Sentara® Health Plans

User Guide
Microsoft Authenticator Installation and Secure Log in Approval Process

Table of Contents

Purpose

Sentara Health Plans now uses **Microsoft Authenticator** to confirm your identity after you enter your username and password on a secure portal. This extra step is called **multi-factor authentication (MFA)** and helps protect your account by ensuring that only you can approve access and requires all users—internal and external—to sign in using a **standardized username format** so your account can be identified correctly.

Guide Set up

This guide is divided into **two sections** to help you understand **how to set up** Microsoft Authenticator and **how to use it each time you sign in**.

Section 1: Initial Set-Up

Covers the **one-time steps** required to enroll your account in multi-factor authentication (MFA).

You can set up the MFA approval request to be sent to you via the following options:

1. The Microsoft Authenticator App via your mobile device
2. A phone call to a mobile device or land line
3. A text message to a mobile device
4. All of the options listed above

Section 2: Login Instructions

Covers how to log in and how to approve your sign-in request.

📌 MFA approval is required **every time you log in** to a secure Sentara website.

Section 1- Initial Set up of Microsoft Authenticator (One-time Setup)

This section explains **how to set up Microsoft Authenticator or an alternate verification method** (using your phone or a text message) for the first time. Complete the initial setup process from a **computer**, not your mobile phone.

Set up Options:

- Set up **Option 1** to use the **Microsoft Authenticator app** on your mobile device.
- Set up **Option 2** if you want to use **Phone Call or Text Message** and do **not** want to use the **Microsoft Authenticator app**.
- Set up **both Option 1 and Option 2** to have additional options (*Recommended).

⚠ IMPORTANT SET UP INSTRUCTIONS

Sentara uses Microsoft's security platform to protect access to its portals and requires all users—internal and external—to sign in using a **standardized username format** so your account can be identified correctly.

When signing in to **https://mysignins.microsoft.com** the first time to set up your sign-in notifications (as instructed in the steps below), you must enter your **username** in the following format: **username@sentara.com**.

- @sentara.com **does not mean** you have (or need) a Sentara email account
- It is used to **identify the correct secure system** that manages access and verification

---

Option 1 – Install and Set up Microsoft Authenticator

Getting Started: Your mobile device will be needed to scan a QR code and receive verification.

Step 1: Install Microsoft Authenticator on Your Phone

1. On your mobile device, open the **Apple App Store** or **Google Play Store**
2. Search for **Microsoft Authenticator**
3. Install the app before continuing

Step 2: From a Computer Sign In to the Microsoft Security Portal

1. Open a web browser on your **computer**
2. Go to: **https://mysignins.microsoft.com**
3. Sign in using your **Sentara username** (⚠️ **username@sentara.com**) and password

Step 3: Add a Sign-In Method

1. On the **Security info** page, select **+ Add sign-in method**
2. Choose **Authenticator app**

Step 4: Set Up Microsoft Authenticator App

Apple (iPhone)

1. Open Microsoft Authenticator
2. Tap **Scan a QR code**
3. **Scan the QR code** displayed on your computer screen

Android

1. Open Microsoft Authenticator
2. Tap **+ Add account**
3. Select **Work or School account**
4. Tap **Scan a QR code**
5. **Scan the QR code** on your computer screen

Step 5: Approve a Test Notification

1. A test push notification will be sent to your phone
2. Open Microsoft Authenticator on your device and tap **Approve**

Option 2 - Phone Call or Text Message Set up

Getting Started: Your phone will be needed to receive verification.

Step 1: From a Computer Sign In to the Microsoft Security Portal

1. Open a web browser on your **computer**
2. Go to: **https://mysignins.microsoft.com**
3. Sign in using your **Sentara username** (⚠️ **username@sentara.com**) and password

Step 2: Add a Sign-In Method

4. On the **Security info** page, select **+ Add sign-in method**

Select one of the following:

- **Text message** – receive a one-time code by SMS
- **Phone call** – receive an automated approval call

Step 3: Enter and Verify Your Phone Number

5. Enter your **mobile or office phone number**.
6. Complete the verification:
    - For text: enter the code sent to your phone.
    - For phone call: answer the call and follow the instructions.

ACTION REQUIRED

After completing your initial MFA setup, go back to the website you were trying to access and log in again. The system will not take you back automatically.

Section 2 – Logging in - Approving Your Sign-in Request

This section explains how to approve your sign-in request after entering your username and password. 📌 MFA approval is required **every time you log in** to a secure Sentara website.

- Follow **Option 1** if you set up push notification on your **Mobile Device**
- Follow **Option 2** if you set up notification via **Text Message**
- Follow **Option 3** if you set up notification via **Phone call**

Option 1: Mobile Device

Approving Sign-In Using a Mobile Device Push Notification

1. Navigate to your desired secure website
2. Enter your **username** and **password** on the website.
3. A Sentara security prompt will display with a Microsoft Authenticator **two-digit number**.

How to Approve

1. Open the **Microsoft Authenticator** app on your mobile device.
2. When prompted, you will see a message such as **"Approve sign-in?"**
3. Enter the two-digit number into the app.
4. Tap **Approve**

✅ Once approved, you will automatically be signed in.

Option 2: Text Message

Approving Sign-In Using a Text Message (SMS)

Text message approval sends a one-time code to your mobile phone.

1. Enter your **username** and **password**.
2. When the Security Prompt displays, select "**Use a different verification option**"
3. When asked "How do you want us to verify your account? Select **Text me at +x xxxxx**
4. You will receive a **text message** containing a **6-digit verification code**.
5. Enter the code on the website when prompted.

✅ Once the correct code is entered, your sign-in will be approved.

Option 3: Phone Call

Approving Sign-In Using a Phone Call

This option is helpful if you do not have access to the app or texting.

1. Enter your **username** and **password**.
2. When the Security Prompt displays, select "**Use a different verification option"**
3. When asked "How do you want us to verify your account? **Select Call me at +x xxxxx**
4. You will receive an **automated phone call**.
5. Follow the voice instructions (for example, press **#** or a number on your phone keypad) to approve the sign-in.

✅ After confirming, you will be signed in.

Tips for Successful Authentication

- Keep your mobile device **nearby** when signing in.
- If you do not receive a push notification, **open the Microsoft Authenticator app manually**.
- Ensure your phone has **cell service or internet access**.
- Contact support if you lose access to your phone or change numbers.
- Set up more than one verification method (for example, Authenticator plus SMS) in case you lose access to your device.
- Keep your phone number up to date in your Security info settings
- Never approve a sign-in request you did not initiate
- If prompted for number matching, carefully enter the number shown on your computer

---

Enrollment & Setup Support

If you are having trouble enrolling or setting up multi-factor authentication:

📞Microsoft Authenticator Support

- 757-857-8190 or
- 855-306-2252 (Option 6)