

# PingFederate®

## SharePoint 2013 People Picker Extension

Version 1.0

## User Guide



© 2016 Ping Identity® Corporation. All rights reserved.

PingFederate Sharepoint 2013 People Picker Extension User Guide  
Version 1.0  
March, 2016

Ping Identity Corporation  
1001 17th Street, Suite 100  
Denver, CO 80202  
U.S.A.

Phone: 877.898.2905 (+1 303.468.2882 outside North America)

Fax: 303.468.2909

Web Site: [www.pingidentity.com](http://www.pingidentity.com)

## Trademarks

Ping Identity, the Ping Identity logo, PingFederate, PingOne, PingConnect, and PingEnable are registered trademarks of Ping Identity Corporation ("Ping Identity"). All other trademarks or registered trademarks are the property of their respective owners.

## Disclaimer

The information provided in this document is provided "as is" without warranty of any kind. Ping Identity disclaims all warranties, either express or implied, including the warranties of merchantability and fitness for a particular purpose. In no event shall Ping Identity or its suppliers be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages, even if Ping Identity or its suppliers have been advised of the possibility of such damages. Some states do not allow the exclusion or limitation of liability for consequential or incidental damages so the foregoing limitation may not apply.

## Document Lifetime

Ping Identity may occasionally update online documentation between releases of the related software. Consequently, if this PDF was not downloaded recently, it may not contain the most up-to-date information. Please refer to [documentation.pingidentity.com](http://documentation.pingidentity.com) for the most current information.

From the Web site, you may also download and refresh this PDF if it has been updated, as indicated by a change in this date: **March 10, 2016**.

# Contents

- Introduction ..... 4**
  - System Requirements..... 4
  - User Guide Assumptions and Prerequisites..... 4
- Installation ..... 5**
  - Adding the Solution..... 5
  - Deploying the Solution ..... 5
  - Activating Features ..... 5
  - Setting the Default Claims Provider ..... 6
- Configuration..... 7**
  - People Picker Configuration ..... 7
  - Configuration Storage ..... 10
- Diagnostic Logging ..... 11**
- Supported Search Attributes with Examples ..... 13**
  - Search by User ..... 13
  - Search by Group..... 13
- Instructions to Uninstall (Rollback) the solution ..... 15**
- SharePoint Log Location ..... 18**

# Introduction

The People Picker control is a central component in Microsoft SharePoint Server 2013 that is used to search and select users and groups when a resource owner assigns permissions. By default, when a SharePoint web application is configured to use SAML token-based authentication or “SAML claims”, all queries entered in the People Picker are automatically displayed as if they had been resolved, regardless of whether they are valid users or groups. This poses a significant usability problem for SharePoint users and administrators, particularly in collaboration-oriented deployments where potentially every user has the ability to edit file and library permissions using the People Picker.

To address this issue, Microsoft recommends you build a custom claims provider to provide capabilities for custom search and name resolution. The Ping Identity Custom Claims Provider for SharePoint 2013 is an implementation capable of connecting to one or more LDAP user stores or domains to fulfill search and name resolution queries.

When this custom claims provider is associated with a Trusted Login Provider (referred to in the Management Shell as a Trusted Identity Token Issuer) in SharePoint, such as might be configured to accept inbound SAML claims from PingFederate for one or more SharePoint web applications, the People Picker will provide functionality similar to that seen with classic-mode authentication where users and groups in Active Directory are available for search, name resolution, and attribute listing.

## System Requirements

This version of the Ping Identity Custom Claims Provider for SharePoint 2013 requires the following:

- Microsoft SharePoint Server 2013 – specifically an environment that is already configured with PingFederate as the Trusted Identity Token Issuer.
- Connectivity to one or more backing LDAP user stores. Testing has been conducted against Microsoft Active Directory 2008 R2

## User Guide Assumptions and Prerequisites

This document assumes:

- A Trusted Identity Token Issuer, referred to hereon as the Partner STS, has been created and enabled as an Authentication Provider for at least one SharePoint web application.
  - SAML token-based authentication has been successfully tested for the SharePoint web application using the Partner STS
  - The Partner STS is configured to send the user identity claim type that will be used by SharePoint (for example <http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress>)

---

**Note:** Make note of the name of the Partner STS. You will need it when associating the Custom Claims Provider with the Partner STS. You can view all Trusted Identity Token Issuers and their names by executing the following command from the Management Shell: *Get-SPTrustedIdentityTokenIssuer* and looking at the *Name* attribute.

