

canarie



Technical Guide

Canadian Access Federation ADFSToolkit Installation Guide

Software Version: 1.0.0

Revision Date: April 16 2018

Technical Support: tickets@canarie.ca

canarie.ca | [@canarie_inc](https://www.instagram.com/canarie_inc)

Table of Contents

1. Using this Guide.....	3
1.1 Preface	3
1.2 Who Should Read This Guide	3
1.3 Skill and Knowledge Expectation of Installation Personnel	3
1.3.1 Required Operational Institutional Knowledge	3
1.3.2 Recommended Skills and Technology Familiarity	3
2 Installation Overview	3
3 Planning Your Installation	4
3.1 System Requirements	4
3.1.1 Minimum Server OS	4
3.1.2 Minimum PowerShell Version	4
3.1.3 Attribute Release Practices	5
4 Installation Procedure	6
4.1 Required Security Conditions	6
4.2 Install the Module	7
4.3 Configure ADFSToolkit for CANARIE's Canadian Access Federation	7
4.4 Bootstrapping Trust Explained	7
4.5 Configuring CAF's Domestic Aggregate	8
4.6 Loading the CAF Domestic Aggregate	10
4.7 In Case of a Problem	10
4.8 Configuring CAF's Inter-Federation Aggregate	11
4.9 Loading the CAF Inter-Federation Aggregate	12
4.10 Scheduling sync-ADFSTkAggregates to Run	12
4.11 Reviewing Runtime Logs	13
5 Configuring Attribute Release	14
6 ADFSToolkit Operational Behaviour.....	15
6.1 ADFSToolkit's Lifecycle Management	16
6.2 Testing with CAF Test Federation	17
7 Connecting to FIMS Production	18

1. Using this Guide

1.1 Preface

The ADFSToolkit was designed to rapidly configure your Active Directory Federation Services (AD FS v3 or higher) in order to connect to the CANARIE Canadian Access Federation's Federated Identity Management (FIM) service. The ADFSToolkit reduces the installation and configuration time for CAF services to a matter of minutes and offers techniques to manage trust in a scalable fashion.

1.2 Who Should Read This Guide

This guide is intended for person(s) responsible for the planning, preparation, installation, and administration of CAF services at their institution.

1.3 Skill and Knowledge Expectation of Installation Personnel

Although the installation tools and process are intended to minimize the required depth of knowledge across all components, the following skills and knowledge would be beneficial:

1.3.1 Required Operational Institutional Knowledge

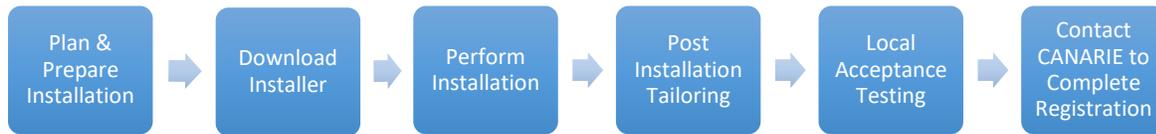
- Web-based sign-on technologies
- Service and deployment management strategy
- Active Directory Federation Service administration
- Ability to navigate, configure and manage Active Directory Federation Services components (start/stop services, managing configuration within AD FS, review logs, etc.)
- Ability to download, configure, and execute PowerShell scripts
- Firewall configuration, management, and/or ability to request updates

1.3.2 Recommended Skills and Technology Familiarity

- Web sign-on strategies and techniques
- Testing and change control practices

2 Installation Overview

The following steps will be followed to successfully complete installation, configuration, and verification of CAF services to a test and/or production environment.



3 Planning Your Installation

3.1 System Requirements

CANARIE's ADFSToolkit must be installed on a Windows Server (your AD FS host) with:

- Microsoft AD FS v3 or higher
- Local administrator privileges to schedule privileged jobs
- AD FS administrator-level permissions to run PowerShell commands
- Acceptance of the security considerations running PowerShell retrieved from Microsoft's PowerShellgallery.com

While not a firm requirement, we strongly suggest a test AD FS environment to perform the installation prior to installing in production. You should be aware that after installation, you will see a few thousand trusts displayed within the administration toolset, AD FS-Microsoft Management Console (MMC).

3.1.1 Minimum Server OS

Windows Server 2012 R2 or newer is the minimal level of OS supported. You should also be current on latest OS and security patch/updates provided by Microsoft.

3.1.2 Minimum PowerShell Version

ADFSToolkit uses Microsoft's PowerShell with Windows Management Framework (WMF) 5.1. To see if your host is WMF5.1 ready, check the [Microsoft Compatibility Matrix](#).

To quickly see which version of PowerShell you have, open a PowerShell window or PowerShell ISE window and enter `$PSVersionTable`. If you do not see version 5.1, you will need to update your environment first.

Name	Value
PSVersion	5.1.14393.1944
PSEdition	Desktop
PSCompatibleVersions	{1.0, 2.0, 3.0, 4.0...}
BuildVersion	10.0.14393.1944
CLRVersion	4.0.30319.42000
WSManStackVersion	3.0
PSRemotingProtocolVersion	2.3
SerializationVersion	1.1.0.1

Figure 1 - PowerShell at Version 5.1, the Minimal Required to Proceed

WMF 5.1 can be downloaded from here: <https://docs.microsoft.com/en-us/PowerShell/wmf/5.1/install-configure>

ADFSToolkit will not proceed until your environment has been upgraded to at least this latest PowerShell version.

3.1.3 Attribute Release Practices

ADFSToolkit is a component built for and by the research and education (R&E) community that embraces scalable attribute release management principles of R&E federations. One of these principles is the use of Entity Categories for attribute release. Entity Categories are tags on an entity in SAML2 metadata that indicate membership in a given category of service. The attribute release model using Entity Categories has a release policy set against the category, not the entity.

When ADFSToolkit parses entities to load into AD FS and encounters an Entity Category called 'Research and Scholarship' (R&S)¹, it automatically creates multiple AD FS transform rules that reflect the minimal set of attributes released, not much different than your public directory pages. For R&S, the attributes are:

- eduPersonPrincipalName (left hand of the "@" sign of the UPN, concatenated with your domain)
- mail
- displayName
- givenName
- sn (Surname)
- eduPersonScopedAffiliation (controlled vocabulary mapped from groups in AD)

This is the default behaviour of ADFSToolkit. By using it, you are enabling this model of attribute release by default. You are encouraged to contact CANARIE and register your organizations as supporting the

¹ <https://refeds.org/category/research-and-scholarship>

Research and Scholarship entity category to realize full benefits. See this link for more details:
<https://www.canarie.ca/identity/fim/research-and-scholarship-entity-category/>

4 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

4.1 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. CANARIE is in the process of acquiring a certificate for the secure delivery 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
```

4.2 Install the Module

The module will be 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:

```
Untrusted repository
You are installing the modules from an untrusted repository. If you trust this repository, change its
InstallationPolicy value by running the Set-PSRepository cmdlet. Are you sure you want to install the modules from
'PSGallery'?
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "N"): _
```

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 #\]](#)

4.3 Configure ADFSToolkit for CANARIE's Canadian Access Federation

CANARIE's Canadian Access Federation (CAF) produces two aggregates for trust data that AD FS needs to load; the domestic aggregate for Canadian elements and the inter-federation aggregate for the worldwide Research and Education (R&E) entities in which Canada participates. Between these two aggregates, more than 1,000 Relying Parties will be added to your AD FS infrastructure.

The ADFSToolkit is designed to load a single aggregate at a time for simplicity. To be fully connected to CAF, two configuration files, one for each aggregate, are needed. ADFSToolkit provides a command to create the necessary configuration and can schedule the loading (automatic updates of metadata aggregates) for you as well.

4.4 Bootstrapping Trust Explained

AD FS does no trust verification on the data it loads other than having a valid HTTPS endpoint. This minimal validation alone is insufficient for AD FS to participate in a Federation's circle of trust. ADFSToolkit helps elevate or 'bootstrap' AD FS as a trusted endpoint in the federation by:

- Verifying the veracity of the key being used by the SHA256 fingerprint that you provide
- Based on this key, you can trust that the aggregate has not changed since being cryptographically signed with that key

ADFSToolkit processes help ensure that the content is valid and safe for AD FS to load and that it originated from an authority that you trust: CANARIE CAF.

The validation approach ADFSToolkit uses is based on the user supplying the fingerprint of the certificate that they want to trust.

The SHA256 fingerprint of the CANARIE certificate is:

36CFD8090A88B8D75264E790FEA1B6F7ECBECF42C881AAF6F459D3AE3B459304

This fingerprint can be verified manually by:

- Fetching CANARIE's public portion of our certificate that we use to sign our aggregates here: https://caf-shib2ops.ca/CoreServices/caf_metadata_verify.crt
- Using the following OpenSSL command to find the fingerprint of the certificate you just downloaded:

```
canlt084:tmp$ openssl x509 -noout -fingerprint -sha256 -inform pem -in ./caf_metadata_verify.crt  
SHA256  
Fingerprint=36:CF:D8:09:0A:88:B8:D7:52:64:E7:90:FE:A1:B6:F7:EC:BE:CF:42:C8:81:AA:F6:F4:59:D3:AE:3  
B:45:93:04
```

The latest information for the configuration is available on the Identity section of the CANARIE website, under CAF Support, FIM Tools: (<https://www.canarie.ca/identity/support/fim-tools/>).

4.5 Configuring CAF's Domestic Aggregate

To create the configuration file for CAF's Domestic Aggregate, issue these commands:

```
PowerShell  
  
New-ADFSTkConfiguration
```

The command will prompt you for the following answers (see table below) and results in a configuration file created on disk. Optionally, a scheduled job to hourly process the aggregate can be created. The scheduled job is disabled by default.

Question	Answer
Metadata Aggregate	https://caf-shib2ops.ca/CoreServices/caf_metadata_signed_sha256.xml
Certificate Fingerprint	This is the Canadian Access Federation's fingerprint: 36CFD8090A88B8D75264E790FEA1B6F7ECBECF42C881AAF6F459D3AE3B459304
Metadata Prefix	<ul style="list-style-type: none"> This is the prefix added to each Relying Party (RP, also known as Service Provider) entry in AD FS. Defaults to 'ADFSTK' unless you provide one here. We recommend having different prefixes for each aggregate to distinguish their origin when detecting differences in AD FS as compared to the aggregate. Note that colons are used as a separator and are not allowed to be used as part of the prefix
Institution Name	<ul style="list-style-type: none"> This populates the Attribute 'o' for Organization Name. Recommended value is your Organization's official name
Country Name	<ul style="list-style-type: none"> This populates the Attribute 'co' for Country Name. Recommended value is 'Canada'
Country Code	<ul style="list-style-type: none"> This populates the Attribute 'c' for Country code Recommended value is 'CA'
Institution Domain	<ul style="list-style-type: none"> Recommended value is the domain of your institution. It is used as the scope for certain attributes to ensure unique identifiers are unique globally
Short Name for Your Institution	<ul style="list-style-type: none"> Recommended value is a short name representation of your institution that you commonly use, e.g. University of British Columbia may be known as UBC.
External DNS Name of Your AD FS Infrastructure	<ul style="list-style-type: none"> This is the Fully Qualified Domain Name (FQDN) of your AD FS instance

When the configuration is complete, the resulting XML configuration file will be found in the `"/config"` folder in the PowerShell Module's base directory. It is this configuration file that will be processed in a subsequent PowerShell command to load (or synchronize) metadata aggregate into AD FS.

```
PowerShell Hint: Use this to see ADFSToolkit's Module base directory
Get-Module -Name ADFSToolkit).ModuleBase
```

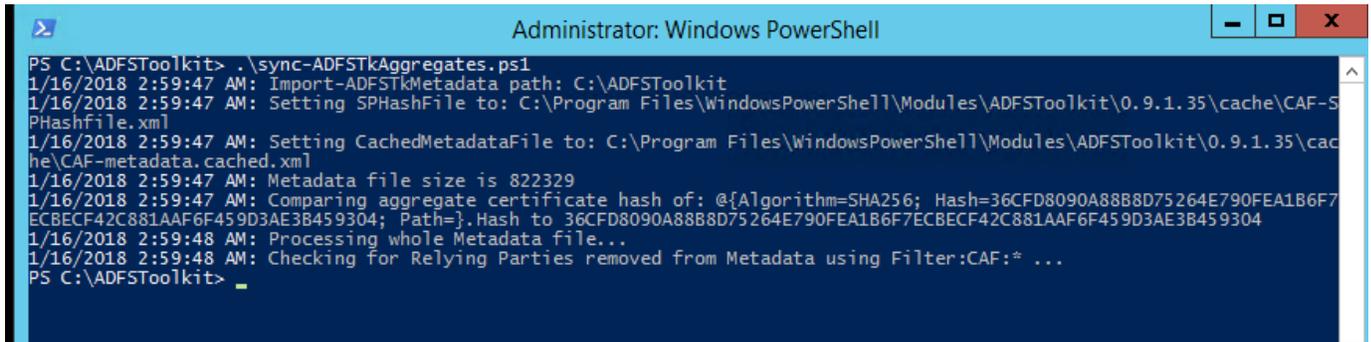
In addition, a new directory will be created on disk in: `C:\ADFSToolkit\`. Additionally, a subdirectory is created correlating to the version of the ADFSToolkit module in use. This sub-directory contains the Task Scheduler job `sync-ADFSTkAggregates.ps1` and other version-specific configuration of ADFSToolkit. This permits one or more aggregates to be loaded (or re-loaded) with a single command and previous versions of ADFSToolkit to remain intact during updates. This document will refer to the directory of the latest version of ADFSToolkit (`C:\ADFSToolkit\#.##.#\`) as the latest ADFSToolkit home directory.

Subsequent runs of “New-ADFSTkConfiguration” command in PowerShell will append a command to load that aggregate in the [sync-ADFSTkAggregates.ps1](#) PowerShell script.

4.6 Loading the CAF Domestic Aggregate

Once the domestic aggregate configuration has been created, the latest ADFSToolkit home directory will contain the PowerShell script `<sync-ADFSTkAggregates.ps1>` used to load the aggregate. To load the Domestic Aggregate, simply execute the [sync-ADFSTkAggregates.ps1](#) command and observe the output on the screen or via the Event Viewer in the ADFSToolkit event log.

This command is designed to run repeatedly, synchronizing the aggregate and keeping it up-to-date. The first execution of the command may take over a minute to synchronize all entities, and will run at about 100 entities per minute. Subsequent runs will perform more quickly in comparison, as the records have already been created and are only updated if a change is detected.



```
Administrator: Windows PowerShell
PS C:\ADFSToolkit> .\sync-ADFSTkAggregates.ps1
1/16/2018 2:59:47 AM: Import-ADFSTkMetadata path: C:\ADFSToolkit
1/16/2018 2:59:47 AM: Setting SPHashFile to: C:\Program Files\WindowsPowerShell\Modules\ADFSToolkit\0.9.1.35\cache\CAF-SPHashfile.xml
1/16/2018 2:59:47 AM: Setting CachedMetadataFile to: C:\Program Files\WindowsPowerShell\Modules\ADFSToolkit\0.9.1.35\cache\CAF-metadata.cached.xml
1/16/2018 2:59:47 AM: Metadata file size is 822329
1/16/2018 2:59:47 AM: Comparing aggregate certificate hash of: @{Algorithm=SHA256; Hash=36CFD8090A88B8D75264E790FEA1B6F7ECBECF42C881AAF6F459D3AE3B459304; Path=}.Hash to 36CFD8090A88B8D75264E790FEA1B6F7ECBECF42C881AAF6F459D3AE3B459304
1/16/2018 2:59:48 AM: Processing whole Metadata file..
1/16/2018 2:59:48 AM: Checking for Relying Parties removed from Metadata using Filter:CAF:* ...
PS C:\ADFSToolkit>
```

Figure 2 - Sample Execution of Loading CAF Domestic Aggregate

If all appears as it should, you can proceed to adding the second CAF aggregate (Inter-Fed) which is done by running the [New-ADFSTkConfiguration](#) command again, with some minor differences outlined in Section 4.9 below.

Note: You will notice some errors or warnings in the PowerShell Console window. This is expected and you can review details in the Event Viewer to determine severity or if any action needs to be taken (See Section 4.11 for more details).

4.7 In Case of a Problem

If for any reason you want to revert or remove all the trusts created from loading the aggregate, we have provided a command within the ADFSToolkit called [unpublish-ADFSTkAggregates](#) to do just that. If this command is invoked without any arguments, it will assume the default prefix of ‘ADFSTK’. The metadataPrefix is the value you set for each of the entities when they are loaded and is stored in the configuration file. You do not need to include the prefix separator of a colon “:” in the prefix definition.

This command will select all entities with this prefix and delete them. Please take special care using this command, as it is a non-reversible, destructive action.

```
1/16/2018 2:59:48 AM: Processing whole Metadata File...
1/16/2018 2:59:48 AM: Checking for Relying Parties removed from Metadata using Filter:CAF:* ...
PS C:\ADFSToolkit> Unpublish-ADFSTkAggregate

Confirm
Are you sure you want to perform this action?
Performing the operation "Unpublish-ADFSTkAggregate" on target "ADFSTk;".
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "Y"): N
PS C:\ADFSToolkit> Unpublish-ADFSTkAggregate -FilterString CAF

Confirm
Are you sure you want to perform this action?
Performing the operation "Unpublish-ADFSTkAggregate" on target "CAF".
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "Y"): Y
PS C:\ADFSToolkit> _
```

Figure 3 - Sample Invocations of `unpublish-ADFSTkAggregates` (With and Without `-FilterString` Argument)

4.8 Configuring CAF's Inter-Federation Aggregate

To create the configuration file for CAF's Inter-Federation Aggregate, issue the same `New-ADFSTkConfiguration` command using the same answers you provided (Section 4.5) above with the exception of a new aggregate URL and metadataPrefix.

Notes:

- It is important that you use a different metadataPrefix to ensure no collisions occur between other aggregates and the caches ADFSToolkit uses outside of AD FS.
- The aggregate uses the same CAF signing key, so the fingerprint remains the same.

CAF Inter-Federation Aggregate metadataURL:

https://caf-shib2ops.ca/CoreServices/caf_interfed_signed.xml

Certificate Fingerprint:

36CFD8090A88B8D75264E790FEA1B6F7ECBECF42C881AAF6F459D3AE3B459304

A new metadataPrefix of:

CAF-Interfed

This configuration will append the necessary command to `sync-ADFSTkAggregates.ps1` in the latest ADFSToolkit home directory, provided you agree to that when asked during the configuration.

```
PS C:\ADFSToolkit> more .\sync-ADFSTkAggregates.ps1

$cmd=get-module -ListAvailable adfstoolkit; Import-module $cmd

Import-ADFSTkMetadata -ProcessWholeMetadata -ForceUpdate -ConfigFile 'C:\Program Files\WindowsPowerShell\Modules\ADFSToolkit\0.9.1.35\config\config.CAF.xml'

#Updated as of: 01/16/2018 02:47:03

Import-ADFSTkMetadata -ProcessWholeMetadata -ForceUpdate -ConfigFile 'C:\Program Files\WindowsPowerShell\Modules\ADFSToolkit\0.9.1.35\config\config.CAF-interfed.xml'

#Updated as of: 01/16/2018 03:15:03

PS C:\ADFSToolkit>
```

Figure 4 - sync-ADFSTkAggregates.ps1 after Your Second Configuration is Complete

4.9 Loading the CAF Inter-Federation Aggregate

To load the Inter-Federation Aggregate, simply re-execute the [sync-ADFSTkAggregates.ps1](#) command in the latest ADFSToolkit home directory and observe the output on the screen or via the Event Viewer in the ADFSToolkit event log.

Note: *Since the Inter-Federation Aggregate is significantly larger, you should expect execution time to run between 45-60 minutes.*

The CAF Inter-Federation Aggregate consists of more than 1100 entities (30 MB). To avoid congestion or latency with AD FS, the ADFSToolkit batches the entity import creation process using a default of 80 entities created per batch.

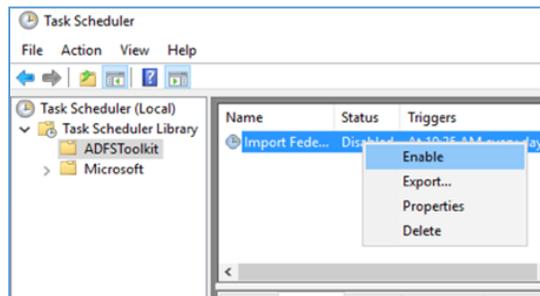
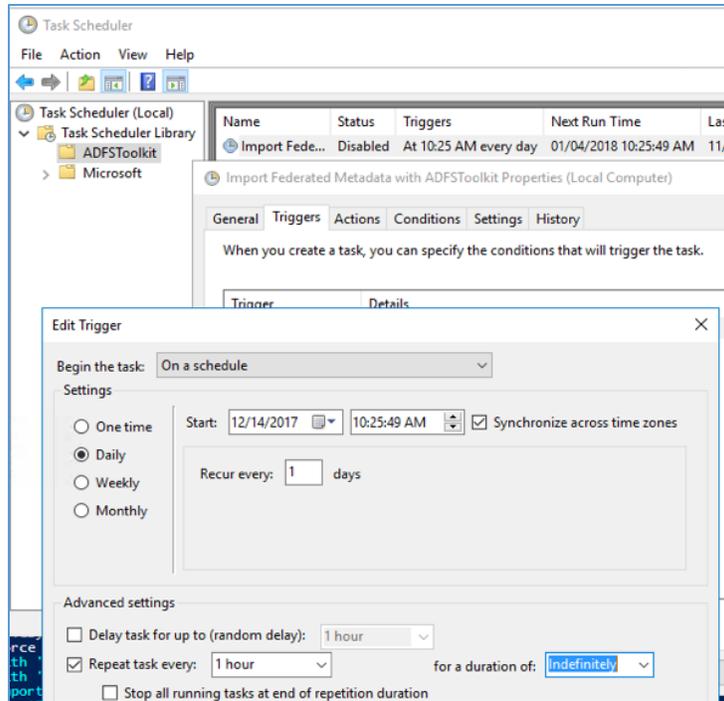
```
1/16/2018 3:45:44 AM: Adding https://sgw.garr.it/shibboleth as SP...
1/16/2018 3:45:45 AM: Successfully added 'https://sgw.garr.it/shibboleth!'
1/16/2018 3:45:45 AM: Adding https://sgw.africa-grid.org/shibboleth as SP...
1/16/2018 3:45:45 AM: Successfully added 'https://sgw.africa-grid.org/shibboleth!'
1/16/2018 3:45:46 AM: Adding https://wifi.dir.garr.it:12081/shibboleth as SP...
1/16/2018 3:45:46 AM: Successfully added 'https://wifi.dir.garr.it:12081/shibboleth!'
1/16/2018 3:45:47 AM: Done!
1/16/2018 3:45:47 AM: Working with batch 3/23 with C:\Program Files\WindowsPowerShell\Modules\ADFSToolkit\0.9.1.35\ADFSToolkit.psml
1/16/2018 3:45:48 AM: Import-ADFSTkMetadata path: C:\ADFSToolkit
1/16/2018 3:45:48 AM: Setting SHashFile to: C:\Program Files\WindowsPowerShell\Modules\ADFSToolkit\0.9.1.35\cache\CAF-interfed-SHashFile.xml
1/16/2018 3:45:48 AM: Setting CachedMetadataFile to: C:\Program Files\WindowsPowerShell\Modules\ADFSToolkit\0.9.1.35\cache\CAF-interfed-metadata.cached.xml
1/16/2018 3:45:49 AM: Metadata file size is 34998045
1/16/2018 3:45:49 AM: Comparing aggregate certificate hash of: @{Algorithm=SHA256; Hash=36CFD8090A88B8D75264E790FEA1B6F7ECBECF42C881AAAF6F459D3AE3B459304; Path=}.Hash to 36CFD8090A88B8D75264E790FEA1B6F7ECBECF42C881AAAF6F459D3AE3B459304
```

Figure 5 - Example of the Automatic Batch Loading by ADFSToolkit

4.10 Scheduling sync-ADFSTkAggregates to Run

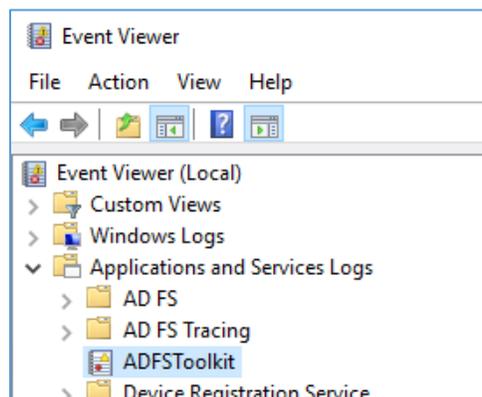
ADFSToolkit automatically creates a scheduled job with a default status of “Disabled”, allowing you to make edits to the configuration settings and to test them before enabling the automatically scheduled operation.

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



4.11 Reviewing Runtime Logs

ADFSToolkit 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.



5 Configuring Attribute Release

ADFSToolkit externalizes attribute release settings per Relying Party (RP) away from AD FS by housing the attribute release policies in a single PowerShell script file located in 'config' subdirectory of the latest ADFSToolkit home directory (c:/ADFSToolkit/###.##/config/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

~<latest_ADFSToolkit_home_dir>/config/get-
ADFSTkLocalManualSPSettings.ps1
```

It is possible to see examples of settings through the Microsoft PowerShell get-help function once you have dot sourced the PowerShell to make the command available:

```
PowerShell

. ~<latest_ADFSToolkit_home_dir>/config/get-
ADFSTkLocalManualSPSettings.ps1
Get-help get-ADFSTkLocalManualSPSettings -Detailed
```

```
PS C:\ADFSToolkit\0.9.1.60\config> . .\get-ADFSTkLocalManualSpSettings.ps1
PS C:\ADFSToolkit\0.9.1.60\config> get-help get-ADFSTkLocalManualSPSettings -Detailed
NAME
get-ADFSTkLocalManualSPSettings

SYNOPSIS
This is the file that site admins edit to locally control per Relying Party/Service provider attribute release.
ADFSToolkit attempts to detect the presence of variable ADFSTkSiteSPSettings and then ingest it to control specific rules.
```

6 ADFSToolkit Operational Behaviour

ADFSToolkit (PowerShell Module) is designed for one installation per machine. Attempting to install multiple live instances of ADFSToolkit on a single host with different versions is not recommended or supported. During the Update-Module phase, multiple versions will exist. Once you have migrated to the new version, before resuming service we recommend moving the old directory (version) out of the default location that Powershell examines when it runs.

The modular design of ADFSToolkit 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 [ADFSTkLocalManualSPSettings.ps1](#) in the latest ADFSToolkit home config sub-directory 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.
- The script [ADFSTkLocalManualSPSettings.ps1](#) is used in one installation and is shared regardless of which aggregate is processed.
 - This means that attribute release for ANY number of aggregates is centralized in one file and there is no need to make a copy for a different job.
- **IMPORTANT:** When you have completed editing [ADFSTkManualSPSettings.ps1](#), you **MUST** re-issue the Import-Module ADFSToolkit 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).

6.1 ADFSToolkit's Lifecycle Management

ADFSToolkit's Module uses the PowerShell Gallery tool command '[Update-Module](#)' to manage delivery of updates. Sites using ADFSToolkit are strongly encouraged to have a test system to review changes between versions. In cases where there is no test system, a snapshot/backup of their environment is strongly recommended.

Note that some updates may require removing the cache files and running again completely to apply new features. Updates that require this will be flagged as such in the release notes. It is up to the site operator to determine when to do this and to allow for sufficient time to recalculate the new, improved settings. ADFSToolkit is designed to be idempotent in its operation, which means that no matter how many times it is run, the resulting set will be the same.

The process to handle an update of ADFSToolkit is to:

- Back up the [C:\ADFSToolkit](#) directory
- Create a system snapshot/recovery point to return to
- Disable/suspend the ADFSToolkit scheduled job
- Issue 'Update-Module ADFSToolkit'
 - When Update-Module is run, it will attempt to detect if there is a newer version available from PowerShellGallery.com and download it.
 - Note that each module is downloaded into its own directory containing the version number of the script. ADFSToolkit will not run properly with more than one version available; once the new version is confirmed on disk and available, we recommend moving the older version out of the PowerShell path so that only the latest version is available.
- **Migrate existing configuration file and related cache files**
 - This is possible but if you hand edited the settings before, you need to re-apply the same edits to the new configuration file format. There are two ways to do this:
 - Create the configuration first, entering answers by hand
 - OR
 - Take advantage of the pipelining features of New-ADFSTkConfiguration, which can ingest your existing configuration and fetch many of the existing settings and bring them into the new format.

Regardless of which strategy chosen to recreate the configuration file, you will still need to inspect to ensure your hand edits were fully applied.

Example of pipelining your old configuration into the new is below:

```
PowerShell
"C:\ADFSToolkit\0.9.1.55\config\config.CAF.xml" | New-ADFSTkConfiguration
```

Once you have completed the review of the settings in configurations from the old configuration to the new configuration you can continue.

- **Determine migrating caches from old to new.**
 - A sub-directory called 'cache' in the live ADFSToolkit home is used to track changes in metadata and save time re-calculating entity records in ADFS.
 - It is possible to copy the cache from the old version to the new one to preserve current processing status.
 - If there are major changes in how ADFSToolkit processes records, it is recommended to permit ADFSToolkit to recreate the cache. The cache is automatically refreshed if the 'cache' directory is empty.
- **Migrate site-specific overrides**
 - The file `c:\ADFSToolkit\#.#.#.#\get-ADFSTkLocalManualSpSettings.ps1` contains all your local settings. Review the release notes and if no instructions are available, simply copy the file from the old version to the new one.
 - If you do not copy this file into the newly created folder with the latest version of the ADFSToolkit job, all your settings for existing entities will be removed.
- **Resuming synchronization of Metadata**
 - Once manual operation has been validated, the ADFSToolkit job should be validated for:
 - using the new `sync-ADFSTkAggregates.ps1` file
 - using the latest configuration file
 - Once this is done, the ADFSToolkit job can be resumed in the Microsoft Job Scheduler and your migration is considered complete.

6.2 Testing with CAF Test Federation

CAF has a test federation that CAF participants are encouraged to use. This test federation has its own discovery service and a test service provider that should be used to test your IdP installation. To join the test federation, send a request to tickets@canarie.ca and include your metadata (if it has not already been sent).

7 Connecting to FIMS Production

Once you have fully completed verifying your installation, your institution's authorized CAF technical contact (identified in the application to join CAF) must contact CANARIE at tickets@canarie.ca and indicate that your institution is ready to connect your site to the CAF FIM service.

The following information must be included in the email to tickets@canarie.ca:

- Your entityid
 - usually '<http://fs.yourschoolname.ca/adfs/services/trust>'
- The name of your organization or institution
- The display name for your organization
 - This will be how your institution is seen in pick lists for discovery purposes
- A short description of your organization
- A URL for the logo of your organization
 - URL should be served via SSL, usually from your IdP itself
 - image size should be 100x100 pixels
- The domain over which you have authority
 - this will be your official scope in CAF metadata
- Your entity metadata URL to retrieve your metadata
 - <https://fs.yourschoolname.ca/FederationMetadata/2007-06/FederationMetadata.xml> will be presumed otherwise
- Appropriate contact information for:
 - one role-based help desk account with
 - a phone number and an email
 - one or more personal technical contacts with
 - a phone number and an email