal Identifiable Information (PII).
- Your PII is required to reset your password.
- Call the VUMC IT/NTT Help Desk at 615-343-HELP/3-4357 to get a one-time passcode.
- Use your one-time passcode to sign on at any time, follow the same steps, and, once you arrive at this screen, enter the code and click **Continue**.
- You can then follow the remaining instructions to reset your password.



The screenshot shows a web interface for 'AccessVUMC'. The main heading is 'AccessVUMC'. Below it, the instruction reads 'Enter your password reset code'. A sub-instruction says 'Enter the requested information below and click **Continue**.' There are two input fields: 'VUMC ID: Your VUMC ID' and 'Password Reset Code'. Below the 'Password Reset Code' field are two buttons: 'Continue' and 'Cancel'. The background features a faint image of a building with the number '2105'.

- Confirm your identity by entering your personal identifiable information (PII).
- Click **Continue**.



The screenshot shows the 'AccessVUMC' login page. At the top, the text 'AccessVUMC' is displayed in a blue font. Below this, the heading 'Confirm your identity' is centered. Underneath the heading, a prompt reads: 'Enter the requested information below and click **Continue**.' The form consists of five input fields, each with a label and an asterisk indicating it is required: 'First Name*', 'Last Name*', 'Last Five Digits of SSN (ex:99999)*', 'Confirm Last Five Digits of SSN (ex:99999)*', and 'Date Of Birth*'. At the bottom of the form, there are two buttons: 'Continue' and 'Cancel'. A white hand cursor is pointing at the 'Continue' button. The background of the page is a faded image of a large, multi-story brick building, likely a hospital or university building.

- Enter your new password and confirm.
- Click **Submit**.

AccessVUMC

Reset your password

Enter your new password below, following the listed requirements.
Clicking **Submit** will complete the process of resetting your VUMC ID password.

VUMC ID: Your VUMC ID

New Password:*

Confirm New Password:*

The form may take a moment to process when submitted.

Submit **Cancel**

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

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



Reset a Password

For VUMC EMPLOYEES or VUMC ID HOLDERS NOT ENROLLED in Multi-Factor Authentication

Access [VUMC Identity Management](#)

[Return to "Reset Password" Menu](#)

If you are a VUMC employee or active VUMC ID holder and are **NOT** enrolled in Multi-Factor Authentication, contact the VUMC IT/NTT Help Desk at 615-343-HELP/3-4357 to start the Password Reset (reauthentication) Process.

You will receive a temporary password that will be valid for three days.

Use the temporary password to login to MyMFA and enroll in Multi-Factor Authentication. [Enroll in MFA.](#)

After enrolling in MFA, follow the steps from slide #8 and go through regular change password process. [Go to Slide #8.](#)