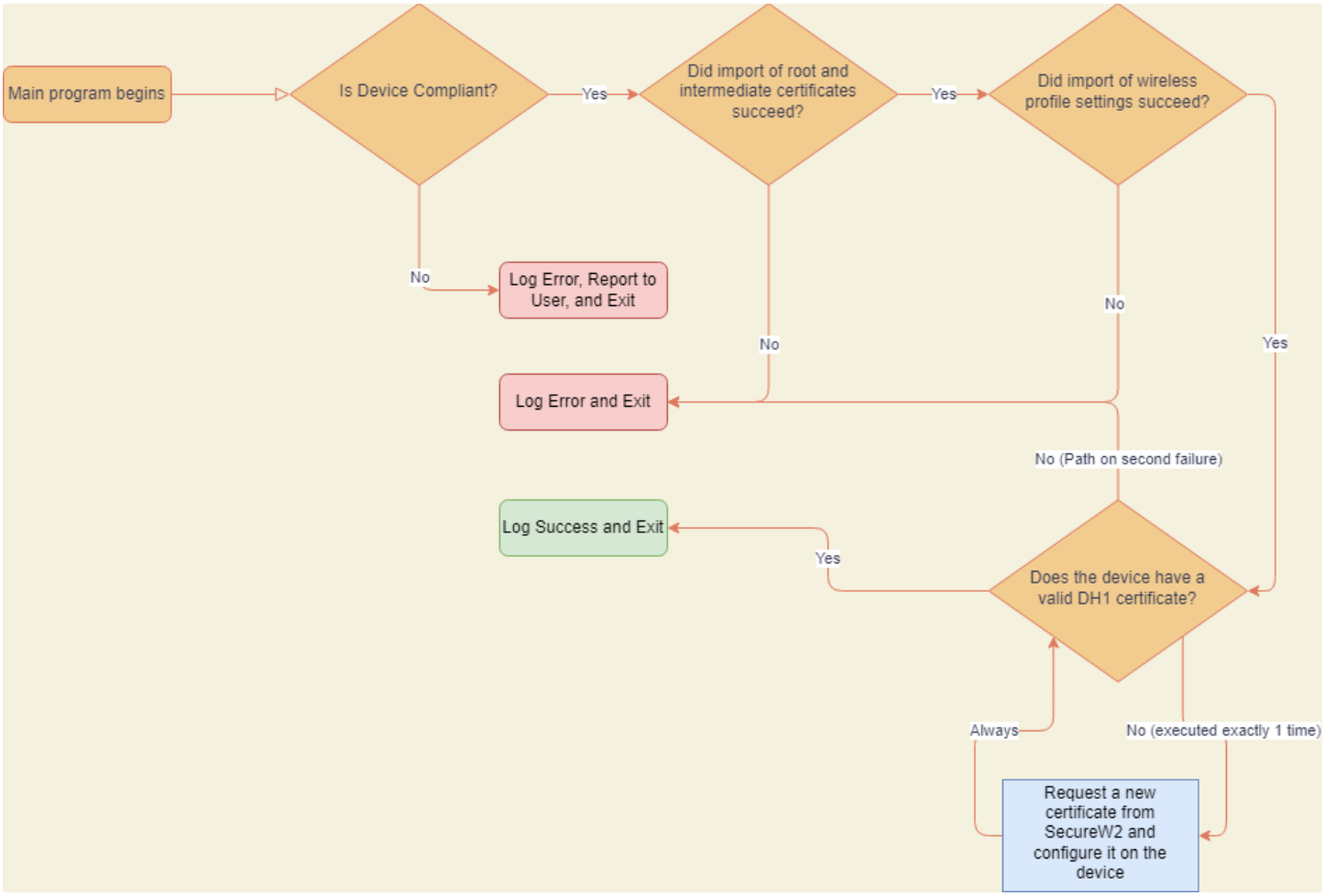
CONTENTS

SUMMARY

This document will outline the Duke Health developed solution that seamlessly configures wireless for managed devices/shared devices to leverage the new wireless project with no additional burden on the end-user while also working within the constraints of the existing capabilities.

The main driver for implementing this solution is that our current configuration, which consists of two Active Directory trees, cannot fully sync with Azure Active Directory. We have one Active Directory tree for Duke University (WIN) and one Active Directory tree for Duke Health (DHE), but only WIN fully synchronizes back to Azure Active Directory. Without one unified, on-prem Active Directory tree syncing back to Azure Active Directory with both user and device objects, we cannot auto-enroll devices in Intune for a seamless, zero-touch solution for managed devices/shared devices. If at some point in the future we consolidate domains, this solution would be retired in lieu of using the auto-enrollment option.

