How to consume SWAMID metadata with ADFS Toolkit

Installation/upgrading Procedure

The latest documentation for installation and upgrading can always be found here:
https://github.com/fedtools/adfstoolkit

Federation Defaults

The "Federation Defaults" is files provided by SWAMID that helps you configure ADFS Toolkit for our federation.
They also contain the specific SWAMID-versions of the Entity Categories which includes Swedish-specific attributes like norEduPersonNIN, etc.

When using the cmdlet Get-ADFSTKFederationDefaults you should point to the following URL:
https://mds.swamid.se/md/SWAMID_FederationDefaults.zip

Like this:

```
Get-ADFSTkFederationDefaults -URL https://mds.swamid.se/md/SWAMID_FederationDefaults.zip -InstallDefaults
```

Installation Procedure

Downloading the ADFS Toolkit uses Microsoft's PowerShellGallery.com service as the official primary distribution channel of ADFS Toolkit as a PowerShell Module. This allows us to rely on Microsoft's approach to managing distribution and updated PowerShell Modules for the lifecycle of ADFS Toolkit.

To install ADFS Toolkit you will need to:

- Visit https://PowerShellgallery.com and follow the instructions to install the latest PowerShellGet Module from PowerShellGallery
- Alter your Execution Policy for PowerShell scripts on your AD FS Server

Required Security Conditions

All installation steps are assumed to be performed by a user with both Local Administrator level access and AD FS Administrator access. SWAMID is in the process of acquiring a certificate for the securely deliver of the ADFS Toolkit through PowerShellGallery as a known trusted source. Until the certification process is in place, ADFS Toolkit requires the ability to run AD FS modules from unsigned origins.

To prepare your system for the ADFS Toolkit Execution policy settings issue the following PowerShell command to relax the policy.

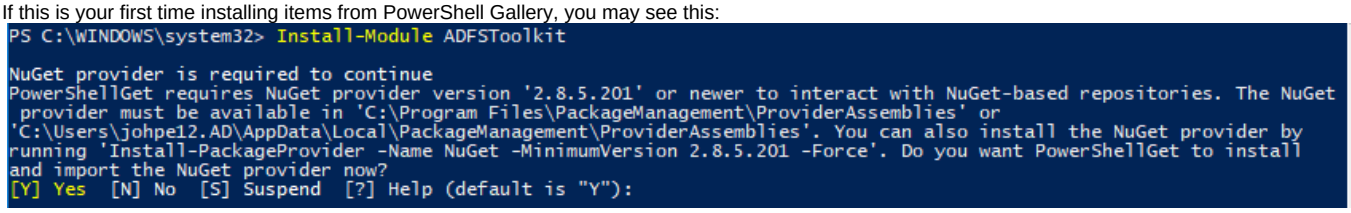
PowerShell
Set-ExecutionPolicy -ExecutionPolicy Remotesigned

Install the Module

The module is installed by issuing the command:

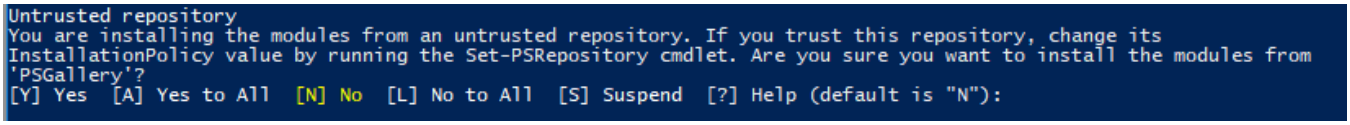
```
PowerShell

Install-Module –name ADFSToolkit
```

If this is your first time installing items from PowerShell Gallery, you may see this:



Answer yes to install the required NuGet provider

You may also see this:



Either update the PowerShell Gallery to be trusted or answer ‘Y’ to proceed.

