Network Access Control (NAC) Project

Traci Farrell on February 8, 2019
Overview

Network access control (NAC) will provide IT with visibility into the tens of thousands of
devices on our network, will help users know whether or not their devices meet UCSF security standards, and, eventually, will prevent non-compliant devices from connecting to the UCSF network.

Ensuring UCSF computers meet the minimum security standards is critical to keeping a sprawling enterprise like UCSF secure. Certain types of malware have the ability to spread to other computers on the same network. Our NAC project aims to decrease the likelihood of infected or vulnerable computers joining our network.

What to expect

We will begin operating in monitoring mode only, continuing to allow all devices to join the UCSF network. Eventually, devices that pose a threat will be isolated to prevent them from stealing data or interfering with UCSF clinical, research, and education missions.

While in monitoring mode, users of IT-managed computers shouldn’t notice anything. Lightweight agent software will run in the background. Users of self-managed devices will have to install the agent. NAC agents do not track your activity or read your email?they collect information like encryption status, the age of virus definitions, etc. Detailed information about the client will be available.

Timeline

Early 2018: NAC project planning, infrastructure planning, and design commences.

Summer 2018: Installation of NAC agents begin.

Winter 2019: NAC agent requirement begins to be enforced.

More information

Please visit https://nac.ucsf.edu/ [1] (accessible from the UCSF network) or read the Security 2.0 FAQ [2] for more information (MyAccess login required).

GET IT HELP. Contact the Service Desk online, or phone 415.514.4100