---

- Connectivity and trust (for LDAPS connections) exists to all domain controllers that are to be searched.
- A provisioned service account with read access for each domain controller to be searched is available.
- The Sharepoint Administration service must be running prior to installing the solution (.wsp) file.

## Installation

### Adding the Solution

1. Copy the solution (WSP) file to the SharePoint server.
2. Open the SharePoint Management Shell (PowerShell) as Administrator and use the Add-SPSolution command to add the solution to the farm:

```
Add-SPSolution -LiteralPath  
C:\path\PingIdentity.SharePoint.PPClaimsProvider.wsp
```

### Deploying the Solution

---

**Note:** The solution must be deployed to all servers in the farm including application servers. In some multi-server farms the SharePoint Web Application service (Microsoft SharePoint Foundation Web Application) is only running on web servers. This service must be started on application servers during deployment in order for the solution assembly to be installed on those servers. If the solution assembly is not deployed to application server the claims picker will not work when assigning permissions in the web application user policy.

---




Deploy the solution using Central Adminor using the Install-SPSolution command:

```
Add-SPSolution -LiteralPath Install-SPSolution  
PingIdentity.SharePoint.PPClaimsProvider.wsp -GACDeployment
```

### Activating Features

1. Login to your SharePoint 2013 Central Administration site
2. Go to Central Administration >> System Settings >> Manage farm features
3. Activate the Ping Identity People Picker Claims Provider feature if it is not already Active

## Manage Farm Features

Name	Status
 Offline Synchronization for External Lists Enables offline synchronization for external lists with Outlook and SharePoint Workspace.	Deactivate <b>Active</b>
 Ping Identity People Picker Claims Provider	Deactivate <b>Active</b>
 SharePoint Server to Server Authentication This feature provides the server to server authentication capabilities.	Deactivate <b>Active</b>




---

**Note:** Activating the feature registers the claim provider in SharePoint.

---

4. Click on the gear icon on the top right corner of the Central Admin site
5. Click on Site Settings >> go to Site Actions >> click on Manage site features
6. Activate the Ping Identity People Picker Claims Administration feature

## Site Settings › Site Features

Name	Status
 Features enabling the PerformancePoint Services list and document library templates.	Activate
 Ping Identity People Picker Claims Administration	Deactivate <b>Active</b>
 Project Functionality	...

### Setting the Default Claims Provider

Once the claims provider is installed and activated you can set it as the default claims provider for your PingFederate Partner STS by doing the following:

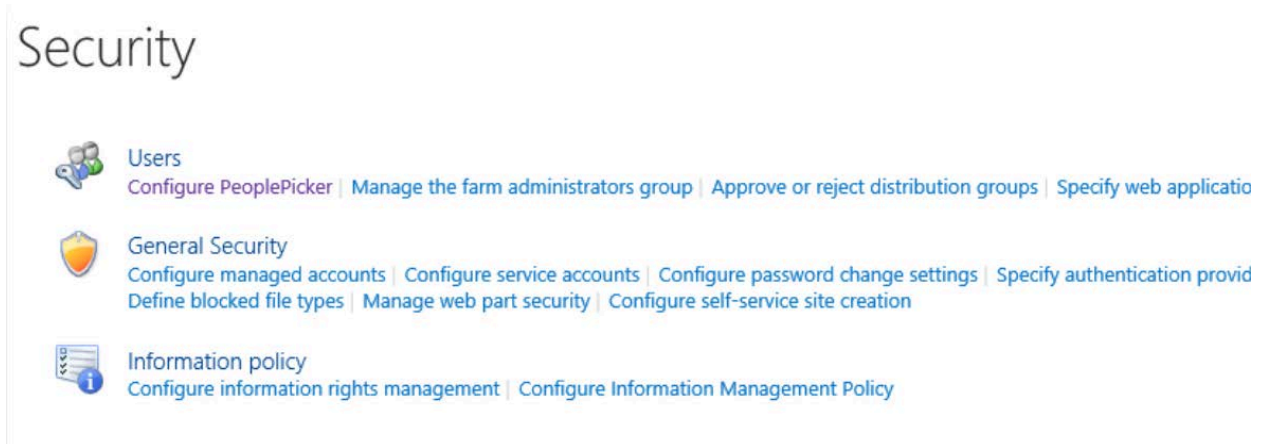
1. Open SharePoint 2013 Management Shell as an Administrator
2. Execute each command listed below
3. Replace "<PartnerSTSName>" with the Name of your configured Trusted Identity Token Issuer

```
$ti = Get-SPTtrustedIdentityTokenIssuer "<Partner STS Name>"
$ti.ClaimProviderName = "PingIdentityPeoplePickerProvider"
$ti.Update()
```

