My1Login Group Policies

Contents

1 Introduction

This document outlines the various aspects of the My1Login SSO solution that require or are enhanced by Active Directory Group Policies.

The word “plug-in” is used throughout this document as a generic term for browser extensions, Internet Explorer Browser Helper Objects (BHO) or any other browser specific name for such a feature.

2 Overview of Policy Use

The table below summarises the aspects of the My1Login system that support or require group policy settings and gives direct links to the relevant document sections.

Area	Reference	Notes
COMMON		
AD Connector Endpoint in Local Intranet Zone	5	Required to enable Zero Login. Not needed if suitable wildcard URL already in Local zone
Add custom My1Login sub-domain to default browser pages.	6	The My1Login account may be configures to automatically open the user’s vault page. Sometimes the user experience is improved if this is done via a browser home page.
INTERNET EXPLORER		
EXE / MSI deployment of plugin	7.1	Not required if customer uses deployment tools other than GPO.
Enabling of plugin	7.3	Prevents users being prompted to enable the plugin.
Disable IE Password Manager	7.4	Prevents the browser password manager from capturing and exposing user credentials.
CHROME		
Deployment of extension	8.2	Browser plug-in is installed from Chrome store and auto updated.
Setting start-up page to use M1L query string	8.3	Enables the My1Login Chrome plug-in to login to My1Login in the background.
Disable Chrome Password Manager	8.4	Prevents the browser password manager from capturing and exposing user credentials.
FIREFOX		
Deployment of plugin	9.1	Browser plug-in is installed from a local copy of the extension file.
Enable Firefox to use Windows certificates and to trust the AD Connector Endpoint	9.4	Required to enable Zero Login for Firefox users.
Disable Firefox Password Manager	9.5	Prevents the browser password manager from capturing and exposing user credentials.
EDGE		
Deploy and configure Edge	10	How to deploy Edge via GPO, bypassing the need to use Developer mode.
DESKTOP AGENT		
MSI deployment of desktop agent Windows app	11.1	Not required if customer uses deployment tools other than GPO. Not in GPO document. Download MSI from https://download.my1login.com/Deployment/Desktop%20Connector/

3 General Group Policy Notes

3.1 Use Just One Group Policy

For simplicity in administering group policies we suggest that all My1Login related settings are made in the same group policy (e.g. “My1Login SSO”). However, this is merely a suggestion, we recognise that some products, particularly Firefox, tend to work better if all group settings are in the same group policy and that you may already have some settings enabled.

This document assumes that all settings are in a policy called “My1Login SSO”.

3.2 Merging Settings

The instructions in this document assume that you are starting from a clean sheet and that the settings may be freely applied.

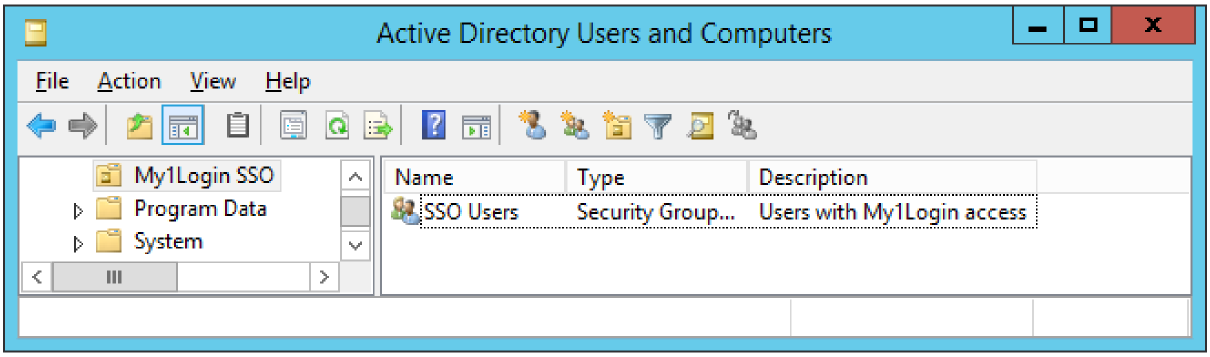
Some browser settings, e.g. setting startup pages, can influence what users can do so it may be desirable to merge existing settings with the My1Login settings. Contact My1Login if you have any questions on this.

3.3 Linking the Group Policy

The My1Login SSO policy should be deployed to those users who are synchronised to the My1Login system with the Active Directory Connector.

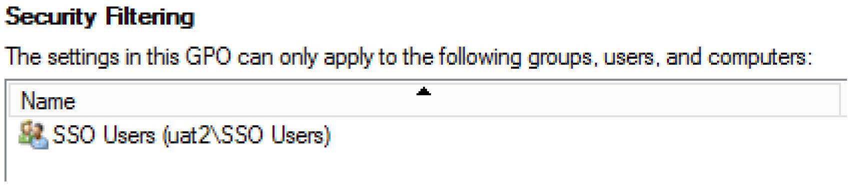
Deploying the policy to users that are not synchronised will not break anything, but users will see the browser plug-in icons and may see warnings that they do not have permission to use the My1Login system.

In a typical install the users permitted to use My1Login would be in one, or more, groups under a suitable OU. In the example below the users are in a group called “SSO Users” under an OU called “My1Login SSO”.



Name	Type	Description
SSO Users	Security Group...	Users with My1Login access

The My1Login SSO policy may be linked to the domain but to restrict the deployment of the My1Login group policy to those users permitted to use the system (using the above example), you would remove “Authenticated Users” from the Security Filtering section of the Scope tab of the policy and add the “SSO Users” group.

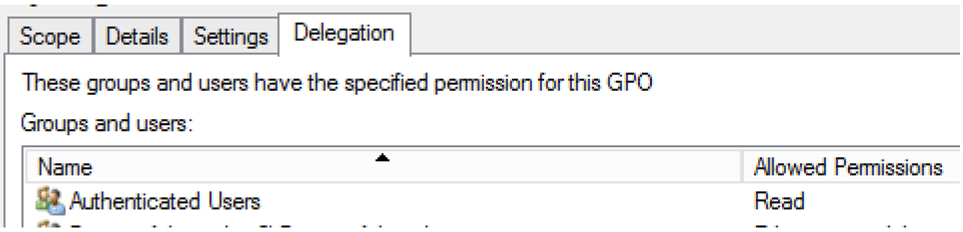


Security Filtering

The settings in this GPO can only apply to the following groups, users, and computers:

Name
SSO Users (uat2\SSO Users)

Removing “Authenticated Users” from this section requires it to be added, with read permissions, under the delegation tab.



These groups and users have the specified permission for this GPO

Groups and users:

Name	Allowed Permissions
Authenticated Users	Read

3.4 Location of Administrative Templates

It is necessary to install administrative templates for several of the browsers.

This document assumes that administrative templates are in the central store.

If your practice is to add templates to specific policies then you will need to amend the paths in the document to take account of the additional Classic Administrative Templates folder

Setting up the central store is beyond the scope of this document. Full details may be found at:

https://support.microsoft.com/en-ph/help/929841/how-to-create-the-central-store-for-group-policy-administrative-templa

Central store templates will be found in the PolicyDefinitions folder under your domain’s SYSVOL directory.

- Browse to %logonserver%\sysvol
- Drill into the folder named after your domain
- Drill into Policies \ PolicyDefinitions

3.5 Browser Password Managers

My1Login recommend disabling browser password managers (and other password vaulting tools).

One of the security goals of the My1Login system is to, where applicable, hide passwords from users. This is defeated if the browser password manager captures the password.

It is also possible for the browser password manager to mix up the credentials sent to websites.

The browser specific sections below explain how to perform this task.

4 Zero Sign-on and Non-IE Browsers

This section is not applicable to Internet Explorer.

Zero Sign-on may be triggered by the user browsing to your account’s My1Login subdomain and, if you decide to set one of your users’ browser home pages to that subdomain then no further action is required.

However, if you wish to utilise My1Login without forcing the users to access the My1Login portal then the browser plug-in needs to be told which My1Login account it is installed on.

We have developed a URL query string parameter that may be appended to your users’ homepage. This parameter identifies your My1Login account to the browser plug-in which, in turn, allows the plug-in to login to My1Login with no user intervention.

The query string has the format “?m1l=ABC123”.

The query parameter value for your account is available from the Administration / Security / Key Management page of the My1Login web app.

If one of the home pages was google, then you would append the query string as follows:

https://www.google.co.uk/?m1l=ABC123

The browser specific sections below explain how to set this value for each applicable browser.

5 Add AD Connector Endpoint to Local Intranet Zone

The zero sign-on feature of My1Login requires that a Kerberos ticket can be passed from the user’s browser to the My1Login Active Directory Connector (ADC). By default, only sites in the Local Intranet zone pass the credentials with the Kerberos ticket. This setting places the endpoint of the My1Login AD Connector into the Local Intranet zone.

Section	**User Configuration**		
Path	Policies\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel\Security Page		
Policy	Site to Zone Assignment List	**Action**	• Enable • Click Show • Add the FQDN of the AD Connector to the Value Name column. • Set the Value column to 1

5.1 Using IE Enhanced Protected Mode

Your organisation may already have a wildcard entry for the AD domain in the local intranet zone. This is perfectly satisfactory, if you are not using IE in Enhanced Protected Mode. When using EPM the entry MUST be the fully qualified domain name of the AD Connector’s host.

6 Adding My1Login Sub-Domain to Browser Home Pages

Some customers choose to have the My1Login vault page opened automatically for their users.

This may be accomplished via Account Settings within the My1Login administration area without the use of GPO settings.

When this is configured the My1Login browser plugin first logs into My1Login and then opens the vault page. This results in the vault page appearing to take longer than necessary to open. The actual time taken varies from customer to customer, for some the timescales are perfectly acceptable and for others they can appear to take too long.

If you wish to have the My1Login vault open as soon as possible after starting the browser then it is better to set your My1login.com sub-domain as one of the browsers startup / home pages because this avoids the initial delay of waiting for the browser plugin to login before starting to open the vault.

This document does not cover the browser specific settings for this.

7 Internet Explorer Browser Support

This section explains how to deploy and configure My1Login's Internet Explorer Plug-in.

