Welcome to Cardinal Health!

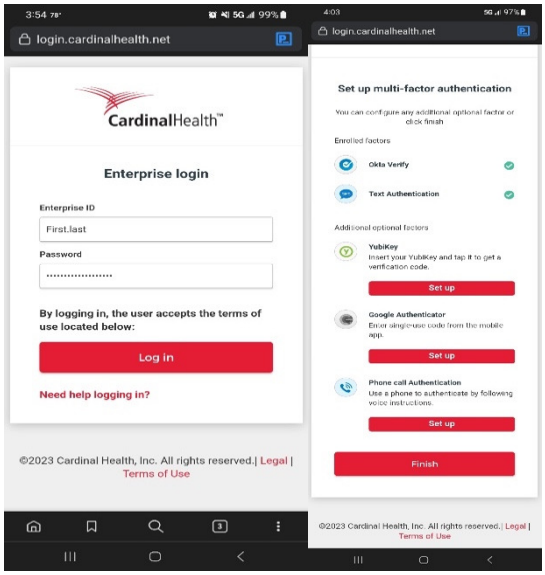
New Hire Set up video	EIT Service Center	Docking Monitor Set up	Get IT Help
PW: Welcome2CAH	866.300.4357 (HELP)		https://cardinal.service-now.com/gith

Computer Equipment Policy: The purpose of the policy outlines rules related to your company issued device.

- The computer equipment should not be physically modified in any capacity. This includes the removal of asset tags or applying stickers or skins to the device.
- Do not expose the computer equipment to liquid or moisture of any kind. If a spill does occur to your laptop, shut down the laptop immediately, unplug from any power and attempt to dry the device off. Immediately reach out to EIT Service Center or local IT Support for assistance.
- We do not recommend separating yourself from your laptop at any time when traveling. Do not store your laptop in your car, even in your trunk. If you place it in an overhead bin or under a seat, remember to grab it. Any lost or stolen devices need to be reported to the Security Operations and Information Center (SOIC) immediately: 614.757.3333.
- Global Technology and Business Services does not supply headsets. If you want to order a headset, please contact your department's administrative assistant.
- All computer equipment being replaced due to tech refresh, breakage, or separation needs to be returned within 14 days. Computing devices not returned within this timeframe will result in a charge against the business's cost center.

First day password

Do NOT login until your start date, unless directed otherwise from your hiring manager. A password was generated for you as part of the onboarding process. We recommend that you contact your manager to obtain your first-day password. If you have not received it, please contact the EIT Service Center to request a password reset.



Okta setup

Multi-factor authentication is a mandatory security measure for all employees, it adds an extra layer of security and prevents unauthorized access to sensitive company information and resources.

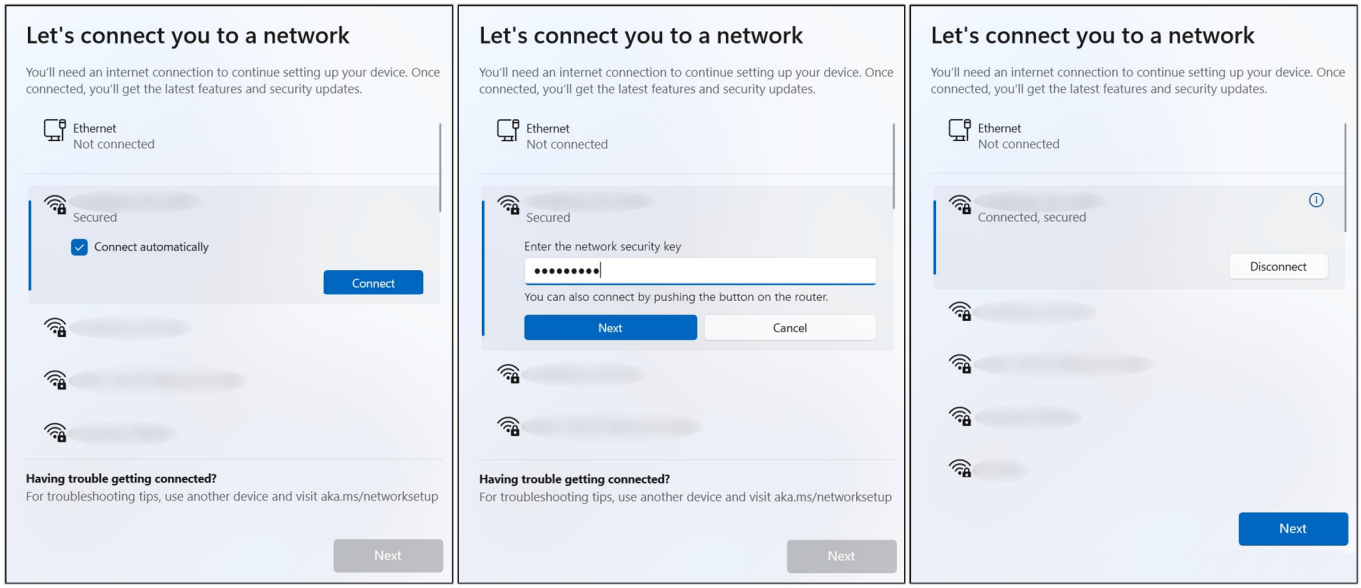
- Scan the barcode on the right or go to **login.cardinalhealth.net** on your phone.
- Log into Okta with your Enterprise ID.
- Setup the multi-factor authentication.
- Once the setup is completed: Click Finish.

login.cardinalhealth.net

Laptop setup

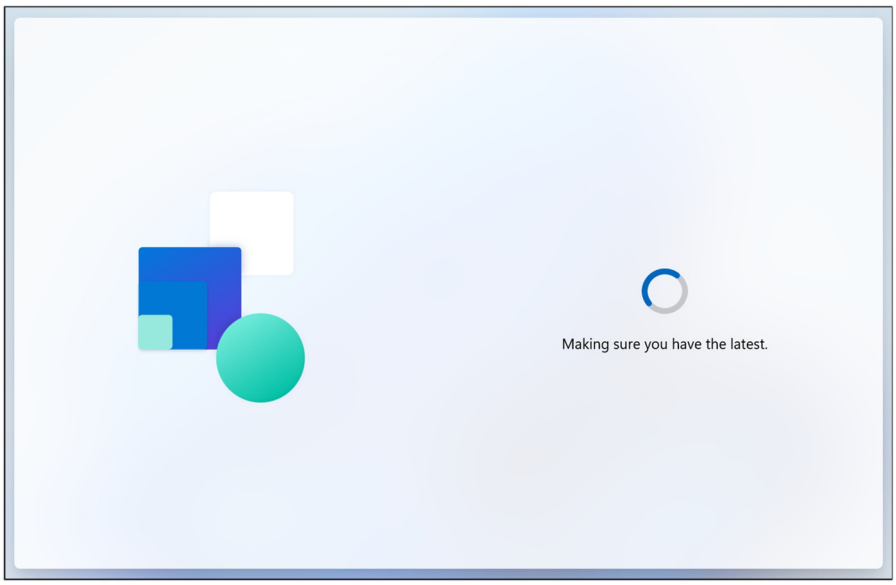
After setting up your Okta multi-factor authentication, power your computer on by **connecting the power adapter** and **pressing the power button**. **Do not turn off** or **restart** your computer during the setup process.

1. **Let's start with region. Is this correct?** Select your country or region from the list and select **Yes.**
2. **Is this the right keyboard layout?** Select the desired keyboard layout and select **Yes.**
3. **Do you want to add a second keyboard layout?** Select **Skip.**
4. **Let's connect you to the network.** Select an available network and connect to the Internet. If you are attempting the setup at a Cardinal Health facility, select the Guest wireless network.

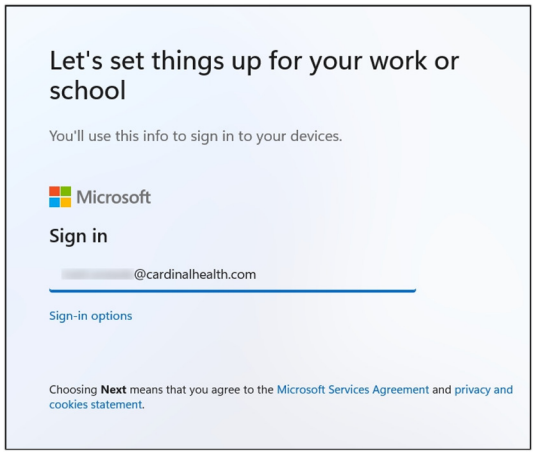


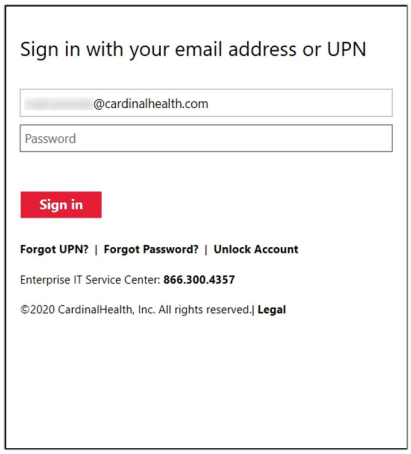
Connecting to a wireless network.

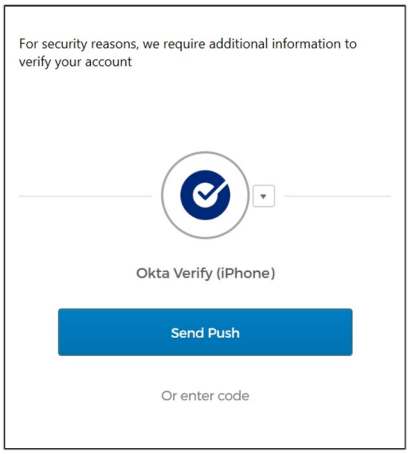
5. You will see the screen below once you connect to the internet. Please give it a few moments to update.



