SID Mismatch Re-Enrollment Process

Goal

To automatically un-enroll and re-enroll and Windows 10 device in the case where the enrollment SID does not match the logged in user SID. Since we don't yet support multi-user, this results in only partial management of the device. Several things stop working such as App Sampling and Cert Sampling. Because App Sampling fails, this causes the SFD agent to not automatically upgrade itself on console upgrades. It will also prevent any user context profiles or apps from being deployed.

Change-Log

v2.3 - Jun 29, 2020

- Added disabling/re-enabling toast notifications for silent un-enrollment and re-enrollment process
- Renamed file to be WS1-ReEnroll.ps1

v2.3 - March 5, 2020

- Added in PSADT class for querying logged in active user
- Changed enrollment check logic to check for positive enrollment vs non-valid enrollment
- added pinging Workspace ONE server before running
- Some updates to logging text and bug fixes
- Changed parameter from UPN to Username

v2.1 - Mar 3, 2020

- Fixed issue with renaming old log files
- Added additional logging info when enrolling via HUB

v2 - Feb 28, 2020

- Added 5 min wait after oma-dm removal to ensure everything is removed properly
- Added logic to re-name hub logs after removal of hub

Files

1. Enrollment Batch file WS1-ReEnroll.bat, and WS1-ReEnroll.ps1 **https://github.com/vmware-samples/euc-samples/tree/master/Windows-Samples/Product%20Provisioning/Re-Enroll%20Workspace%20ONE%20-%20SID%20Mismatch**
2. Airwatch Agent (get correct version matching customer console or download latest from getwsone.com)

Pre-reqs:

- Has 4 required parameters. These are used for the silent enrollment command line:
    - Server
    - LGName (Org Group ID)
    - Username
    - Password
- A logged in user does have to be detected. If no logged in user is detected the script will exit.

Usage

- Note this does require 64bit powershell
    - 64bit - powershell -executionpolicy bypass -file .\WS1-ReEnroll.ps1 -server ws1uem.awmdm.com -lgname staging -username staging@staging.com -password 11111
    - 32bit - %WINDIR%\Sysnative\WindowsPowerShell\v1.0\powershell.exe -executionpolicy bypass -file .\WS1-ReEnroll.ps1 -server ws1uem.awmdm.com -lgname staging -username staging@staging.com -password 11111
- Logfile is saved: C:\ProgramData\Airwatch\UnifiedAgent\Logs\WS1-ReEnroll.log

Script Process:

1. Sets variables
2. Checks for elevation. If not run with elevation privileges it will exit.
3. Tests log path (function), if not found will create it
4. Gets current architecture. If 32bit: exits. If 64: continues.
5. Checks agent path (function Check-Agent-Path). Script expects AirwatchAgent.msi to be in same directory as script. If not found, will download from getwsone.com
6. Enrollment Check (function Enrollment-Check) - verifies if there is a valid MDM enrollment and returns UPN
    a. Get GUID here: HKLM:SOFTWARE\Microsoft\Provisioning\OMADM\Accounts*
    b. Checks other registry keys to ensure that there is a valid enrollment
        i. if Valid, returns the UPN email of enrolled user
        ii. if null or enrollment state is not valid, returns $false
7. Checks windows SID (function Check-SID)

Copyright © 2019 VMware. All rights reserved. Proprietary & Confidential

    a. Uses a C# class from PSADT to detect current logged in user.
    b. If valid, then compares logged in user SID with the enrollment SID. Does additional logic to ensure that the MDM SID its comparing is really one of ours (ProviderID = AirwatchMDM).
    c. If windows SID and Enrollment SID match, return $true, else return $false
8. If Enrollment-Check and Check-SID both return $true, then script knows there already is a healthy enrollment with correctly matching SIDs and exits.
9. if one or both are false,
    a. Disables toast notifications so the end user doesn't see a scary message about Work resources being removed from their PC
    b. Calls Uninstall-Hub function
        i. Uninstall-Hub searches for any installed Hub GUID and ADA(software distribution client) Guid and uninstalls them. This should also trigger MDM unenrollment, but in case it doesn't we call DeviceEnroller.exe to force a sync which then will trigger un-enrollment since Hub is missing
    c. Enroll-Hub function is called and does command line enrollment with values from the parameters passed to it as well as ASSIGNTOLOGGEDINUSER=Y parameter. It then waits 5 min for enrollment to complete and then does another Enrollment-Check.

