Secure Authentication (SecureAuth)
Frequently Asked Questions

What is Secure Authentication (SecureAuth)
Secure Authentication (Or SecureAuth) is Baylor Scott & White Health's two-factor authentication technology to prevent unauthorized access and protect your personal information, as well as that of our patients. Instead of prompting you to just enter your username and password (one-factor authentication), two- factor authentication adds extra steps to the login (adding a pin, answering knowledge questions) to ensure the person logging into the system is you.

When will I be prompted for two-factor authentication?
Logging in from the BSWH network, or from the same browser and device (whether pc, mobile phone, tablet or laptop) combination that you've used previously, will typically not require additional, manual authentication. Logging in from outside the BSWH network, or from a different browser and device combination than you're used recently, may require additional, manual authentication.

Logging in from a "public computer" (selecting a different option than "private computer" on the initial login screen) or changing your password will always trigger a request for additional, manual authentication.

Do I log in multiple times to access different applications that are all protected by Secure Authentication?
Using multiple browsers to access different applications will require a login for each browser.
In most cases, logging in once to Secure Authentication will facilitate access to ServiceNow and other business-oriented applications.

Accessing applications that contain sensitive information, such as the self-service password reset tool, myHR and myBaylorEMR, will always require a specific login to that application.

What browsers are compatible with Secure Authentication?
Secure Authentication supports the latest versions of Google Chrome, Internet Explorer, Mozilla Firefox and Safari. Please note each application protected by Secure Authentication may have its own browser requirements.

What BSWH applications are protected by Secure Authentication?

Central Texas:
MyHR (PeopleSoft)
Oracle Cloud Compensation
ProofPoint
MyPassword.sw.org self-service password reset site
ServiceNow service desk application
Thrive for Wellness site
United Way site

North Texas
Baylor Learning Network
CVIS Lumedx
Employee Giving
G9MD
HR WorkWays
Kaufman Hall
Leadership Journey Portal
myBaylorEMR
Office 365
Recondo
Self-service password reset site
ServiceNow service desk application
Thrive for Wellness site
United Way site

Additional applications targeted for FY16-FY17:

AccessONE	EpicCare Link
Citrix/Netscaler	Meditract

How do I register for Secure Authentication?

Make sure you are you logged into the Baylor Scott & White Health network at a facility or via VPN (e.g. AP-Black, AP-Access, WIFON).

Click on the appropriate link for Secure Authentication registration in your division:

- Central Texas: https://saml.sw.org/registration/
- North Texas: https://saml.baylorhealth.com/registration

You will be prompted to provide your mobile number to activate self-service password reset options, as well as select three knowledge-based questions that will be used to confirm your identity when logging in outside the BSWH Network.

Why do I need to provide a mobile number?

A mobile number is needed to access the self-service password reset option. It will not be published or used in SecureAuth for anything other than this function.

How do I update my Secure Authentication registration details (e.g. mobile phone number, knowledge-based questions)?

Make sure you are you logged into the Baylor Scott & White Health network at a facility or via VPN (e.g. AP-Black, AP-Access, WIFON).

Click on the appropriate Secure Authentication link for your division:

- Central Texas: https://saml.sw.org/registration/
- North Texas: https://saml.baylorhealth.com/registration

Once you have logged in, Secure Authentication will display your current options and you can make edits to the registration information.

Secure Authentication is displaying an incorrect or out-of-date phone number - how can get it updated?

Office numbers for physicians are updated by Medical Staff Services in North Texas and by submitting changes to the Physician Directory Exchange Form in Central Texas. Office numbers for other clinical and corporate staff may be updated by contacting the Service Center.

If I am registered for Secure Authentication, does this mean I automatically have access to all the applications it protects?

No, application access is granted on an application-by-application basis, and is typically requested through AccessOne, MyID or by contacting the Service Desk. Some applications, such as myBaylorEMR, have a special link on their login page that can be used to request access to that application.

I have already registered for Secure Authentication. Why is the system prompting me to re-register? What happened to the knowledge-based questions I provided when I first registered?

For security reasons, Secure Authentication will prompt you to re-register every six months, usually during the login process for one of the applications you are attempting to access. Registration should take less than a minute and gives you the opportunity to update your mobile number (needed for self-service password resets) as well as select knowledge-based questions that are easiest for you to remember.

Previously, users needed two Secure Authentication registrations: one for Central Texas and one for North Texas. As this process is streamlined to a single registration, you may be prompted to update your knowledge-based questions.

How does Caps Lock affect my Secure Authentication login?

Passwords are case-sensitive. The password field will provide an on-screen notification if Caps Lock is enabled on your device. Caps Lock should not be used during password entry. In contrast, the User ID field is not case-sensitive and will not provide an on-screen notification if Caps Lock is enabled.

What happens if I enter the wrong password?

If you enter an incorrect password, Secure Authentication will clear the password field and allow you to try again.

If you enter an incorrect password more than 12 times, your account will be locked and you will need to click on the appropriate Secure Authentication link for your division to unlock your account and reset your password:

- Central Texas: https://saml.sw.org/pwd-reset/
- North Texas: https://saml.baylorhealth.com/pwd-reset/

What if I don't remember my password?

If you provided a mobile phone number when you registered with Secure Authentication, you can access our self-service tool to reset your password or unlock your account, 24/7.

If you did not provide a mobile number when you registered with Secure Authentication, you can update your registration details to provide a mobile number, or simply contact the Service Center for assistance in resetting your password or unlocking your account.

Why won't Secure Authentication accept my new password?

The password may not have been "strong" enough. BSWH requires the following for password configurations:

- Password must not contain your username.
- Password must differ from previous 12 passwords.
- Password length must be greater than 8 characters.
- Must contain at least 3 of the following:
- 1 digits (0-9).
- 1 symbols (!, @, #, $, %, *, etc.).
- 1 uppercase English letters (A-Z).
- 1 lowercase English letters (a-z).

I entered the correct User ID and password for Secure Authentication, but still received an invalid login or denied access message.

Please confirm with your management team or the Service Center that your access to that individual application is valid and has not expired.

Application access is granted on an application-by-application basis, and is typically requested through AccessOne, myID or ServiceNow.

When I log out of an application protected by SecureAuth (or the application times out), I can't log back in from the page that is displayed after logout and/or timeout. How can I log back in?

Most applications display a logout page from Secure Authentication. Clicking the "restart login" link should return you to the appropriate login page.

Some legacy applications continue to display a default logout (or timeout) page that is not integrated with Secure Authentication. We are working to clean up these pages to provide a consistent experience for our Secure Authentication users.

If you encounter one of these legacy logout (or timeout) pages, please close your browser and use the primary link for that application to log back in.