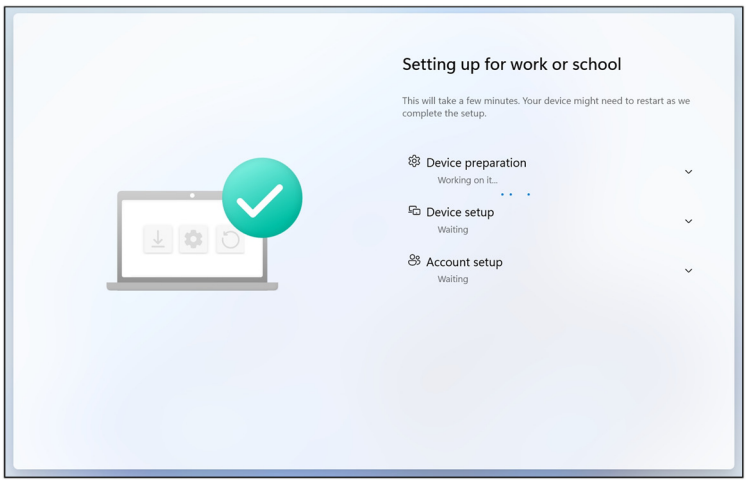
6. **Sign in with Microsoft.** Enter your **Cardinal Health email address** and select **Next**.
7. Enter in your **Cardinal Health email address** and **password.**
8. Authenticate your enterprise logon with **Okta.**



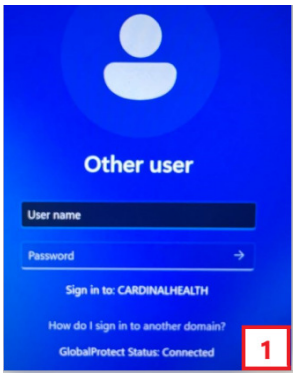


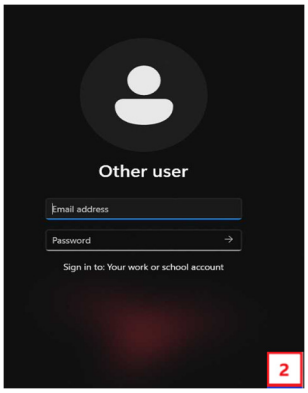


9. You will see the screen below and the device will reboot several times. This is entirely normal and may take a couple of hours to complete. **Do not power the laptop down manually unless instructed to by the Service Center.**

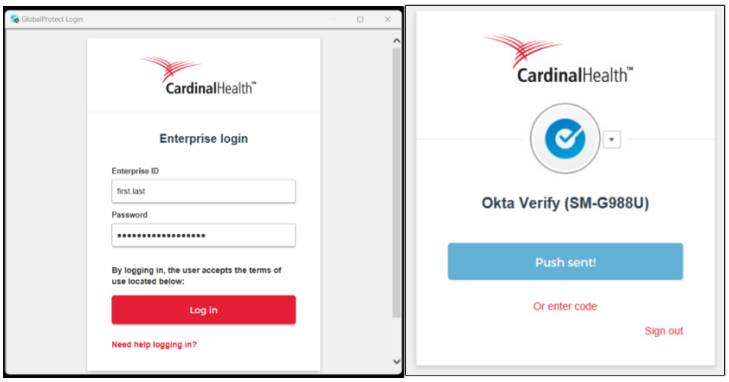


10. Once this process has completed, log into your computer by pressing CTRL+ALT+DELETE. Your login screen will appear in one of these formats. If you see option #1 login with your Cardinal Health Enterprise ID (first.last) and password. If you see option #2 login with your Cardinal Health eMail address (@CardinalHealth.com) and password.

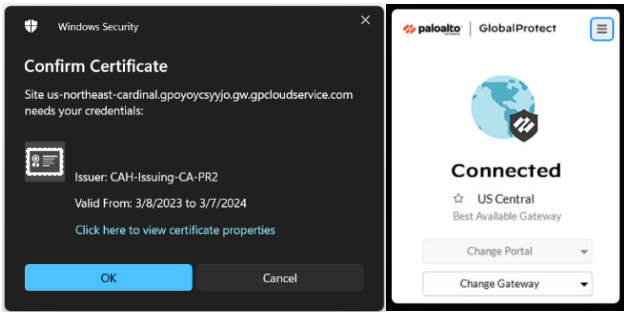




11. Once your successfully logged in, a **GlobalProtect** login screen will pop up and require login. Enter in your **enterprise credentials** and **authenticate through Okta Verify.** GlobalProtect is the primary virtual private network client here at Cardinal Health. Global Protect is necessary to establish a secure and encrypted connection to our internal network.



12. You might be prompted to confirm your certificate. **Click Ok** and confirm your connectivity by checking your **GlobalProtect client.**



13. **Microsoft Company Portal is your primary source for installing applications.** To access Company Portal, go to the desktop and select: **Company Portal.** You can also search **Company Portal** in the start menu, and it should be the top result. If an application isn't available in the Company Portal, submit a **Software License Request** via **Get IT Help** to acquire access to the software you need.