Once connected, the Module will be installed in the default PowerShell home of:

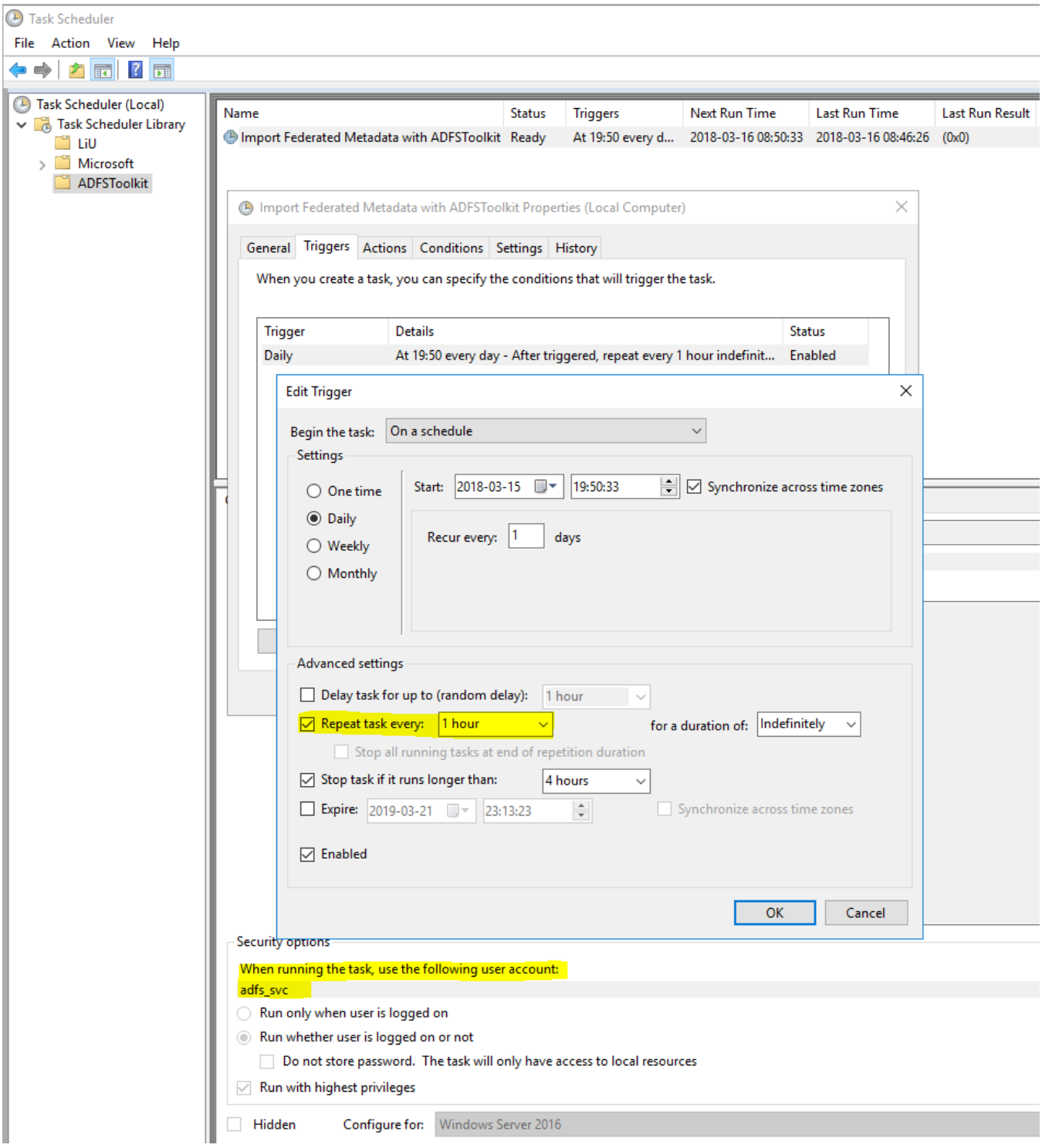
C:\Program Files\WindowsPowerShell\Modules\ADFSToolkit\[version #]

Scheduling Sync-ADFSTkAggregates to Run

ADFS Toolkit automatically creates a scheduled job with a default status of “Disabled”, allowing you to make edits to the configuration settings and to test them before enabling the automatically scheduled operation.