The instructions in this section assume that you are using group policy to distribute and install the plug-in. If you use a different technology then please review this section for applicability.

7.1 Deployment and Installation of the My1Login Plug-in

The My1Login Internet Explorer Plug-in is available as 32 bit or 64 bit msi files or as a unified 32 and 64 bit exe installer.

The installers may be downloaded from:

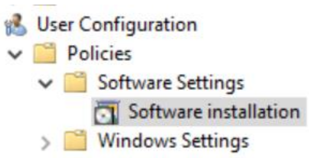
https://download.my1login.com/Deployment/My1LoginSSOConnector/Explorer/

The file name convention for this app is: My1Login_IE_SSO_Add-On_<architecture>_<version>.msi

The remainder of this section outlines how to deploy the IE Plug-in via Group Policy. If your organisation users another technology, then please use it.

7.2 GPO Deployment

Copy the msi or exe to an appropriate location (e.g. User\Applications under the Group Policy's folder). See 12 for details on this folder location.

Section	**User Configuration**		
Path	Policies \ Software Settings \ Software installation		
Policy	Configure the deployment of the desktop agent's msi.  User Configuration Policies Software Settings Software installation Windows Settings	**Action**	Right Click on "Software installation" Select New > Package… From the Open dialog select the plug-in's msi file then click "Open" In the Deploy Software dialog; select the "Assigned" option to have the agent automatically installed for the user, then click Ok. Double click on the Package created in the right-hand window of the GPO Editor. Click on the Deployment tab and ensure the "Install this application at logon" box is checked.

7.3 Automatically Enabling the Plug-in

The setting below prevents the user having to manually enable the My1Login plug-in.

Section	**User Configuration**		
Path	Policies \ Administrative Templates \ Windows Components \ Internet Explorer \ Security Features \ Add-on Management		
Policy	Add-on List	**Action**	• Enable • Click the Show… button • Set Value Name to {8741521A-2759-4DAC-A1CD-B586675E916A} • Set the Value to 1

7.4 Disabling Internet Explorer’s Password Manager

The following setting disables Internet Explorer’s password manager.

Section	**User Configuration**		
Path	Policies \ Administrative Templates \ Windows Components \ Internet Explorer		
Policy	Turn on the auto-complete feature for user names and passwords on forms	**Action**	• Disable

8 Chrome Browser Support

This section explains how to deploy and configure My1Login's Chrome Plug-in.

8.1 Import Chrome ADMX Templates

If the Chrome ADMX templates are already installed, then skip this section.

Obtain the Templates

The Chrome ADMX templates are available from:

https://dl.google.com/dl/edgedl/chrome/policy/policy_templates.zip

Extract the zip file to a temporary location.

There are multiple ways to host template files. The following sections cover the adding them to the policy being edited or using a central store.

Using the Central Store

Open the PolicyDefinitions folder (see section 3.4).

From the unzipped policy templates folders, copy the following to the PolicyDefinitions folder:

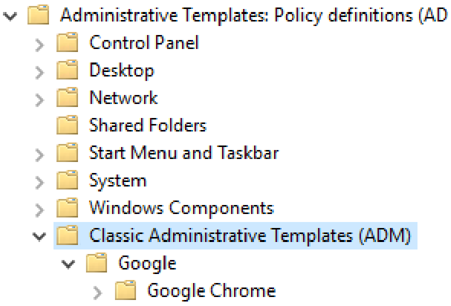
- The Chrome policy template
    - .\windows\admx\chrome.admx
- The relevant localisation folder (most likely en-US)
    - .\windows\admx\en-US

Using the Local Policy Store

The target group policy must exist before following these instructions.

- Edit the target group policy.
- Navigate to the User or Computer Configuration \ Policies \ Administrative Templates section
- Right click on Administrative Templates
- Select Add / Remove Templates
- Click the Add button
- Browse to the appropriate localisation template folder in the unzipped policy templates
    - E.g. \windows\adm\en-GB
- Select Chrome.adm
- Click Open
- Close the Add / Remove Templates dialog

The Chrome templates are now available under the Classic Administrative Templates section:



8.2 Deployment and Installation of the Plug-in

This setting will configure the installation of the My1Login Chrome plug-in from the Chrome store.

Section	**User Configuration**
Path	Administrative Templates\ Google Chrome\ Extensions
Policy	Configure the list of fore-installed apps and extensions
Action	Enable and set one of the Value entries to: nmmjlkfpmjldpacpocblimkniapnigff;https://clients2.google.com/service/update2/crx

8.3 Configure Chrome Start Page with My1Login Query String

See section 3.4 for a description of the My1Login Query String.

Section	**User Configuration**		
Path	Administrative Templates\ Google Chrome\ Startup pages		
Policy	Action on startup	**Action**	Enable and select “Open a list of URLs” from the dropdown.
Policy	URLs to open on startup	**Action**	Enable and click the Show button. Set one of the values to have the m1l query parameter. E.g. https://www.google.co.uk/?m1l=ABC123

8.4 Disable Chrome Password Manager

The following setting prevents the Chrome password manager from storing new passwords.

