

SharePoint Security Pre-Trimmer 3.2

On this page:

- [Requirements](#)
- [Installation](#)
 - [I. Download and uncompress deployment package](#)
 - [II. Configure installation settings](#)
 - [III. Run setup script](#)
- [Removal](#)
 - [Manual Removal](#)
 - [Automatic Removal](#)
- [Reconfiguration](#)
- [FAQ & Troubleshooting](#)
 - [Can the Security Pre-Trimmer be Hosted on a Separate Server?](#)
 - [Security Pre-Trimmer is Never invoked](#)
 - [Search Not Working At All](#)
 - [Verify That the Trimmer is Installed](#)

SharePoint Security Pre-Trimmer

Currently Supporting:	SharePoint 2013 and 2016 Aspire Group Expander 3.2
------------------------------	---

Security trimming is available within SharePoint itself. To make this work, a SecurityTrimmerPre interface must be created.

The ISecurityTrimmerPre interface adds claims to the query prior to the security trimming, so it executes "pre" (prior to) the security trimmer. With the exception of *deny ACLs*, the function of the ISecurityTrimmerPre module is to always add results to the result set, rather than to remove them. In this sense, it is the opposite of a security trimmer.



It is critical to understand that if the ISecurityTrimmerPre interface malfunctions, then you get no secure search results. (If it performed "classic" security trimming and malfunctioned, then you would get back extra unauthorized results.) On each search request, the Security Pre-Trimmer is invoked to enhance the search query with ACL information. This information is retrieved from an Aspire Group Expander (LDAP, Lotus Notes ...)

Requirements

The following items are required by this component:

- SharePoint 2013 or SharePoint 2016
- Group Expansion REST Service



A separate service from group expansion can be used if:

- It is a REST endpoint that accepts the parameter username.
- The response is an xml with the same format as this one.

URL Request

- For example, <http://call-to-a-different-service:1234/getGroups?username=admin>

XML Response

```
<groups>
  <group>tesla</group>
  <group>scientists</group>
  <group>italians</group>
  <group>group1</group>
  <group>group2</group>
  <group>group3</group>
  <group>group4</group>
  <group>PUBLIC:ALL</group>
  <group>xxxxxx</group>
</groups>
```

Installation

I. Download and uncompress deployment package

1. Get the latest deployment package from [here](#).
2. Download and uncompress.

II. Configure installation settings

Configure the setup settings in the **configurationParameters.xml** file located under **Deploy\config**.

```
<securityTrimmer>
  <inputs>
    <groupExpansionService>http://HOST:PORT/groupExpansion</groupExpansionService>
    <groupExpansionTimeout>6000</groupExpansionTimeout>
    <useDomain>false</useDomain>
    <claimIssuer>aspire</claimIssuer>
    <searchApplicationName>Search Service Application</searchApplicationName>
    <id>1</id>
    <assemblyVersion>x.x.x.x</assemblyVersion>
    <userProfileWebApp>[WEB APPLICATION URL]</userProfileWebApp>
    <!-- Valid values: INFO, WARN, ERROR -->
    <minimumEventLevel>INFO</minimumEventLevel>
  </inputs>
</securityTrimmer>
```

The Security Trimmer section defines the properties that the Trimmer component needs to access the group expansion service in order to verify the claims of a user requesting documents.

Field	Description
Group Expansion Service	Url of the Aspire Group Expansion service
Group Expansion Timeout	Timeout to wait for Group Expansion response
Use Domain	Use domain in security trimmer
Claim Issuer	If you are using "Use Aspire" option in the SharePoint2013 Publisher, type "aspire"
Search Application Name	Name of the Search Application
Id	The trimmer instance Id in SharePoint. Default is 1.
Assembly Version	Version of the trimmer dll registered on the GAC
User Profile Web App	Specifies the url of a custom ACL service. Leave empty to use Aspire.
Minimum Event Level	Specifies what level of logging should the trimmer use

III. Run setup script

1. Install the Security Pre-Trimmer on all servers hosting a Query Processing component. Check this from SharePoint Central Administration > Manage Service Applications > Search Service Application.
2. Make sure all firewalls to the Aspire server are open for the Aspire service port (default: 50505).
3. From the **Deploy\scripts** folder, run the corresponding **DeployAspireSecurityTrimmer** script in a SharePoint Management Shell (run as Administrator):

```
.\DeployAspireSecurityTrimmer_2013.ps1 -configurationFilePath ..\config\configurationParameters.xml
.\DeployAspireSecurityTrimmer_2016.ps1 -configurationFilePath ..\config\configurationParameters.xml
```

4. To make sure the security trimmer DLL is registered correctly, restart the **SharePoint Search Host Controller** service.



Consider that default value **public** for the **claimIssuer** field in the securityTrimmer section will make all the documents visible. This applies for both configuration files, the main and the one defined for every connector configured for SharePoint.


Removal

Manual Removal

1. Open your preferred internet explorer (IE, Chrome, Firefox, etc) with the "Run as Administrator" option. Otherwise, you will not be able to accomplish the next two steps due to a SharePoint error.
2. Go to **SharePoint Central Admin > System Settings > Manage Farm Solutions**
3. Select **aspiresecuritytrimmer.wsp** and **Retract Solution**.
4. In the following page, make sure the option under *Retract When?* is set to **Now**.
5. Select **OK**.

