[](http://diplopedia.state.gov/images/IRM-Logo-Print-Small.jpg)

IRM – Local and AD Account Password Reset Tool

11 November 2014

Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Name | Description of Change | Version |
| 11/11/2014 | Danh Nguyen-Huynh | Script Author | V01.00 |
| 11/11/2014 | Kevin Berkheiser | First Draft Document | V01.00 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Table of Contents

[1. Purpose 1](#_Toc403501247)

[2. Local Account Script Capabilties 1](#_Toc403501248)

[3. AD Account Script Capabilties 1](#_Toc403501249)

[4. Roles and Responsibilities 1](#_Toc403501250)

[5. Local Account Script Procedures 1](#_Toc403501251)

[6. Active Directory Account Script Procedures 12](#_Toc403501252)

Table of Figures

**No table of figures entries found.**

Table of Tables

[Table 4‑1: Roles and Responsibilities 1](#_Toc403501243)

[Table 5‑1: Procedure Tasks 1](#_Toc403501244)

# Purpose

To document how to use IRM’s local and IRM’s Active Directory PowerShell Scripts for password resets.

# Local Account Script Capabilties

The local account script provides a GUI interface that allows admins to reset local admin account passwords on all or selected workstations in their organizational unit (OU). A unique password can be set for each local account that is a member of the local Administrators group on that workstation.

# AD Account Script Capabilties

The AD account script provides a GUI interface that allows admins to reset multiple AD user account passwords to a randomly generated 15 character value. This script also flags the account so the user must change their password at next logon, unless the account has been identified as a Service Account.

# Roles and Responsibilities

Table 4‑1: Roles and Responsibilities

|  |  |
| --- | --- |
| Role Title | Responsibilities |
| IRM/OPS/ENM/NED/EMS | Create and maintain the scripts and documentation |
| Local and AD administrators around the world | Optionally use these scripts around the world to maintain local account password age of 60 days or less and to conduct bulk AD and local account password resets. |

# Local Account Script Procedures

[*List all procedure steps in order of occurrence. Add the responsible party (individual or group), listed by functional title, as well as all activities involved in that step. Also include any procedure aids (manuals, guides, etc.) that are used while completing that individual task.*]

Table 5‑1: Procedure Tasks

|  |  |  |
| --- | --- | --- |
| Task | Description of Task | Procedure Aid |
|  | Logon to a Windows 2008 R2 or Windows 2012 R2 Server using an account that has Local Server and/or Local Workstation Admin rights |  |
|  | Download the latest version of the script. | http://irm.m.state.sbu/sites/ops/ENM/NED/EMS/DSE/Shared%20Documents/Forms/AllItems.aspx?RootFolder=%2Fsites%2Fops%2FENM%2FNED%2FEMS%2FDSE%2FShared%20Documents%2FSystems%20Administrator%20Tools&FolderCTID=0x012000108DB9E9187411459D8D2EDCAA0912A7&View={E293C952-EAB5-46C2-A81F-883D103C9948} |
|  | Create folder on your server for the script and put the script in the folder. |  |
|  | Find Windows PowerShell under “Accessories” in the start menu or on Windows 2012 R2 go to the start screen and simply type “Windows PowerShell” |  |
|  | Right click “Windows PowerShell” and Run as administrator |  |
|  | In the PowerShell window, check the script execution policy. It should be remote signed.  Run the command  get-executionpolicy | PS C:\Windows\system32> get-executionpolicy  RemoteSigned |
|  | If the execution policy is not RemoteSigned…  Run the command  set-executionpolicy remotesigned | PS C:\Windows\system32> set-executionpolicy remotesigned  Execution Policy Change  The execution policy helps protect you from scripts that you do not trust. Changing the execution policy might expose  you to the security risks described in the about\_Execution\_Policies help topic. Do you want to change the execution  policy?  [Y] Yes [N] No [S] Suspend [?] Help (default is "Y"): y  PS C:\Windows\system32> |
|  | Change to the folder you created for the script.  Run the command  Set-location <your folder in quotes>  Or use the alias  CD <your folder in quotes> | PS C:\Windows\system32> set-location "C:\!PS\!Fix-Passwords\IRM Local Account Password Reset Tool"  PS C:\!PS\!Fix-Passwords\IRM Local Account Password Reset Tool> |
|  | Look at the contents of the folder  Run the command  Get-ChildItem  Or use the alias  DIR | PS C:\!PS\!Fix-Passwords\IRM Local Account Password Reset Tool> get-childitem  Directory: C:\!PS\!Fix-Passwords\IRM Local Account Password Reset Tool  Mode LastWriteTime Length Name  ---- ------------- ------ ----  d---- 11/11/2014 6:53 PM \_Archive  -a--- 11/11/2014 8:06 PM 19743 IRM Local Account Password Reset Tool v1.0.ps1  PS C:\!PS\!Fix-Passwords\IRM Local Account Password Reset Tool> |
|  | Run the script.  Type the first few letters of the script and hit tab and powershell will cycle through the files in the folder that start with those letters.  Once you see the script hit enter. | PS C:\!PS\!Fix-Passwords\IRM Local Account Password Reset Tool> & '.\IRM Local Account Password Reset Tool v1.0.ps1' |
|  | This PowerShell script has a graphical user interface.  At the top, under the tile you will see a drop down menu for you to select the domain the computers are in.  Select your domain. |  |
|  | IMPORTANT. The GUI for this is scripted, this is not a programming language. There are several points where the script will have to connect to multiple computers you will have to watch the bottom left corner of the window to know what the script is doing. **Some of the queries this scripts has to make take some time to accomplish because the script must connect to one or many computers to obtain information.** Please be patient and wait for the script to complete each query. |  |
|  | WARNING  Don’t double click anything in the OU box until you have fully drilled down to the OU where you wish to find computers.  SINGLE CLICK the domain AND wait for the + to appear. |  |
|  | SINGLE CLICK each OU and wait for the + each time until you get to the OU where you want to search for computers.  When you reach the final OU, double click it and WAIT for it to show you all the computers it found in the bottom left.  This query will take a while to complete so be patient.  Once returned, the table can be sorted by clicking any of the column headers.  Any computer accounts that are highlighted in red and marked as OFFLINE did not successfully return a ping. |  |
|  | Select the computer(s) you would like to reset the password on (you can select multiple using shift+click, or ctrl+click) and select the [Scan Selected Computer(s) for Local Admin Accounts] button.  The script will scan each computer and list out all the local accounts found in the Administrators group. An aggregate of this list will be populated on the right-hand window. |  |
|  | Once the admin accounts are enumerated for all the selected computers, you will be required to set a password for each account found. It is strongly recommended that you select a complex password that is greater than 15 characters.  Once a password has been populated for each account, the [Reset Password for ALL Local Admin Accounts] will be enabled.  Click the [Reset Password for ALL Local Admin Accounts] button. |  |
|  | After completing, a text file will be placed on the desktop for each computer selected in the following format: [LocalAccountReset-COMPUTERNAME-Datetime.log]. Inside this file will be a list of local admin accounts that were reset using this script. |  |