Section	**User Configuration**		
Path	Administrative Templates\ Google Chrome\ Password Manager		
Policy	Enable saving passwords to the password manager	**Action**	Disabled

Once the password manager is disabled any previously stored passwords are still available for use. These need to be removed to prevent interference with the My1Login passwords.

Section	**User Configuration**		
Path	Policies \ Windows Settings \ Scripts (Logon /Logoff)		
Policy	The actions create a script that deletes the password cache file from the user's computer when they login.	**Action**	• Double click on "Logon" • Create Delete script (see below) • In the Logon Properties dialog click the Add button and select the DeleteChromePassword.cmd file using the Browse button. • Click Ok to close the Add dialog, then Ok to close the Logon Properties dialog.

Creating the Delete Script

Open the Logon script folder as per section 12.

- Create a text file called DeleteChromePassword.cmd in this folder
- Edit the file and paste in the following line:

```
del "%LocalAppData%\Google\Chrome\User Data\Default\Login Data" /q
```

- Save the changes.

9 Firefox Browser Support

This section describes the policies required to install the My1Login Firefox browser plug-in and to enable Firefox to support the Zero Login feature.

Firefox configuration is largely done through JavaScript configuration files. This section assumes that you have no other Firefox policy settings in place. If you do you should compare them with the instructions below and merge them as appropriate.

9.1 Deploying the Plug-in

The Firefox plug-in may be obtained from the My1Login download site and the group policy configured to deploy it to the correct folder in a user's environment.

Download the Plug-in

Browse to

https://download.my1login.com/Deployment/My1LoginSSOConnector/Firefox

and download the file called

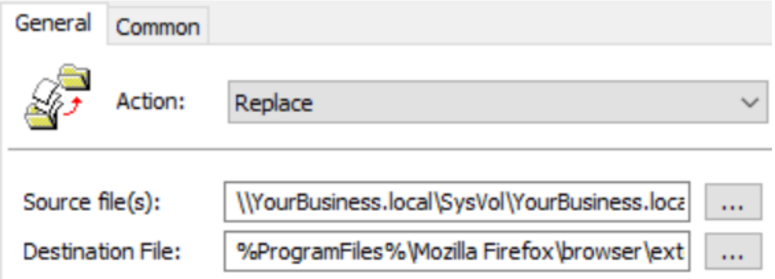
{09bb4618-94d1-4f5c-ba1f-6cf99054af19}.xpi

Do not change this filename, Firefox requires the name to be in this format.

Unless your organisation has other places to store common files, copy the xpi file to the Group Policy's "User\Documents & Settings folder" (see Appendix in section 12).

Deploying the Plug-in

The xpi file is deployed to the browser extensions folder of the users' Firefox installation. Note that Firefox will prompt the user to install the plug-in the first time it is used, this is standard Firefox behaviour.

Section	**User Configuration**		
Path	Preferences \ Windows Settings \ Files		
Policy	The actions deploy the xpi file to the correct folder on the user's desktop.	**Action**	- Right click on "Files" and select New > File - Set the Action setting to "Replace" - From the Source Files edit box; Browse to the xpi file location and select it. - Enter the following in the Destination File edit box: %ProgramFiles%\Mozilla Firefox\browser\extensions\{09bb4618-94d1-4f5c-ba1f-6cf99054af19}.xpi  General Common Action: Replace Source file(s): \\YourBusiness.local\SysVol\YourBusiness.loca Destination File: %ProgramFiles%\Mozilla Firefox\browser\ext

9.2 Firefox Settings File

The Firefox settings will be deployed in a custom My1LoginSettings.js file. If you already have Firefox configurations, then you should review merge the settings below with your existing ones and use this section as a guide rather than absolute instructions.

- Open the group policy’s “Documents & Settings” folder as per section 12.
- Create a file called My1LoginSettings.js in this folder.

Configure the deployment of this file in the same manner as for the plug-in:

Section	**User Configuration**		
Path	Preferences \ Windows Settings \ Files		
Policy	The actions deploy the settings file to the correct folder on the user’s desktop.	**Action**	• Right click on “Files” and select New > File • Set the Action setting to “Replace” • From the Source Files edit box; Browse to the My1LoginSettings.js file location and select it. • Enter the following in the Destination File edit box: %ProgramFiles%\Mozilla Firefox\defaults\pref\My1LoginSettings.js

9.3 Firefox Zero Login Support

By default, Firefox does not trust the certificates in the window’s certificate store. This must be enabled for Firefox to support the Zero Login feature.

Firefox must also be configured to trust the Zero Login endpoint of the My1Login AD Connector.

- Paste the following into the My1LoginSettings.js file and change the ADC DNS to reflect your environment.

```
// Firefox insists on the first line being unused.

pref("security.enterprise_roots.enabled", true);

pref("network.negotiate-auth.trusted-uris", "https://ADC DNS Name:47810");

pref("network.automatic-ntlm-auth.trusted-uris", "https://ADC DNS Name:47810");
```

9.4 Configure Firefox Start Page with My1Login Query String

See section 3.4 for a description of the My1Login Query String.