Create a Product in WS1

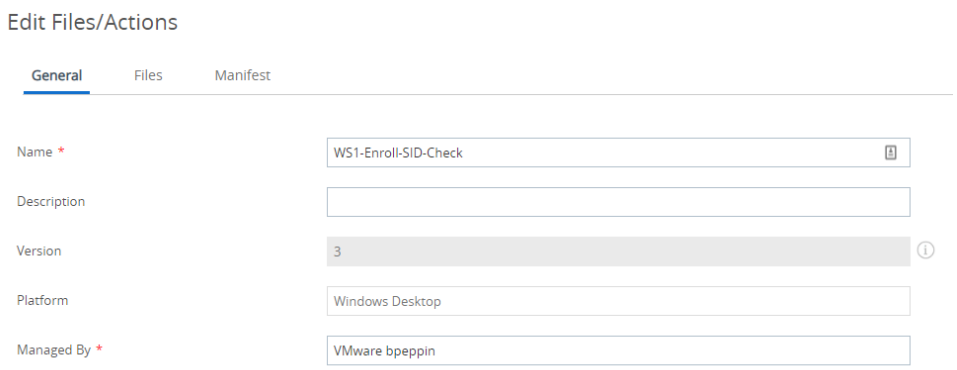
Prep:

1. Download the batch file above and update the content with your environment specific details. Example:

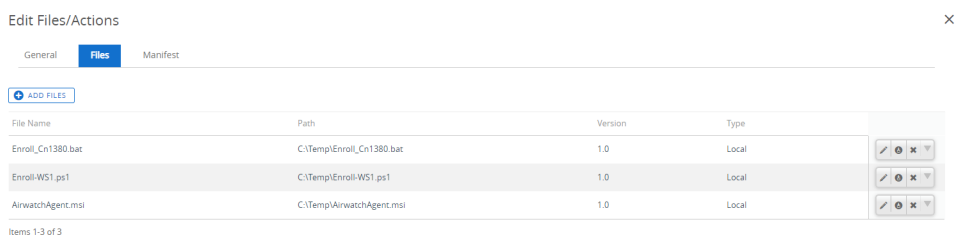
   cd %~dp0
   %WINDIR%\Sysnative\WindowsPowerShell\v1.0\powershell.exe -executionpolicy bypass -file .\WS1-ReEnroll.ps1 **-Server ds1380.awmdm.com -LGName bpeppin -Username username -Password N0tReal**
2. Download or get the correct version of Intelligent hub (Airwatch Agent.msi)
3. Download WS1-ReEnroll.ps1 file

Create Files/Actions

1. Go to Devices > Provisioning > Components > Files/Action
2. Click "Add Files/Actions"
3. General tab - fill out basic details



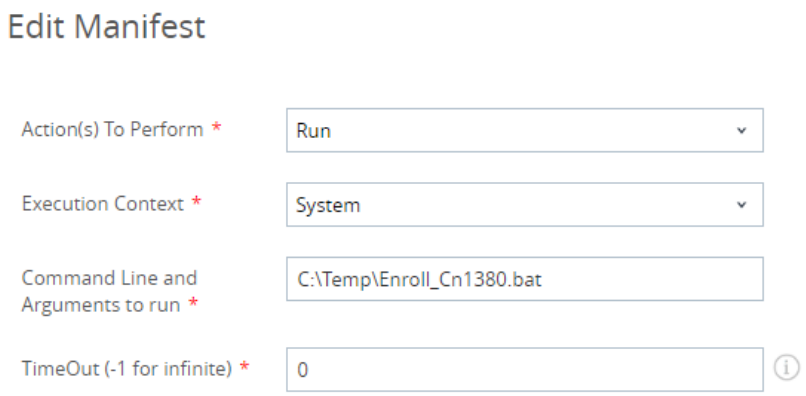
4. Files Tab. Upload the 3 files and specify target path (such a C:\temp)



5. Manifest.
    a. Click Add Action

Copyright © 2019 VMware. All rights reserved. Proprietary & Confidential

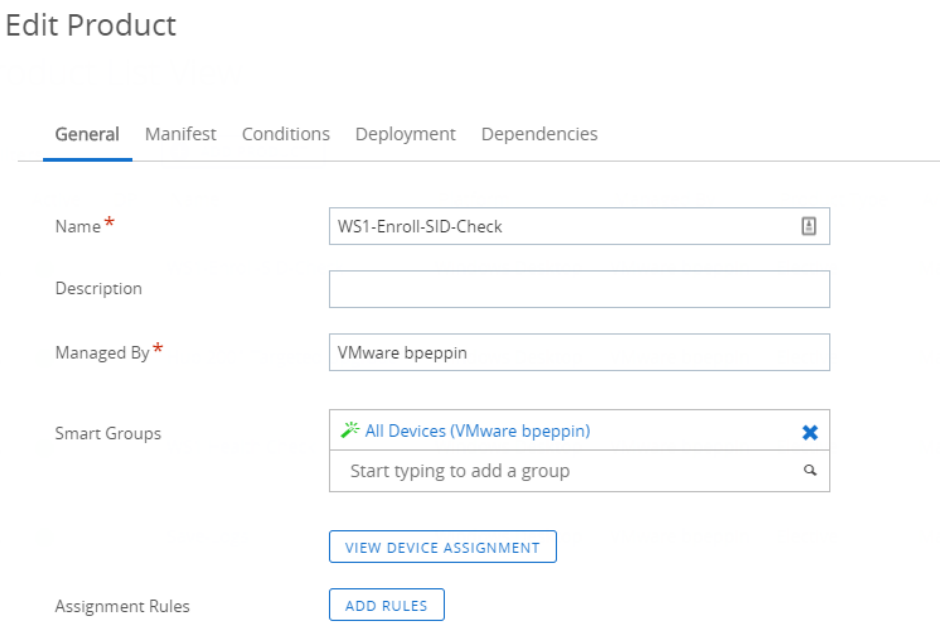
b. Run, System, Path to your batch file



6. Click Save

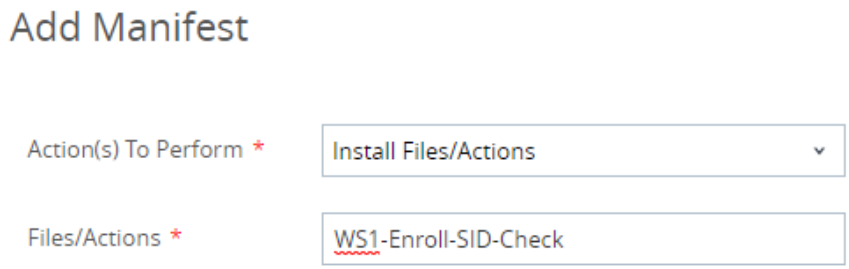
Create Product

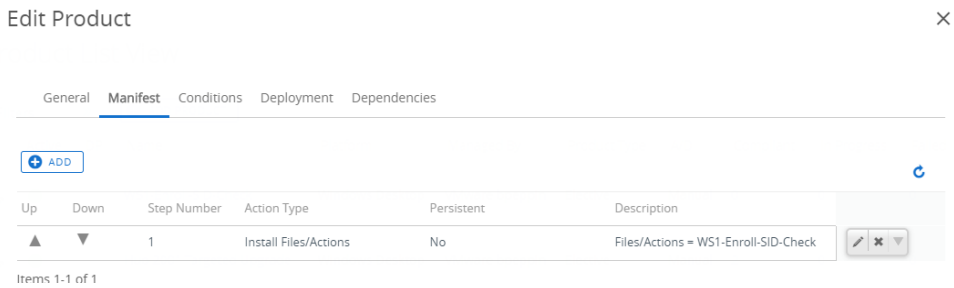
1. Go to Devices > Provisioning > Product List View and click "Add Product"
2. General Tab - fill out and assign smart group



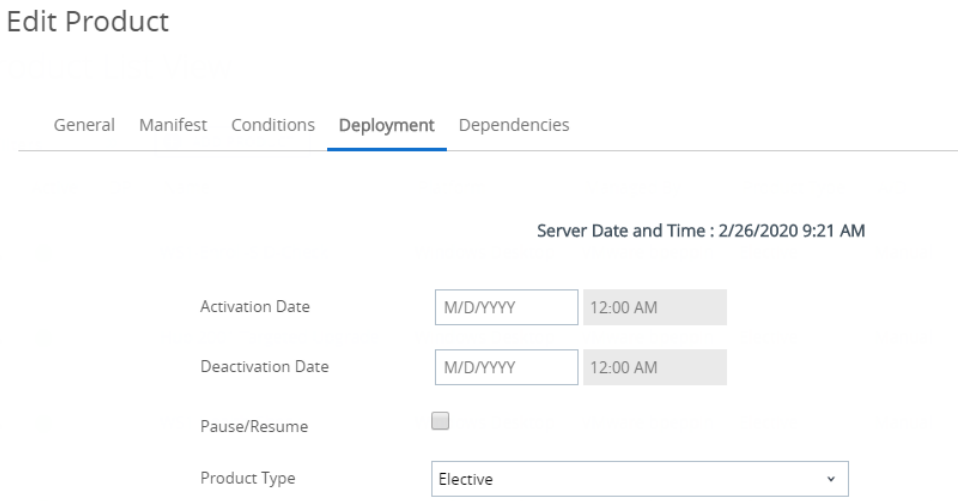
3. Manifest Tab. Click "Add" and select "Install Files/Action". Select the Files/Action item you just created.

Copyright © 2019 VMware. All rights reserved. Proprietary & Confidential





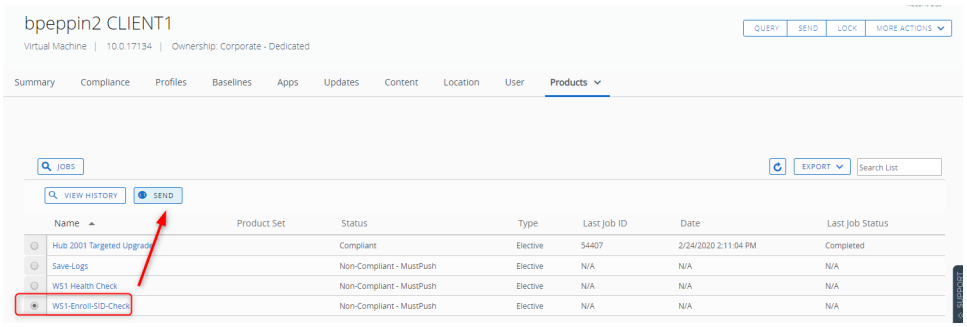
4. Conditions tab - leave default
5. Deployment Tab - change Product Type to "Elective". This will require you to manually push the product to devices ad-hoc.