# Active Directory Account Script Procedures

Table 6‑1: Procedure Tasks

|  |  |  |
| --- | --- | --- |
| Task | Description of Task | Procedure Aid |
|  | Logon to a Windows 2008 R2 or Windows 2012 R2 Server using an account that has Local Server and/or Local Workstation Admin rights |  |
|  | Download the latest version of the script. | http://irm.m.state.sbu/sites/ops/ENM/NED/EMS/DSE/Shared%20Documents/Forms/AllItems.aspx?RootFolder=%2Fsites%2Fops%2FENM%2FNED%2FEMS%2FDSE%2FShared%20Documents%2FSystems%20Administrator%20Tools&FolderCTID=0x012000108DB9E9187411459D8D2EDCAA0912A7&View={E293C952-EAB5-46C2-A81F-883D103C9948} |
|  | Create folder on your server for the script and put the script in the folder. |  |
|  | Find Windows PowerShell under “Accessories” in the start menu or on Windows 2012 R2 go to the start screen and simply type “Windows PowerShell” |  |
|  | Right click “Windows PowerShell” and Run as administrator |  |
|  | In the PowerShell window, check the script execution policy. It should be remote signed.  Run the command  get-executionpolicy | PS C:\Windows\system32> get-executionpolicy  RemoteSigned |
|  | If the execution policy is not RemoteSigned…  Run the command  set-executionpolicy remotesigned | PS C:\Windows\system32> set-executionpolicy remotesigned  Execution Policy Change  The execution policy helps protect you from scripts that you do not trust. Changing the execution policy might expose  you to the security risks described in the about\_Execution\_Policies help topic. Do you want to change the execution  policy?  [Y] Yes [N] No [S] Suspend [?] Help (default is "Y"): y  PS C:\Windows\system32> |
|  | Change to the folder you created for the script.  Run the command  Set-location <your folder in quotes>  Or use the alias  CD <your folder in quotes> | PS C:\Windows\system32> set-location "C:\!PS\!Fix-Passwords\IRM AD Account Password Reset Tool"  PS C:\!PS\!Fix-Passwords\IRM AD Account Password Reset Tool> |
|  | Look at the contents of the folder  Run the command  Get-ChildItem  Or use the alias  DIR | PS C:\!PS\!Fix-Passwords\IRM AD Account Password Reset Tool> get-childitem  Directory: C:\!PS\!Fix-Passwords\IRM AD Account Password Reset Tool  Mode LastWriteTime Length Name  ---- ------------- ------ ----  d---- 11/11/2014 6:53 PM \_Archive  -a--- 11/11/2014 8:06 PM 19743 IRM AD Local Account Password Reset Tool v1.0.ps1  PS C:\!PS\!Fix-Passwords\IRM AD Account Password Reset Tool > |
|  | Run the script.  Type the first few letters of the script and hit tab and powershell will cycle through the files in the folder that start with those letters.  Once you see the script hit enter. | PS C:\!PS\!Fix-Passwords\IRM AD Account Password Reset Tool > & '.\IRM AD Account Password Reset Tool v1.0.ps1' |
|  | This PowerShell script has a graphical user interface.  At the top, under the tile you will see a drop down menu for you to select the domain the computers are in.  Select your domain. |  |
|  | IMPORTANT. The GUI for this is scripted; this is not a programming language. **Some of the queries this script has to make take some time to accomplish.** Please be patient and wait for the script to complete each query. |  |
|  | WARNING  Don’t double click anything in the OU box until you have fully drilled down to the OU where you wish to find computers.  SINGLE CLICK the domain AND wait for the + to appear. |  |
|  | SINGLE CLICK each OU and wait for the + each time until you get to the OU where you want to search for users.  When you reach the final OU, double click it and WAIT for it to show you all the users it found in the bottom section.  This query will take a while to complete so be patient.  Once returned, the table can be sorted by clicking any of the column headers.  These categories are the same ones used in IPOST which keys off of the description field. |  |
|  | Select the user(s) you would like to reset the password on (you can select multiple using shift+click, or ctrl+click) and select the [Reset <type> Account(s) Password] button.  The script connect to each account and reset the password to a randomly generated 15 character password AND set the user must change password at next logon flag for all accounts **except Service accounts**.  Once completed, a message box will appear letting you know the location of the password file. | cid:image004.png@01CFF9F4.CBC92FD0 |
|  | After completing, a text file will be placed on the desktop for each type of account selected in the following format: [Type-AccountReset-Datetime.csv].  Inside this file will be a list of AD user accounts that were reset using this script with their unique password. | cid:image005.png@01CFF9F4.CBC92FD0 |