WORKFLOW DIAGRAM



PRODUCT LIFECYCLE

OVERVIEW

This solution was developed to be completely standalone and may be installed on Windows devices via an MSI package. Installing the software will import root and intermediate certificates into the device's certificate repository, configure two scheduled tasks, create a program directory located in C:\Program Files (x86)\Duke\DH1 Wireless, configure a DH1 Wireless network profile for all users on the device, and request/import a device certificate from SecureW2. You may optionally choose to enforce the root and intermediate certificates as well as the wireless profile via Group Policy. This can prove to be helpful especially if you need to manipulate the order of wireless networks.

Uninstalling the software removes everything except the certificates that have been imported, the wireless profile settings, and the logs in the installation directory.

INSTALLATION

This solution will be available as a Bigfix fixlet to be deployed as support personnel see fit and also as a standalone MSI that can be used with any other deployment mechanism. The manual, silent installation command is **msiexec /I DH1Wireless.msi /qn /norestart.** Keep in mind that you will need to specify the path to the DH1Wireless.msi file.

REMOVAL

The software can be removed via **Programs and Features** in the Windows control panel or via a silent removal command. The manual, silent uninstallation command is **msiexec/x DH1Wireless.msi /qn /norestart.** Keep in mind that you will need to specify the path to the DH1Wireless.msi file.

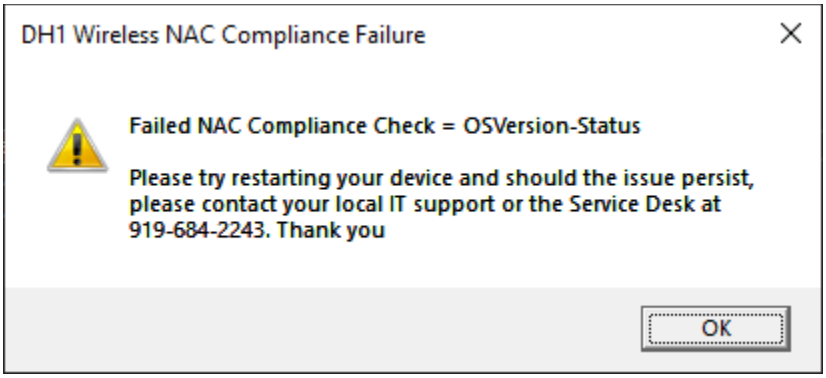
TROUBLESHOOTING

LOGS

Logging for the application can be located in C:\Program Files (x86)\Duke\DH1 Wireless\Logs.

COMPLIANCE CHECK FAILURE

At this time, only compliance check failures will be communicated to the user. The message will contain which check(s) failed and a message to contact support staff for assistance. An example message is below.



QUESTIONS

1) What happens if you have DH1 configured via group policy and/or via the program and the user enrolled the device in Intune which would configure a user-based certificate?
   A: The device will still connect to DH1.

2) After installing the DH1 wireless program, why won't the device connect to DH1?
   A: At this time, the only time we have seen a failure is when a device, which was previously configured for the Intune pilot, was not removed from Intune prior to installing the DH1Wireless program. The DH1 wireless profile settings configured on the device from Intune must not have been 100% correct for machine authentication. Removing the device from Intune and rebooting should configure the correct wireless profile on the device and should connect the device to DH1.

3) Will updating the wireless group policy in production affect existing clubs or other wireless networks?
   A: Our testing has demonstrated that we can configure the wireless policy to have both clubs and DH1, with DH1 being the preferred network. Until such time as the DH1 configuration has been applied to the device, the device will continue to connect to clubs as it does today. Once the DH1 program has been installed and the device configured properly, after a reboot or possibly waiting some time, the device will connect to DH1 going forward.

4) If the DH1 program is installed and everything is configured, what were to happen if the user deleted the DH1 profile beforebringing the device to a Duke site to connect?
   A: Since the program runs every 30 minutes to check for compliance, it would detect the missing DH1 wireless profile and add it back. Additionally, if you have chosen to enforce certificates and wireless settings via Group Policy, the user would not be able to delete the Organization managed wireless profile so nothing would happen.

5) The program logged failures saying that it can't reach SecureW2 to obtain a certificate. By the way, I keep ignoring this ZScaler authentication window and I can't get to any websites. What's wrong?
   A: The program requires an internet connection to complete the certificate request. We have tested with users both off site and on site and they have been successful both retrieving the certificate and connecting to DH1 once they arrive on campus. If the ZScaler prompt has popped up, all internet traffic is halted until you authenticate. Once authenticated and connected to any wireless network, the program will attempt to complete any uncompleted tasks at the next compliance interval check, which is currently every 30 minutes.