- Open the My1LoginSettings.js file and add the following line at the end. Be sure to use the correct home page and My1Login code for your account.

```
pref("browser.startup.homepage", "https://www.google.co.uk/?m1l=YOUR_CODE");
```

9.5 Disable Firefox Password Manager

The following setting prevents the Firefox password manager from storing new passwords.

- Open the My1LoginSettings.js file and add the following line at the end.

```
pref("signon.rememberSignons", false);
```

10 Microsoft Edge Browser Support

Due to Microsoft's current practice of not accepting third party Edge plug-in submissions the My1Login Edge Plug-in is not available from the Microsoft store.

In a non-AD environment, the Edge Plug-in must be installed in developer mode, and this is far from satisfactory for the general user population due to the requirement to enable the developer mode of the browser and for the user to manually enable and install the plug-in.

However, it is possible to deploy the Edge Plug-in using Group Policy settings without having to enable developer mode on the browser. This is known as "sideloading" the plug-in.

This section describes the group policies required to enable sideloading of the Edge plug-in.

Sideloading involves the group policy running a PowerShell script and this will likely involve changes to your organisation's PowerShell script settings (which default to not allowing scripts to execute).

10.1 Scope of GPO

The sideloading of the Edge plugin requires changing some computer configuration policies.

We have found that on Windows Server 2012 this requires the target computers (or simply the Domain Computers group) to be added to the policy's Scope / Security Filtering section.

This does not appear to be necessary on Windows Server 2016.

10.2 Install Microsoft Edge ADMX Templates

The domain controller requires the Windows 10 Administrative Templates to be installed (to give access to the Microsoft Edge settings).

The URL below provides links to all available versions of the Windows 10 Administrative Templates, along with instructions on configuring the required central store and deploying the templates in it.

https://support.microsoft.com/en-in/help/3087759/how-to-create-and-manage-the-central-store-for-group-policy-administra

The names of some policies differ by version of the templates. The notes below will list the synonyms that we are aware of.

10.3 Decide on PowerShell Script Execution Setting

There are four possible settings for PowerShell script Execution:

- Disabled (the default)
- Allow All Scripts
- Allow local and remote signed
- Allow only signed

If you choose to restrict running to signed scripts, then you will need to sign the PowerShell script that is defined later in this document. For brevity, this document assumes that you have set one of the options that allows local, unsigned scripts to execute.

Section	**User Configuration**		
Path	Administrative Templates\Windows Components\Windows PowerShell		
Policy	Turn on Script Execution	**Action**	Enable and set to required "Allow" value

10.4 Enable Sideloading of Apps

These settings allow the My1Login Edge plug-in application package to be installed on a user's computer without the app coming from the windows store or requiring developer mode to be set.

Section	**Computer Configuration**		
Path	Administrative Templates\Windows Components\App Package Deployment		
Policy	Allow all trusted apps to install	**Action**	Enable
Policy	Allow development of Windows Store apps without installing a developer license -or- Allows development of Windows Store apps and installing them from and integrated development environment (IDE)	**Action**	Enable

10.5 Enable / Disable Edge Developer Tools (Optional)

This setting determines whether the end users have access to the F12 developer tools.

If the My1Login Edge plug-in is manually installed, then the users must have the developer tools enabled. If it is sideloaded using the methods described in this document, then the developer tools may be enabled or disabled according to your company policy.

Section	**User Configuration (or Computer Configuration if required)**		
Path	Administrative Templates\Windows Components\Microsoft Edge		
Policy	Allow Developer Tools	**Action**	Enable or disable according to your company policy.

10.6 Configure Edge Start Page with My1Login Query String

See section 3.4 for a description of the My1Login Query String.

Section	**User Configuration (or Computer Configuration if required)**		
Path	Administrative Templates\Windows Components\Microsoft Edge		
Policy	(User Config) Configure Home Pages -or- (Computer Config) Configure Start Pages	**Action**	Enable and set one of the pages to have the m1l query parameter. E.g. <https://www.google.co.uk/?m1l=NHL6A8> Note that Edge uses angle brackets to separate multiple startup pages.

10.7 Deploy and Install the Edge Plug-in Package

This section describes where to place the plugin package file, how to add a PowerShell script to load the package and how to execute the script from the group policy.

If your organisation has other methods for deploying such products then they should be followed, using this section as a guide.

We have occasionally seen windows report that it takes two user logons for the package to be deployed by GPO.

Plugin Package

The My1Login Edge browser plug-in package may be download from:

https://download.my1login.com/Deployment/My1LoginSSOConnector/Edge

This should be copied to the policy's User\Application scripts folder.

- See section 12 for location of the Logon folder, the User\Application folder is above this.
- Copy the Edge Plug-in package file (file extension is .appx) to this folder.

Create the Install Script

1. Create a text file in the Logon folder called

   InstallMy1Login.ps1

   and open it in a text editor.

2. Copy the following two lines into the script:

```
echo Installing Edge Plugin
add-appxpackage "\\<Your SySVOL Path to Applications>\My1LoginEdgePlugIn.appx"
```

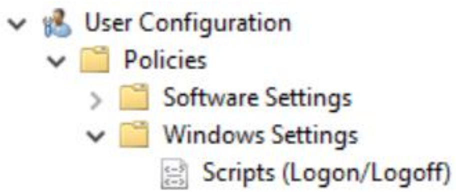
   You need to change the path to the plugin file to match your environment and the exact name of the plugin file that you downloaded.

