

Workspace ONE Re-Enrollment

Goal

To automatically un-enroll and re-enroll and Windows 10 device in various use cases:

1. On SID Mismatch. 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.
2. Always re-enroll. This is useful when fixing broken clients or when migrating WS1 Environments.
3. Never. This is for new enrollments only and will not un-enroll if an existing enrollment is found.

Change-Log

v2.5 - September 8th, 2020

- Added new parameter "Unenroll" to support various unenroll scenarios. Available Options are **Always**, **OnSIDMismatch**, **Never**
- Added new parameter RemoveLegacyCatalog in case admins don't want to remove the older WS1 App catalog.
- Added additional oma-dm clean up items

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 - [Link](#)
2. Airwatch Agent (get correct version matching customer console or download latest from getwsone.com)

Pre-reqs:

- Has 5 required parameters. These are used for the silent enrollment command line:
 - Server
 - LGName (Org Group ID)
 - Username
 - Password
 - Unenroll
- A logged in user does have to be detected. If no logged in user is detected the script will exit.

Usage

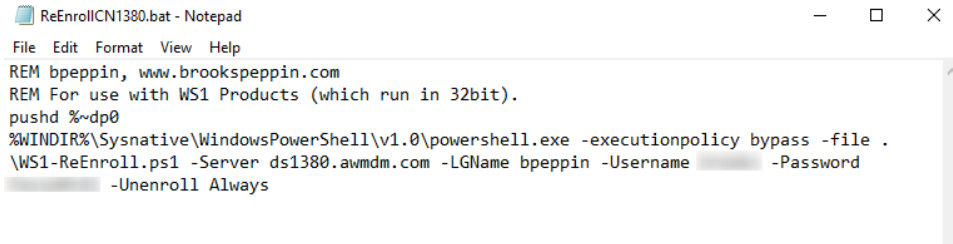
- Note this does require 64bit powershell. WS1 Products are 32bit and so you will need to update the batch file with this:
 - OnSIDMismatch:
 - %WINDIR%\Sysnative\WindowsPowerShell\v1.0\powershell.exe -executionpolicy bypass -file .\WS1-ReEnroll.ps1 -server [ws1u.em.awmdm.com](#) -lgname staging -username [staging@staging.com](#) -password 11111 - Unenroll OnSIDMismatch
 - Always
 - %WINDIR%\Sysnative\WindowsPowerShell\v1.0\powershell.exe -executionpolicy bypass -file .\WS1-ReEnroll.ps1 -server [ws1u.em.awmdm.com](#) -lgname staging -username [staging@staging.com](#) -password 11111 - Unenroll Always
 - Never
 - %WINDIR%\Sysnative\WindowsPowerShell\v1.0\powershell.exe -executionpolicy bypass -file .\WS1-ReEnroll.ps1 -server [ws1u.em.awmdm.com](#) -lgname staging -username [staging@staging.com](#) -password 11111 - Unenroll Never
- If using a 64 bit mechanism such as Software Distribution or another PCLM tool:

- powershell.exe -executionpolicy bypass -file .WS1-ReEnroll.ps1 -server [ws1uem.awmdm.com](https://www.brookspeppin.com) -lgname staging -username staging@staging.com -password 11111 -Unenroll OnSIDMismatch
- Logfile is saved in the same directory as the script (Script root)

Create a Product in WS1

Prep:

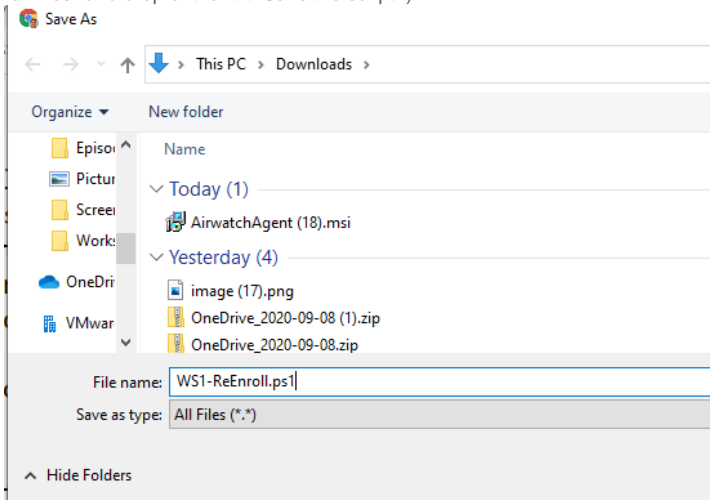
1. Download the batch file above and update the content with your environment specific details. Example:



```

ReEnrollCN1380.bat - Notepad
File Edit Format View Help
REM bpeppin, www.brookspeppin.com
REM For use with WS1 Products (which run in 32bit).
pushd %~dp0
%WINDIR%\Sysnative\WindowsPowerShell\v1.0\powershell.exe -executionpolicy bypass -file .
\WS1-ReEnroll.ps1 -Server ds1380.awmdm.com -LGName bpeppin -Username staging@staging.com -Password 11111 -Unenroll Always
  
```

2. Download or get the correct version of Intelligent hub (AirwatchAgent.msi) from getwsone.com
3. Download WS1-ReEnroll.ps1 file. (Click on the powershell script on Github, then click "raw", then right click "save as". Change "save as type" to "all files" and drop of the .txt. Save the script.)



Create Files/Actions

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

Edit Files/Actions

General	Files	Manifest
Name *	WS1-ReEnroll.ps1	
Description		
Version	11	
Platform	Windows Desktop	
Managed By *	VMware bpeppin	

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

Edit Files/Actions

General **Files** Manifest

+

ADD FILES

File Name	Path
WS1-ReEnroll.ps1	C:\Temp\WS1-ReEnroll.ps1
AirwatchAgent.msi	C:\Temp\AirwatchAgent.msi
ReEnrollCN1380.bat	c:\temp\ReEnrollCN1380.bat

Items 1-3 of 3

6. Manifest.
 - a. Click Add Action
 - b. Run, System, Path to your batch file

Edit Manifest

Action(s) To Perform *	<div>Run</div>
Execution Context *	<div>System</div>
Command Line and Arguments to run *	<div>C:\Temp\ReEnrollCN1380.bat</div>
TimeOut (-1 for infinite) *	<div>30</div> <div></div>

7. 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

General Manifest Conditions Deployment Dependencies

Name *

WS1-ReEnroll.ps1

Description

Managed By *

VMware bpeppin

Smart Groups

All Devices (VMware bpeppin)

Start typing to add a group

VIEW DEVICE ASSIGNMENT

Assignment Rules

ADD RULES

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

Add Manifest

Action(s) To Perform *

File/Action - Install

Files/Actions *

WS1-ReEnroll.ps1

Edit Product

General Manifest Conditions Deployment Dependencies

ADD

Up	Down	Step Number	Action Type	Persistent	Description	
▲	▼	1	Install Files/Actions	No	Files/Actions = WS1-Enroll-SID-Check	

Items 1-1 of 1

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.

General Manifest Conditions **Deployment** Dependencies

Server Date and Time : 9/9/2020 9:23 AM

Activation Date

Deactivation Date

Pause/Resume ☐

Product Type

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

JOBS

VIEW HISTORY SEND

Name	Product Set	Status	Type	Last Job ID
Hub 2003 Targeted Upgrade		Non-Compliant - MustPush	Elective	N/A
Nuke		Non-Compliant - MustPush	Elective	N/A
Save-Logs		Non-Compliant - MustPush	Elective	N/A
WS1 Health Check		Non-Compliant - MustPush	Elective	N/A
WS1-ReEnroll.ps1		Compliant	Elective	181375

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 (in my case I sent it to C:\temp): "C:\Temp\WS1-ReEnroll.ps1.log".

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:

Filters

sid_mismatch starts with s

sid_mismatch Starts With s

Report Preview

This report preview has 2 records. Refreshed a few seconds ago

get_enrollment_sid_workaround	get_windows_sid	sid_mismatch	device_sid
S-1-S-21-3652684359-1046837282-3359684849-1002	S-1-S-21-3652684359-1046837282-3359684849-1002	SID_Match	4f0af95f-9961-4a5f-9e36-465c1d5f6e8d
S-1-S-21-286275542-452634183-1340307340-1118	S-1-S-21-286275542-452634183-1340307340-1107	SID_Mismatch	7321aa65-9739-4bc1-b633-659f6979500