Implementing the Administrative Rights Standard

Carlos Evia, Corey Earles, Scott Shetrone

CLAHS IT snapshot

- About 1,246 computers
- 678 Mac
- 568 Windows
- 11 departments and 3 schools
- 8 IT support specialists
- Lots of changes coming*

LIBERAL ARTS AND HUMAN SCIENCES
VIRGINIA TECH™

CLAHS in 2019

- Faculty and staff woke up to an audit report
- Numerous IT findings showed that CLAHS was not in compliance :-(
- Deans came and went
- Centralized ITSU disbanded in 2016
- Scary: No big picture focus.

LIBERAL ARTS AND HUMAN SCIENCES
VIRGINIA TECH™

Scary sentence

We will **remove** admin accounts from **all** CLAHS computers by {import java.util.Date;}

LIBERAL ARTS AND HUMAN SCIENCES
VIRGINIA TECH™

We needed a taskforce

- Develop a taskforce (March 2021) to address this (and *many* other) recommendations from the audit
- Created the position of CLAHS CTO
- Scheduled twice weekly meetings with BAMS, CLAHS, FASTR, and ITEE.

LIBERAL ARTS AND HUMAN SCIENCES
VIRGINIA TECH™

We needed BigFix

- Address recommendations via BigFix, JAMF, Group Policy, remote sessions, and in person support
- Develop procedures for user installation of BigFix
    - Easy to use, easy to understand, and easy to find (DQTI).

LIBERAL ARTS AND HUMAN SCIENCES
VIRGINIA TECH™

We needed the ITSO

- Joyce Landreth and Dawn Zimmer were essential for connecting the CLAHS taskforce with the ITSO
- ITSO and CIO collaborated on a standard for obtaining (and revoking) admin rights
- CLAHS started a pilot in August 2021
- Whole college adopted the standard in October 2021.

LIBERAL ARTS AND HUMAN SCIENCES
VIRGINIA TECH™

We need a more humane verb

Adjusting accounts worked better than **removing** admin access

LIBERAL ARTS AND HUMAN SCIENCES
VIRGINIA TECH™

Implementation and workarounds

- ***Important point**** This workaround was unique to the CLAHS environment but allowed users to perform necessary admin functions while the full standard was developed.
- Created and implemented plan for IT support staff to supply temporary admin access if necessary.
    - Approach:
        - 1. Create new local admin account
        - 2. Adjust users account to standard status
        - 3. If password needed by user, it will be reset within 24 hours

LIBERAL ARTS AND HUMAN SCIENCES
VIRGINIA TECH™

Current situation and problem(s)

- Number of CLAHS users that have requested a secondary admin account: **48**
- Actual users with problems related to not having an admin account: **2** (users of Microsoft IME for Asian languages)

LIBERAL ARTS AND HUMAN SCIENCES
VIRGINIA TECH™

Overview

CALS Endpoints:

Linux	46
macOS	256
Windows	1949

IT Team:

6 Help Desk, CALS support
5 Area IT, Extension support
3 Departmental IT

About 1400 full time employees from:

7 academic departments and 2 schools
108 County Extension Offices
11 Research Stations
6 4-H Centers

Scott Shetrone | scott@vt.edu

COLLEGE OF AGRICULTURE AND LIFE SCIENCES VIRGINIA TECH

Communications/Timeline

Aug-Dec 2021 - Researching options and working with ITSO & ITPALS on Make Me Admin approval. Writing and testing scripts.

Jan 10 - Admin privileges removed from pilot dept

Feb 1 - Presentation at our yearly in-service, and weekly announcement emails began

Feb - Attended 5 department faculty meeting to field questions on the change

March 1 - Admin privileges were removed from all endpoints

ServiceNow Knowledge Base article:
KB0012671
CALS - How to temporarily elevate your account to Administrator

COLLEGE OF
AGRICULTURE AND
LIFE SCIENCES
VIRGINIA TECH

It's day 31... and it's ok

So far, 63 people have requested admin privileges
~4%

An increase in software installation requests
Tickets: average about 4 per day

COLLEGE OF
AGRICULTURE AND
LIFE SCIENCES
VIRGINIA TECH

Implementation

Windows: Make Me Admin application
by Patrick Seymour (https://github.com/pseymour/MakeMeAdmin)

macOS: Make Me Admin script based on
MakeMeAnAdmin script: https://github.com/jamf/MakeMeAnAdmin
modified with assistance from Matt Poor

Linux: Not yet implemented

Use is limited by user account and computer

COLLEGE OF
AGRICULTURE AND
LIFE SCIENCES
VIRGINIA TECH

Implementation

BigFix did the heavy lifting:

- Powershell and shell scripts removed all users from admin groups except for a set of our allowed users/groups for both Windows and macOS.
- Deploys Make Me Admin to Windows.
- Tasks to uninstall and adjust its settings (allowed user list and timeout).
- Scripts written to add/remove accounts to admin groups for maintenance and edge cases.

Jamf is required on macOS to implement.
The Make Me Admin script is run from the self service tool.

COLLEGE OF
AGRICULTURE AND
LIFE SCIENCES
VIRGINIA TECH

Edge Cases

macOS – the system must be connected to the network to be able to run the script from Jamf's Self Service.

Windows – Make Me Admin only allows the currently logged on user to elevate. It is an issue for systems that need to use a shared account.

Lessons Learned/To-do

Make sure email groups contain all the people to be notified.

We missed some split appointment employees and some graduate students.

Some legacy systems setup with local Windows accounts were unable to login after implementation.

We implemented before this year's computer refreshes (PDN, ACR, CALS), so we expect an uptick in requests once new systems are delivered and previous applications are no longer installed.

To-do: Auditing through Central Logging service

To-do: Implementing controls for Linux

COLLEGE OF AGRICULTURE AND LIFE SCIENCES VIRGINIA TECH

Questions?

Carlos Evia | cevia@vt.edu | 540-231-2373
Scott Shetrone | scott@vt.edu | 540-231-7841
Corey Earles | cearles@vt.edu | 540-231-1917

COLLEGE OF AGRICULTURE AND LIFE SCIENCES VIRGINIA TECH

LIBERAL ARTS AND HUMAN SCIENCES VIRGINIA TECH