Automatic Removal

1. Open SharePoint Management Shell as administrator.

 A machine and farm administrator user is needed for this.

2. Go to the Deploy\scripts directory.
3. Run the following:

```
.\UninstallAspireSecurityTrimmer.ps1 -configurationFilePath ..\config\configurationParameters.xml
```

Reconfiguration

To reconfigure the Pre-Trimmer follow the next steps:

1. Retrieve the current settings in the SharePoint Management Shell

```
PS C:\> $ssa = Get-SPEnterpriseSearchServiceApplication
PS C:\> Get-SPEnterpriseSearchSecurityTrimmer -SearchApplication $ssa

SearchApp      : SearchServiceApplication Name=Search Service Application
Id             : 1
TypeName       : AspireSecurityTrimmer.AspireSecurityPreTrimmer, AspireSecurityTrimmer, Version=1.0.0.0,
                Culture=neutral, PublicKeyToken=e87e053e181b45ec
Properties     : ge-http://localhost:50505/groupExpansion~geTimeout~15000~claimIssuer~aspire~useDomain~false~
IsPrePhase    : True
CrawlRulePath : {0}{}

```

2. Remove the Security Pre-Trimmer using the Id from the previous step as Identity by running the following command:

```
Remove-SPEnterpriseSearchSecurityTrimmer -SearchApplication $ssa -Identity <id goes here>
```

3. Re-register the Security Pre-Trimmer with the necessary changes (i.e. increased timeout)

```
New-SPEnterpriseSearchSecurityTrimmer -Id 1 -TypeName "AspireSecurityTrimmer.AspireSecurityPreTrimmer,
AspireSecurityTrimmer, Version=1.0.0.0, Culture=neutral, PublicKeyToken=e87e053e181b45ec" -SearchApplication
$ssa -Properties "ge-http://localhost:50505
/groupExpansion~geTimeout~2000~claimIssuer~aspire~useDomain~false~"
```

4. Restart the SharePoint Search Host Controller service (*spsearchhostcontroller*) now.

FAQ & Troubleshooting

Can the Security Pre-Trimmer be Hosted on a Separate Server?

It is not recommended. There are content sources, such as Lotus Notes, that use Intersection ACLs, which requires that Group Expansion is executed in the same server where the content source is.

Security Pre-Trimmer is Never invoked

If there is no activity on the Aspire group expansion servlet when searches are executed, check the SharePoint log files. Look for an exception like:

```
Microsoft.Office.Server.Search.Query.Ims.Security.SecurityTrimmerSetup : Failed to setup trimmers for the trimmer type: AspireSecurityTrimmer.AspireSecurityPreTrimmer, AspireSecurityTrimmer, Version=1.0.0.0, Culture=neutral, PublicKeyToken=e87e053e181b45ec
```

Debug the Security Pre-Trimmer

Try to initialize the Security Pre-Trimmer manually using PowerShell (make sure to use the correct AspireSecurityTrimmer version in the Add-Type command):

```
Add-Type -AssemblyName "AspireSecurityTrimmer, Version=1.0.0.0, Culture=neutral, PublicKeyToken=e87e053e181b45ec"
$ast = New-Object AspireSecurityTrimmer.AspireSecurityPreTrimmer
$nvc = New-Object System.Collections.Specialized.NameValueCollection
$nvc.Add("ge", "http://aspire:50505/groupExpansion")
$nvc.Add("geTimeout", "15000")
$nvc.Add("claimIssuer", "aspire")
$nvc.Add("useDomain", "false")
$ssa = Get-SPEnterpriseSearchServiceApplication
$ast.Initialize($nvc, $ssa)
```

Then, check the content of the error objects:

```
$error[0]
$error[0].Exception
$error[0].Exception.InnerException
```

Check Event Log Permissions

In the windows registry, make sure that the user running the SharePoint Search Host Controller (*spsearchhostcontroller*) service, has permissions for this key:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\eventlog
```

Re-Register the Security Pre-Trimmer

Try re-registering the Security Pre-Trimmer. Make sure to restart the SharePoint Search Host Controller (*spsearchhostcontroller*) service after every configuration change.

Search Not Working At All

If Aspire is not running and the Search Center returns with errors, check the Windows Application log for these error messages:

Internal Server Error

```
The remote server returned an error: (500) Internal Server Error.  
at System.Net.HttpWebRequest.GetResponse()  
at AspireSecurityTrimmer.AspireSecurityPreTrimmer.GetAclsFromAspire(String username)
```

Check Aspire for any error messages or exceptions.

Operation Timeout

```
The operation has timed out  
at System.Net.HttpWebRequest.GetResponse()  
at AspireSecurityTrimmer.AspireSecurityPreTrimmer.GetAclsFromAspire(String username)
```

Try to adjust the timeout in the Security Pre-Trimmer configuration. You need to remove and add it again in a SharePoint Management Shell.

Verify That the Trimmer is Installed

1. Open the SharePoint 2013 Management Shell
2. Run the following command: `Get-SPEnterpriseSearchServiceApplication -Identity MySSA | Get-SPEnterpriseSearchSecurityTrimmer`
3. You should see something like this: