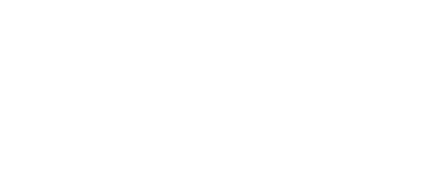
# EPA - Whitelist

*Prepared for*

EPA

14-Jan-15

Version .1 Draft



Whitelist Solution Design



*Prepared by*

**Sofiane ben** Sr. Consultant sofianeb@microsoft.com

Contributors

**David Weinstein**

Principal Consultant, daweins@microsoft.com

# Revision and Signoff Sheet

Change Record

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Author | Version | Change Reference |
| 01/14/2015 | Sofiane Ben | .1 | Initial draft for internal review/discussion |

Reviewers

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Name |  | Version Approved | Position | Date |

# Table of Contents

[1 Introduction 3](#_Toc412189513)

[2 Requirements 4](#_Toc412189514)

[3 Deployment & Configuration 5](#_Toc412189515)

[3.1 Deploying the Script 5](#_Toc412189516)

[3.2 Set up the Configuration File 6](#_Toc412189517)

[3.3 Create Windows Scheduled Tasks 8](#_Toc412189518)

[3.4 Test Check 8](#_Toc412189519)

[4 Usage 10](#_Toc412189520)

[4.1 Executing the Script 10](#_Toc412189521)

[Mismatch 10](#_Toc412189522)

[Mismatch-deep-team 10](#_Toc412189523)

[4.2 Configuring Logging 11](#_Toc412189524)

# Introduction

This document is aimed at providing guidance around the deployment and configuration of EPA’s O365 Whitelist script.

The function of the EPA’s O365 Whitelist script is to audit and monitor the external users invited into EPA’s SharePoint Online environment. The script implement a business logic to identify and revoke users that are out of compliance in addition to providing reports on existing external users.

The solution scans for external users that have accepted their invitation using a different email account then the one invited under. When an external user is identified, the script will revoke the external user and send her an email notification indicating that the account has been revoked and stating the reasons for the revocation.

EPA’s O365 Whitelist script is a console application written in .Net 4.5. The application leverages the APIs provided by Office 365 and SharePoint Online. The script communicate with EPA’s O365 tenant through SharePoint’s Client Side Object Model API (CSOM) and via https.

In addition, the script relies on configuration and report lists hosted within the global administrator site at <https://usepa.sharepoint.com/sites/oei_Community/epascene/globaladmin>.

# Requirements

The table below list the tool’s system requirement.

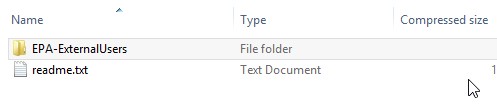
|  |  |  |
| --- | --- | --- |
| Requirement | Category | Comment |
| Windows Server OS | Platform | (any current version) |
| .Net 4.5 | Platform |  |
| Task scheduling solution | Platform | Preferably Windows Tasks Scheduler |
| Internet connectivity with port 443 enabled | Network | Communication with EPA  ‘s O365 is done via https |
| Microsoft.SharePoint.Client.dll | API | Included in package |
| Microsoft.SharePoint.Client.Runtime.dll | API | Included in package |
| Microsoft.SharePoint.Client.Search.dll | API | Included in package |
| Nlog.exe | API | Included in package |

***Note:*** The tool does not require additional technology such as an IIS/ASP.net sever or a SharePoint server.

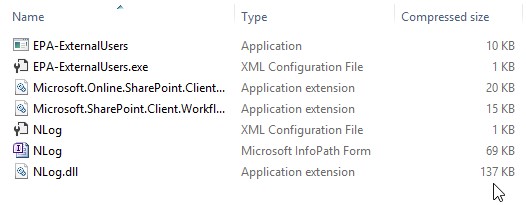
# Deployment & Configuration

## Deploying the Script

Extract the content of EPA-ExternalUsers.zip into your directory of choice. The folder created will contain a script folder as well as a readme file.



The script folder contains the tool’s executable and the supporting files



## Set up the Configuration File

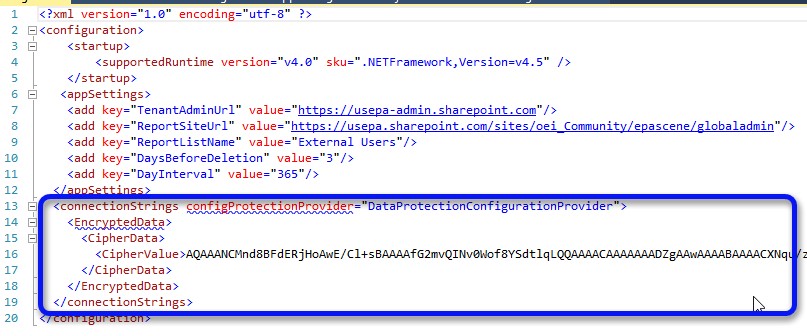
The configuration file is used to store the account credentials used to access EPA’s O365 tenant as well as other configuration parameters used by the script.

The configuration file should be encrypted using the ASP.net registration tool (aspnet\_regiis.exe) which ships with .Net 2.0.

In order to encrypt the configuration file:

* Rename EPA-ExternalUsers.exe.config to web.config
* Open web.config with your XML editor of choice
* Replace the encrypted element with a new connection string element

Replace



With

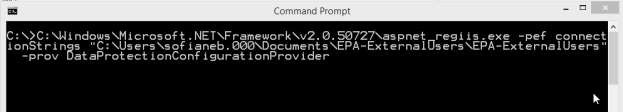


* Execute aspnet\_regiis.exe

Execute the following command prompt: <Path-To-

Windows>\Microsoft.NET\Framework\v2.0.50727\aspnet\_regiis.exe -pef connectionStrings

"<PathToFileDirectory>" -prov DataProtectionConfigurationProvider



* Rename web.config to EPA-ExternalUsers.exe.config

## Create Windows Scheduled Tasks

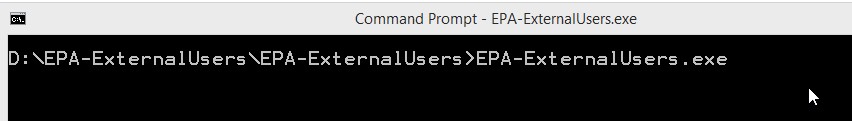
The script should be set up to execute at prescribed schedules and through Windows scheduled tasks. The scheduled tasks can be created with Windows’ GUI or using your command tool of choice.

Create 3 scheduled tasks:

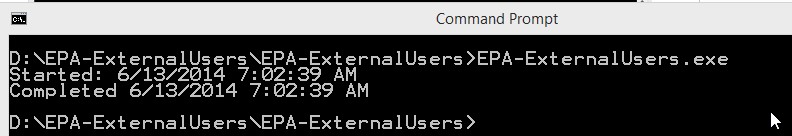
|  |  |  |
| --- | --- | --- |
| **Name** | Schedule | Command |
| EPA-Whitelist-Mismatch | Every 2 minutes | EPA-ExternalUsers.exe mismatch (See usage section ) |
| EPA-Whitelist-Mismatch-Deep-Team | Every 2 hours | EPA-ExternalUsers.exe mismatch-deep-team (See usage section ) |
| EPA-Whitelist-Mismatch-Deep-Team | Once a day | EPA-ExternalUsers.exe mismatch-deep-odfb (See usage section ) |

## Test Check

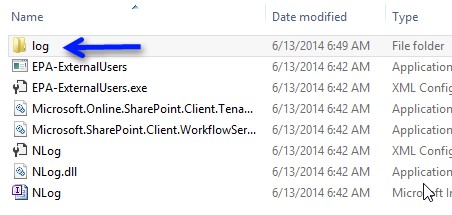
An easy way to test deployment is execute the script without any option parameter.



After few seconds the script executes and simply logs the date and time stamp.



The script will create a log folder if it doesn’t already exist and appends few lines into the contained log file



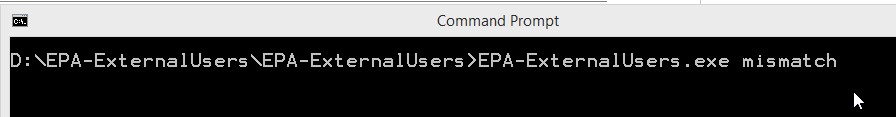
# Usage

## Executing the Script

The script should be executed through the command prompt. The script can be executed in 3 modes uses command line argument:

### Mismatch

This option will instruct the script to process the newly created external users that have accepted the invitation under a different user then the one used to invite them under. This option uses the GetExternalUsers method.



### Mismatch-deep-team

This option will instruct the script to process the newly created external users that have accepted the invitation under a different user then the one used to invite them under. This option uses the GetExternalUsersForSite method and enumerates through team sites only.

**Mismatch-deep-odfb**

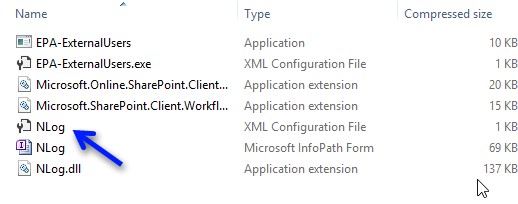
This option will instruct the script to process the newly created external users that have accepted the invitation under a different user then the one used to invite them under. This option uses the GetExternalUsersForSite method and enumerates through ODFB sites only.

## Configuring Logging

The script uses nlog as its underlining logging framework. This enables the tool to have highly configurable logging capabilities including:

* Minimum level
* Logs directory
* Logs files maintained criteria

The nlog dll and configuration files are found within the script folder and referenced in the tool.





Detailed guide to nlog can be found @<https://github.com/nlog/nlog/wiki>