   Hint: left click on the address bar in the file explorer and it will expand to a full text representation of the path to the Login folder. You can then copy and paste this value.

3. Save the updated script.

If you have chosen to only allow signed scripts in your environment, then you will need to sign this file. This is beyond the scope of this document but there is a useful blog post on doing this at https://www.hanselman.com/blog/SigningPowerShellScripts.aspx .

Add the Script to the Policy



Drill down through User Configuration / Policies / Windows Settings to the Scripts entry.

Click on "Scripts…", double-click on Logon, from the open Logon Properties dialog select the PowerShell Scripts tab.

- Click on the Add… button to open the Add a Script dialog

- Click the Browse… button and select the InstallMy1Login.ps1 file
- Click Ok to close the Add a Script dialog
- Click Ok to close the Logon Properties dialog

This step is now complete.

10.8 Updating the Edge Plug-in Package

The add-appxpackage command will take care of automatically updating the package on a user's computer.

To update a package, copy the updated .appx file to the Logon folder and either:

- Delete the old copy and rename the updated one to match the old name.
- Update the powershell script to refer to the name of the updated package file.

10.9 Disable Edge Password Manager

See section 3.5 for notes on browser password managers.

Section	**User Configuration**		
Path	Administrative Templates\Windows Components\Microsoft Edge		
Policy	Configure Password Manager	**Action**	Disable the setting

10.10 Troubleshooting Edge Deployment

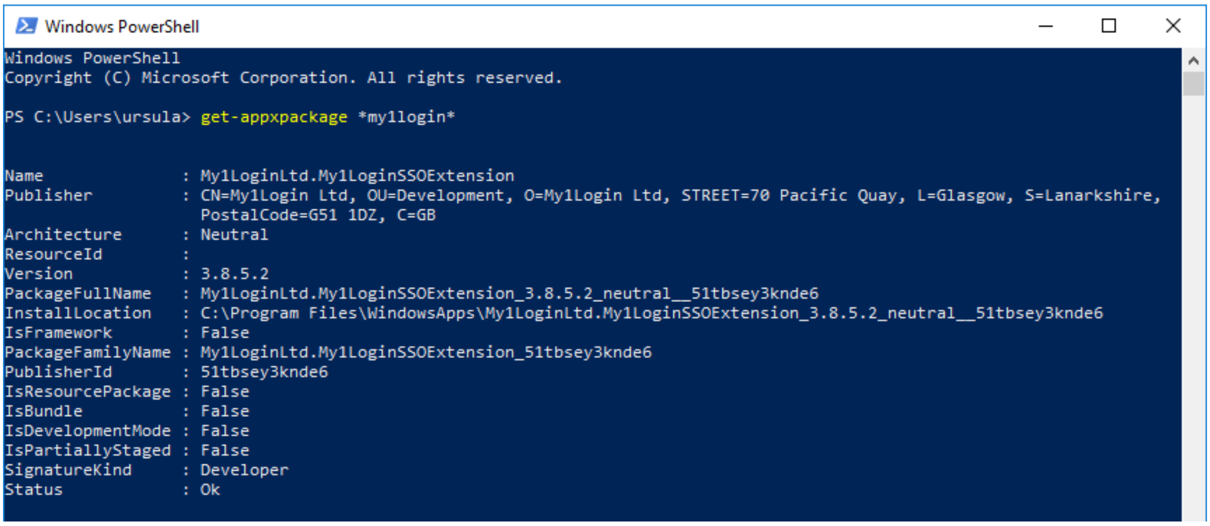
If the Edge plugin does not appear to have installed then there are a few powershell commands and Event Viewer areas that may be used to track down the cause.

10.10.1 Validate if the Package is Installed

- Open Powershell on the client PC

- Enter the command:
    - get-appxpackage *my1login*

- The screenshot below shows the details to expect if the package is installed. If there is no package then Powershell will simply show an empty command prompt.



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\ursula> get-appxpackage *my1login*