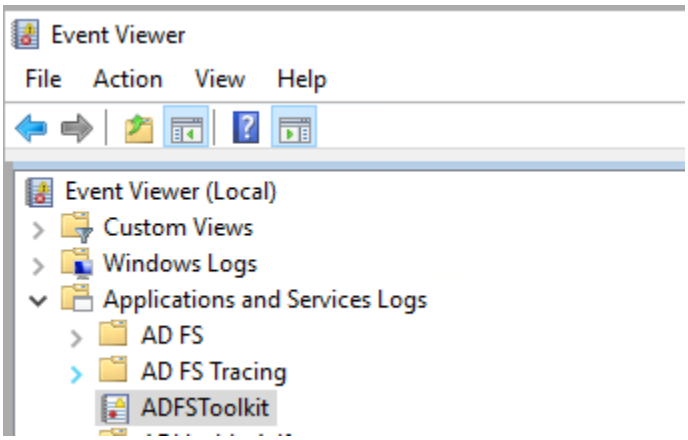
An hourly cycle is recommended and should be activated by the administrator to ensure your AD FS system is always synchronized with the SWAMID metadata.

We also recommend that a service account is used to run the scheduled task.



Reviewing Runtime Logs

ADFS Toolkit uses the Microsoft Windows Event Log infrastructure for application logging, available in the Event Viewer. Each record seen on the command line through manual execution is added to the logs and follows Microsoft recommendations for log rotation.



Configuring manual Attribute Release

ADFS Toolkit externalizes attribute release settings per Relying Party (RP) away from AD FS by housing the attribute release policies in a single PowerShell script file (Get-ADFSTkLocalManualSPSettings.ps1).

This allows administrators to refresh the attribute release for a given RP on each execution of the PowerShell script. It also provides AD FS administrators a convenient way to centrally manage attribute release rather than trying to find an element in the AD FS Administration Console, which may list thousands of RPs.

This script contains a number of commented out attribute release sets that can be copied and uncommented to be put into effect. Lines beginning with the pound '#' character denote a comment and will not execute if they contain code or commands.

The PowerShell script file to edit for releasing attributes is:

```
PowerShell

C:\ADFSToolkit\config\institution\get-ADFSTkLocalManualSPSettings.ps1
```

Import/re-import SWAMID Release Check SP's

It's a good idea to start testing your configuration by running SWAMID Release check (https://release-check.swamid.se).

There are quite some SP's to import or re-import so here's a small script to make it easier:

```
$ReleaseCheckSPs = Get-ADFSTkToolEntityId -Search release-check.swamid.se | Select -ExpandProperty Identifier

$i = 0
foreach ($ReleaseCheckSP in $ReleaseCheckSPs) {
    $i++
    Write-Host "Importing '$ReleaseCheckSP'... ($i/$($ReleaseCheckSPs.Count))" -ForegroundColor Yellow
    Import-ADFSTkMetadata -ConfigFile C:\ADFSToolkit\config\institution\config.Swamid.xml -EntityId
$ReleaseCheckSP -ForceUpdate
}
```

ADFS Toolkit Operational Behaviour

ADFS Toolkit (PowerShell Module) is designed for one installation per machine. Attempting to install multiple instances of ADFS Toolkit on a single host with different versions is possible, but it is not recommended or supported.

The modular design of ADFS Toolkit promotes code simplification and re-use, i.e. the settings and configurations can be re-used regardless of how many aggregates are loaded. Operational decisions and considerations should take into account the following best practices:

- Edits of the PowerShell script *ADFSTkManualSPSettings.ps1* need to result in correct PowerShell syntax and function.
    - This script is used at runtime across all scheduled jobs or installations. If you edit and save the script file in an incomplete state, it will affect the operation of the job and result in possible failure or incomplete operation, both of which may have an impact on the stability of your production service.
    - Before making changes to the script, you should always make a backup copy so that you can revert to the last known “steady state” if needed.
    - Using a test environment outside of and separate from production during development and testing is strongly encouraged. Once edits have been fully verified, you can copy the script to your production environment and execute it in confidence.
- **IMPORTANT:** When you have completed editing *ADFSTkManualSPSettings.ps1*, you MUST reissue the Import-Module ADFS Toolkit command to capture the changes you have just created. This will also validate your PowerShell settings if there is a problem (i.e. fails to reload the module)