**Accman v2.0 – USG – Processing AD Account Deletions**

## Change History

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Revision** | **Summary/Reason** | **Changed By** |
| 11/08/2014 | 1 | Created | APB |
| 29/09/2014 | 2 | Clean up | PD |
| 30/10/2014 | 3 | Minor changes after running “Deletion of AD records” | PD |
| 04/12/2014 | 4 | Further minor changes after running “Deletion of AD records” | PD |

## Table of Contents

[Change History 1](#_Toc426465996)

[Table of Contents 1](#_Toc426465997)

[References 1](#_Toc426465998)

[Referenced by 1](#_Toc426465999)

[Background 1](#_Toc426466000)

[Pre-requisites 2](#_Toc426466001)

[Process 2](#_Toc426466002)

[Prior to Deletion 2](#_Toc426466003)

[Deletion of AD records 4](#_Toc426466004)

[After Deletion 4](#_Toc426466005)

[Appendix A – Example run\_student\_deletions.ps1 5](#_Toc426466006)

[Appendix B – File Structure 5](#_Toc426466007)

## References

## Referenced by

## Background

From time to time, network file store space needs to be freed up by deleting the F:\ drives of AD accounts that are no longer in use. The AD accounts themselves are also deleted, but they can potentially be re-created [with empty F:\ drives] if a person returns to the university at some point in the future.

The account deletion process is a part-manual/part-scripted process in three parts:

1. Bus Apps run a script to identify accounts to be deleted – list is sent to Ops.
2. Ops run a script to carry out the deletions in file store and AD.
3. Bus Apps run a script to update Accman to indicate that each AD account has been deleted.

This is done once a month, usually around 6th-10th of the month.

## Pre-requisites

* Access to uos-p-ambe-01.isdads.salford.ac.uk (also known as uos-p-acbe-01)

## Process

### Prior to Deletion

Run a script to identify accounts to be deleted to be sent to Ops (Mike Taylor).

1. RDP to uos-p-ambe-01. Personal network Credentials can be used for this.
2. Open a CMD prompt
3. cd C:\accman\support\useradmin\Powershell\accman\AD\_DELETIONS\1 - prior to deletions
4. Edit the three Powershell scripts:
   1. run\_associate\_deletions.ps1
   2. run\_staff\_deletions.ps1
   3. run\_student\_deletions.ps1
5. At the end of each script add a new line covering the next date range of accounts to delete.
   1. For the first date, set it to be the same as the previous lines second date.
   2. For the second date, set the day to be the day the scripts are run and set the month as follows:
      1. For associates and students, use 6 months prior.
      2. For staff, use 3 months prior.

A Type line will look like:

* + & .\list\_student\_usernames\_to\_delete 2013-02-01 2013-06-01 # Run on 2013-12-01

1. Run each script in turn:
   1. powershell .\run\_associate\_deletions.ps1
   2. powershell .\run\_staff\_deletions.ps1
   3. powershell .\run\_student\_deletions.ps1
2. The output files have names of the form:
   1. <user type> to delete – disabled between <date1> and <date2>.csv
   2. associates to delete - disabled between 2014-02-11 and 2014-03-16.csv
   3. staff to delete - disabled between 2014-05-11 and 2014-06-16.csv
   4. students to delete - disabled between 2014-02-11 and 2014-03-16.csv
3. Email files to Ops (currently Mike Taylor).

Note the run\_record\_xxx\_deletions.ps1 scripts will run the following script:

* + list\_xxx\_usernames\_to\_delete.ps1

### Deletion of AD records

Once Ops have finished their processes, they will send back three csv files back indicating which accounts were actually deleted. Normally the three lists will be the same as the three lists that were sent in step 1, but could have some usernames removed if Ops had been unable to delete specific usernames for some reason.

Recently Ops have been sending xlsx files back. The required csv file has one column called “username” and is a list of all accounts that need to be marked as deleted.

### After Deletion

Bus Apps run a script to update Accman to indicate that each account has been deleted.

1. Copy CSV files from Ops onto the server uos-p-ambe-01 in the folder:
   1. C:\accman\support\useradmin\Powershell\accman\AD\_DELETIONS\2 - after deletions
2. RDP to uos-p-ambe-01
3. Open a CMD prompt
4. cd C:\accman\support\useradmin\Powershell\accman\AD\_DELETIONS\2 - after deletions
5. Concatenate the three CSV files together:
   1. The CSV file is a single column of usernames, titled “username”.
   2. copy “file 1.csv”+”file 2.csv”+”file 3.csv” “deleted\_AD\_users.csv”
6. Edit the Powershell script:

run\_record\_list\_of\_deletions.ps1

A Type line will look like:

* + & .\record\_list\_of\_deletions\_as\_type\_1001\_transactions.ps1 "2014-08-12 00:00:03" # Run on 2014-08-13
  + The date in quotes needs to be changed to the date that the prior deletion scripts got run.

1. Run the Powershell script:
   1. powershell .\run\_record\_list\_of\_deletions.ps1 > console\_output.txt

Note the run\_record\_list\_of\_deletions.ps1 script will run the following script:

* + record\_list\_of\_deletions\_as\_type\_1001\_transactions.ps1

This script will read the concatenated CSV file and insert a type 1001 transaction into Accman to indicate that the AD account has been deleted. These are "information-only" pseudo-transactions that are flagged 'processed' at the point where they are created - i.e. they are never 'executed' in any way.

If a user comes back to the University, the Accman to AD interface will create a new AD record and empty F:\ drive for them. From an Accman point of view the account is just flagged as 'disabled' and when the user comes back Accman will generate a Type 13 'Enable' transaction. The Type 13 generates both a Type 103 (Enable AD) transaction and a Type 93 (Create AD account) transaction - so the AD account will either be re-enabled or re-created as appropriate.

## Appendix A – Example run\_student\_deletions.ps1

Example contents of run\_student\_deletions.ps1 script:

|  |
| --- |
| #& .\list\_student\_usernames\_to\_delete 2011-09-01 2013-02-01 # Run on 2013-08-01  #& .\list\_student\_usernames\_to\_delete 2013-02-01 2013-06-01 # Run on 2013-12-01  & .\list\_student\_usernames\_to\_delete 2013-06-01 2013-09-24 # Run on 2014-03-24 |

## Appendix B – File Structure

Consists of two main folders for the Prior and After processes:

**C:\accman\support\useradmin\Powershell\accman\AD\_DELETIONS\1 - prior to deletions**

**Control Scripts**

* run\_associate\_deletions.ps1
* run\_staff\_deletions.ps1
* run\_student\_deletions.ps1

**Extraction Scripts**

* list\_associate\_usernames\_to\_delete.ps1
* list\_staff\_usernames\_to\_delete.ps1
* list\_student\_usernames\_to\_delete.ps1

These scripts are all very similar - they query the Accman transactions table looking for 'processed' Disable (type 12) transactions within a certain date range. They also check that the username that the transaction relates to is still flagged 'disabled' - i.e. the account has not been re-enabled since the Disable transaction occurred.

**Archive Folders**

The folders 201405, 201406, 201407 etc. contain data files generated for deletions carried out in May, June, July etc. The data files have names of the form:

* associates to delete - disabled between 2014-01-08 and 2014-02-11.csv
* staff to delete - disabled between 2014-04-08 and 2014-05-11.csv
* students to delete - disabled between 2014-01-08 and 2014-02-11.csv

**C:\accman\support\useradmin\Powershell\accman\AD\_DELETIONS\2 - After deletions**

**Control Scripts**

* run\_record\_list\_of\_deletions.ps1

**Update Scripts**

* record\_list\_of\_deletions\_as\_type\_1001\_transactions.ps1

**Archive Folders**

The folders 201405, 201406, 201407 etc. contain data files generated for deletions carried in in May, June, July etc.