Name              : My1LoginLtd.My1LoginSSOExtension
Publisher         : CN=My1Login Ltd, OU=Development, O=My1Login Ltd, STREET=70 Pacific Quay, L=Glasgow, S=Lanarkshire,
                    PostalCode=G51 1DZ, C=GB
Architecture      : Neutral
ResourceId        :
Version           : 3.8.5.2
PackageFullName   : My1LoginLtd.My1LoginSSOExtension_3.8.5.2_neutral__51tbsey3knde6
InstallLocation   : C:\Program Files\WindowsApps\My1LoginLtd.My1LoginSSOExtension_3.8.5.2_neutral__51tbsey3knde6
IsFramework       : False
PackageFamilyName : My1LoginLtd.My1LoginSSOExtension_51tbsey3knde6
PublisherId       : 51tbsey3knde6
IsResourcePackage : False
IsBundle          : False
IsDevelopmentMode : False
IsPartiallyStaged : False
SignatureKind     : Developer
Status            : Ok
```

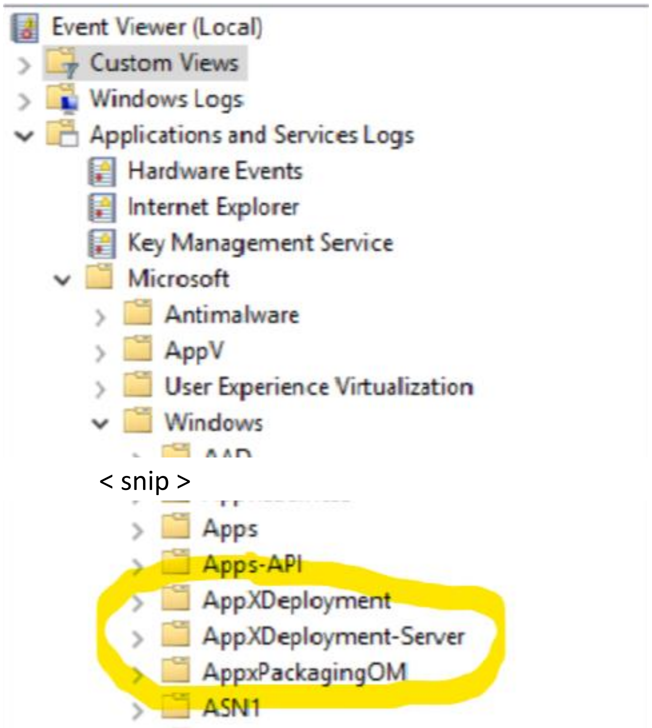
10.10.2 Checking the Event Viewer Logs

There are dedicated Event Viewer areas that relate to Edge package installations under the path

Applications and Services Logs \ Microsoft \ Windows

They are:

- AppxDeployment
- AppxDeployment-Server
- AppxPackagingOM



Any messages related to the My1Login package will contain the text "My1LoginLtd.My1LoginSSOExtension".

Warnings about unrecognized packages or missing resources may safely be ignored.

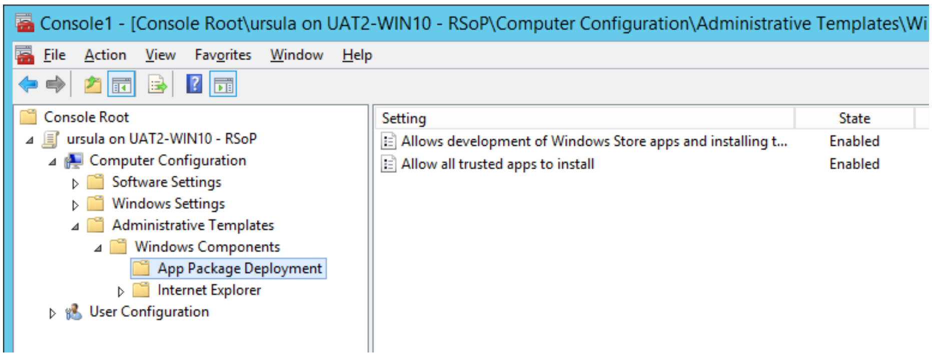
10.10.3 Missing Sideloading Setting

The most common errors that we have observed in testing was in the AppxDeployment-Server area. These errors had text referring to "…no valid license or sideloading policy could be applied." or error code 0x80073CFF.

Both have the same root cause, sideloading of apps (see 10.4) has not been configured.

- Check that the GPO has this policy set.
- Check the policy has been applied on the target computer.
  - Run rsop.exe in an elevated command / powershell window on the client, or run the Resultant Set of Policies simulator snap-in on the server.

- Check that the App Package Deployment settings are applied under the Computer Configuration, as shown below:



Console1 - [Console Root\ursula on UAT2-WIN10 - RSoP\Computer Configuration\Administrative Templates\Wi

Setting	State
Allows development of Windows Store apps and installing t...	Enabled
Allow all trusted apps to install	Enabled

- In our test environments the computer configuration had not deployed on a Windows Server 2012 environment because the target computer was not in scope for the group policy, see 10.1, above.

10.10.4 Other Errors

If you find other errors then check the Microsoft package troubleshooting pages:

https://docs.microsoft.com/en-gb/windows/desktop/appxpkg/troubleshooting

If you are still unable to resolve your issue then contact your My1Login team for assistance.

11 Desktop Agent Installation

The Desktop Agent is a Windows executable that runs on a user's desktop. It is available as a standard msi installer.

