DH1 Enrollment Instructions for Managed-Shared Devices

For use by IT Support Groups Only

This document outlines the requirements and process to install the DH1 Wi-Fi Profile on macOS devices managed in Duke Health's JAMF Pro instance (casper.trinity.duke.edu).

There is a separate process for macOS devices that are user-managed and not enrolled in JAMF Pro.

Summary

The Configuration Profile that installs the DH1 Wi-Fi configuration is managed at the root of JAMF Pro. The Configuration Profile can be scoped to JAMF Pro managed computers in one of three ways:

1. All macOS Computers in a JAMF Pro Site
2. A specific Computer Smart Group managed by each IT group in their own JAMF Pro Site.
3. A specific Computer Static Group managed by each IT group in their own JAMF Pro Site.

User vs. Machine Authentication

- User Authentication
  - Majority of use cases at Duke Health.
  - Authentication via an SSL Certificate issued to the valid Duke User assigned to the device in JAMF Pro.
  - Domain Bind to DHE not required.

- Machine Authentication
  - Specific use cases only, where User Authentication is not appropriate.
  - Authentication via an SSL Certificate issued to a computer object in the DHE Domain. The computer must have a specific service account assigned to it in JAMF Pro to designate the computer for Machine Authentication.
  - Domain Bind to DHE is required.

DH1 Enrollment Instructions

Compliance Checking

Prior to installation of the DH1 Wi-Fi Profile, the device must satisfy the Duke Health Network Access Control (NAC) requirements. These requirements are:

- A supported version of macOS – typically this is the current version plus the previous two versions.
- CrowdStrike Falcon Sensor installed and running.
- FortiNET NAC Agent installed and running.

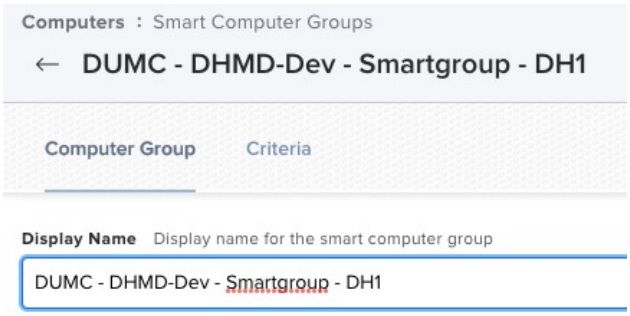
An Extension Attribute has been created in JAMF Pro to perform the NAC Assessment. The Extension Attribute is titled “DH NAC Compliance” and will return a “Pass” or “Fail” depending on the compliance status of the computer. If the computer fails the compliance check, the Extension Attribute will indicate which requirements were not met.

Installing the DH1 Wireless Profile

1 **Decide on a method to scope the DH1 Configuration Profile to the devices:**

- **a. Entire JAMF Pro Site**
  - **i. Easiest to setup and manage**
  - **ii. Impossible to add individual exceptions**
- **b. Computer Smart Group**
  - **i. Preferable if you need to manage exceptions**
- **c. Computer Static Group**
  - **i. Least preferable method but provides the most control over which computers will receive the DH1 Wi-Fi profile.**

2 **Create the Smart or Static Group as necessary and provide your JAMF Pro site name or the group name to one of the project engineers. The name of the smart group should follow established naming conventions in JAMF Pro and reflect its purpose for installing the DH1 Wi-Fi profile. For example:**



DukeHealth

DH1 Enrollment Instructions

3 **Verify NAC compliance of the computers via the DH NAC Compliance Extension Attribute.**

a. **Example DH NAC Compliance Pass:**

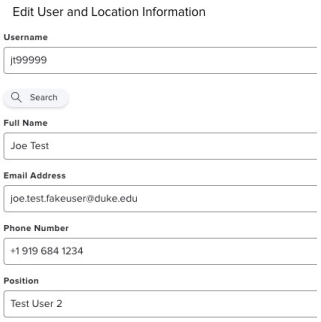
DH NAC Compliance: Pass

b. **Example DH NAC Compliance Fail due to CrowdStrike Falcon not being installed:**

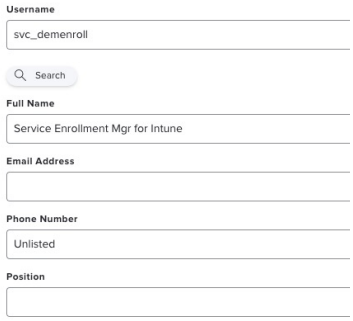
DH NAC Compliance: Fail:Falcon

4 **Verify a valid user has been assigned in the Computer Inventory in JAMF Pro.**

a. **User Authentication. The SSL Certificate will be issued to this user. This should be the primary user of the computer.**

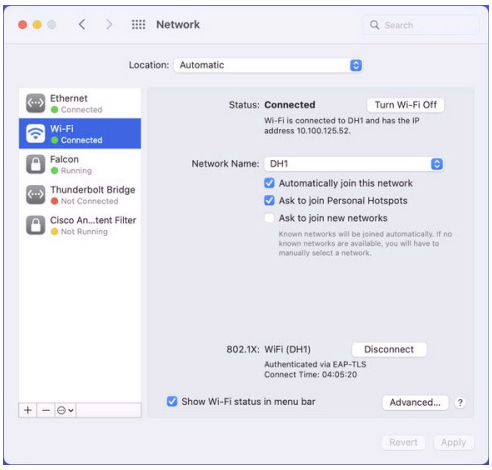


b. **Machine Authentication. Use the service account svc_demenroll or a preferred service account.**



Verify Installation of the DH1 Wi-Fi Profile

When the DH1 Wi-Fi Profile is installed, the 802.1X configuration will be visible in Network Settings on the computer. If the DH1 Wi-Fi network is in range of the computer, it will automatically attempt to connect.



DukeHealth