6. Dependencies Tab - leave default
7. Click save and Activate the product.

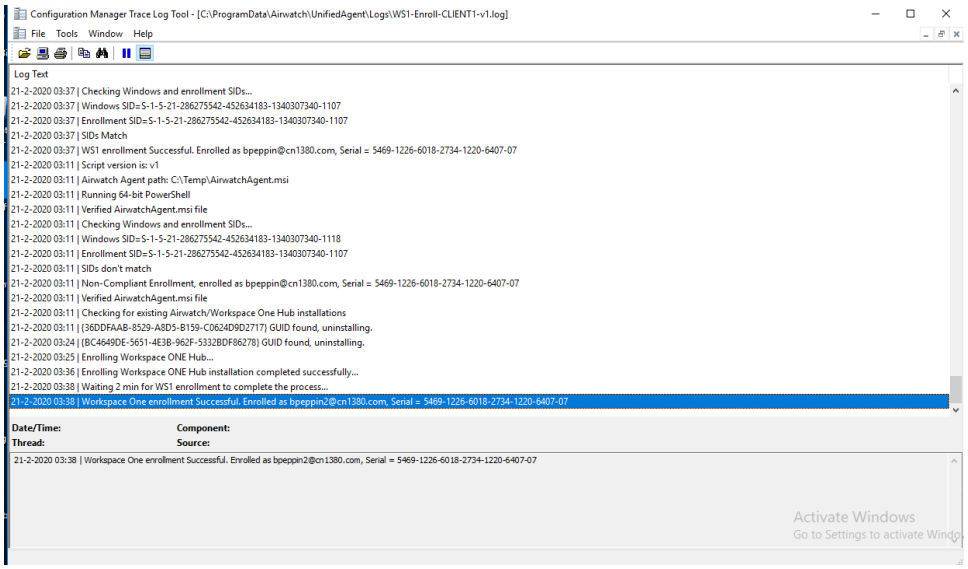
Deploy to Device

1. Go to a device and on device details page click on More > Products.
2. Select the product and click Send



Copyright © 2019 VMware. All rights reserved. Proprietary & Confidential

3. Use the refresh button to check status. Since you included the AiwatchAgent.msi this might take a little longer to run since downloading this file directly from DS servers is slow.
4. On client, check the log: "C:\ProgramData\Airwatch\UnifiedAgent\Logs\WS1-Enroll-[hostname]-v1.log". You can see the test machine I have here where I run it both from a matching SID and mis-matching SID domain accounts.



Checking for mis-matching SID using Sensors

Create Sensors

We can create 3 sensors to check the environment for mismatching SID to get an idea of how many are affected

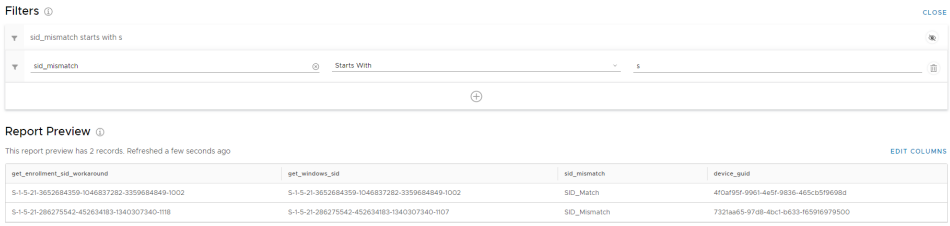
Create each sensor under Devices > Provisioning > Custom Attributes > Sensors. The examples below give sensor details and config details.

1. get_windows_sid - https://github.com/vmware-samples/euc-samples/blob/master/Windows-Samples/Sensors/get_windows_sid.ps1
2. get_enrollment_sid - https://github.com/vmware-samples/euc-samples/blob/master/Windows-Samples/Sensors/get_enrollment_sid_32_64.ps1
3. check_sid_mismatch - https://github.com/vmware-samples/euc-samples/blob/master/Windows-Samples/Sensors/Check_Matching_SID_Sensor_32_64.ps1

Assign to your device and run "query sensors" to force them to run. Note, if a user is logged off, sensors can't be manually triggered. They will run on agent check in schedule (usually every 4 hours).

Create Intelligence Report

1. Launch WS1 Intelligence
2. Go to Reporting > Reports. Add Report
3. Category: Workspace ONE UEM > Device Sensors.
4. Rename the report. Example "Check SID Mismatch"
5. Under Filters select "sid_mismatch" and either select available data or use "start with: s". Add the other columns as well:



Copyright © 2019 VMware. All rights reserved. Proprietary & Confidential