The Desktop Agent's msi may be downloaded from:

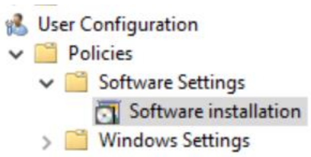
https://download.my1login.com/deployment/Desktop%20Connector/

The file name convention for this app is: My1Login_DesktopAgent_<version>.msi

The remainder of this section outlines how to deploy the Desktop Agent via Group Policy. If your organisation users another technology, then please use it.

11.1 GPO Deployment

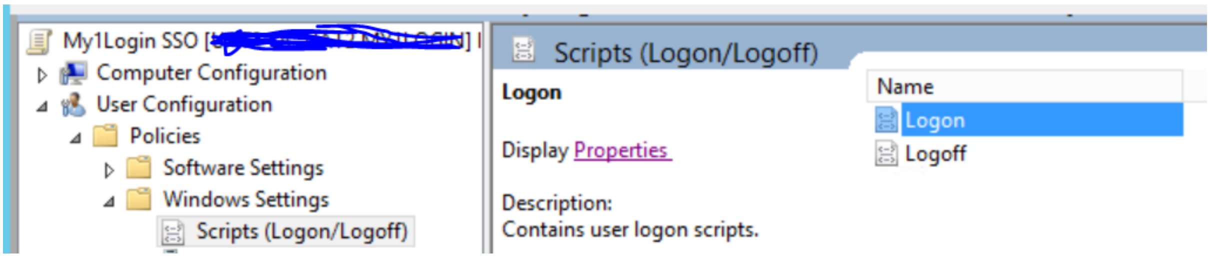
Copy the msi to an appropriate location (e.g. User\Applications under the Group Policy's folder). See 12 for details on this folder location.

Section	**User Configuration**		
Path	Policies \ Software Settings \ Software installation		
Policy	Configure the deployment of the desktop agent's msi.  User Configuration Policies Software Settings Software installation Windows Settings	**Action**	Right Click on "Software installation" Select New > Package… From the Open dialog select the Desktop Agent's msi file then click "Open" In the Deploy Software dialog; select the "Assigned" option to have the agent automatically installed for the user, then click Ok. Double click on the Package created in the right-hand window of the GPO Editor. Click on the Deployment tab and ensure the "Install this application at logon" box is checked.

12 Appendix 1: Location of Policy’s Logon, Script, etc. Folders

Several policies require scripts to be placed in the policy’s folder structure. This section explains how to find that set of folders.

In the Group Policy Management editor (for your My1Login SSO policy) browse to the User Configuration Scripts section, as per the screen shot below.



My1Login SSO [redacted]

- Computer Configuration
- User Configuration
  - Policies
    - Software Settings
    - Windows Settings
      - Scripts (Logon/Logoff)

Scripts (Logon/Logoff)

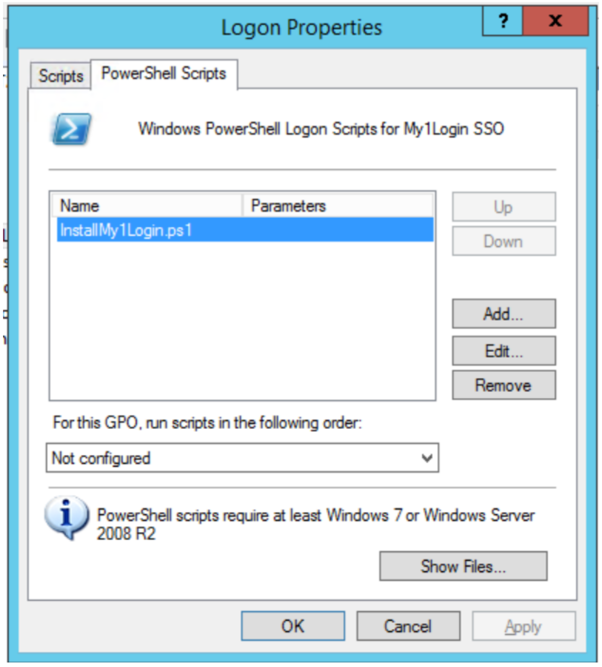
Logon

Display Properties

Description:
Contains user logon scripts.

Name
Logon
Logoff

Double click on the Login setting in the right-hand panel to open the Login Properties dialog.



Logon Properties

Scripts | PowerShell Scripts

Windows PowerShell Logon Scripts for My1Login SSO

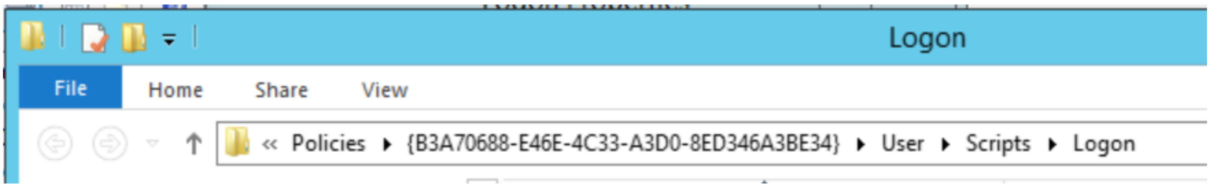
Name	Parameters
InstallMy1Login.ps1	

For this GPO, run scripts in the following order: Not configured

PowerShell scripts require at least Windows 7 or Windows Server 2008 R2

Click on the “PowerShell Scripts” tab and then on the “Show Files…” button.

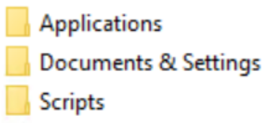
This opens a file explorer at the correct location for the plug-in package and installer file. The file path will resemble the one in the screen shot below.



Logon

« Policies ▸ {B3A70688-E46E-4C33-A3D0-8ED346A3BE34} ▸ User ▸ Scripts ▸ Logon

All other policy folders are under the User folder:



- Applications
- Documents & Settings
- Scripts