# Configuration

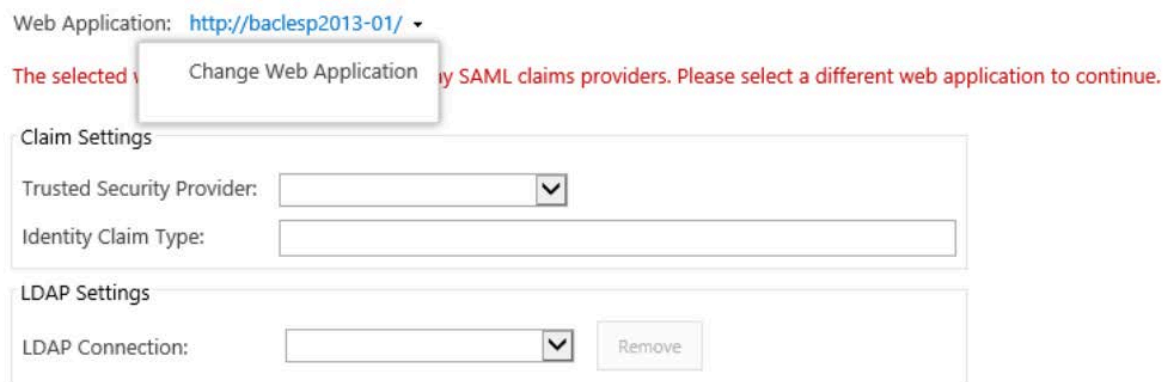
## People Picker Configuration

1. Login to your SharePoint 2013 Central Administration site
2. Go to Central Administration >> Security
3. Click on *Configure People Picker* (under Users)



4. Select the web application that is configured to use the Partner STS (Trusted Identity Provider) for authentication from the drop down at the top of the page)

## Ping Identity Claims Provider Configuration



5. Configure the Claim Settings by selecting the Partner STS and specifying the Identity Claim Type

Identity Claim Type examples:

<http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress>

<http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn>

# Ping Identity Claims Provider Configuration

Web Application: <https://winserv2012vm.local.lab:830/> ▾

Claim Settings

Trusted Security Provider:  ▾

Identity Claim Type:

LDAP Settings

LDAP Connection:  ▾

6. Add LDAP connections by selecting “Add a new connection...” in the drop down, then proceed to fill out the LDAP connection settings as described below



Web Application: <https://winserv2012vm.partnera.com/> ▾

Settings Saved for provider PingFederate

#### Claim Settings

Trusted Security Provider:  ▾

Identity Claim Type:

#### LDAP Settings

LDAP Connection:  ▾

Name:

Server:

Username:

Password:

Search Root:

Identity Attribute:

Server Time Limit (seconds):

Client Timeout (seconds):

Maximum number of objects to return:

Minimum characters to start search:

#### Name

The name of this LDAP connection.

#### Server

The FQDN or IP address for the LDAP server. If using LDAPS, include the relevant port (i.e. ldap.domain.com:636)

#### Username

The username of the LDAP account that will be used to bind to LDAP in order to query users or groups. If the Username field is left blank the LDAP query will be made using the SharePoint farm account.

### Password

The password for the LDAP account.

---

**Note:** Passwords are stored in plain text with the other configuration data.

---

### Search Root

The root (BaseDN) for the LDAP search.

### Identity Attribute

The Identity Attribute refers to the LDAP attribute that is used to populate the Identity Claim Type (which you selected in the Claim Settings at the top of the page). The LDAP attribute configured here must match the LDAP attribute used in PingFederate to populate that WS-Fed attribute.

For example:

LDAP attribute name "Identity Attribute"	Identity Claim Type
userPrincipalName	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn
givenName	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress

### Server Time Limit (seconds)

The maximum number of seconds that the server will wait for a search to complete.

### Client Timeout (seconds)

The maximum number of seconds that the client will wait for the server to return results.

### Maximum number of objects to return

This refers to the maximum number of search results you want the People Picker to return.

- You can set this to a number between 0 and 500.
- If you set this to 0, it will use the SharePoint default size limit of 1000 entries.

### Minimum characters to start search

This refers to the minimum number of characters (letters) an end user must type into the People Picker search window before the search starts to execute.

- You can set this to a number between 4 and 10.
- If you set this to 0, it will use the SharePoint default setting of 3 characters.

---

**Note:** Each LDAP connection you add here will only be enabled for the specific SharePoint web application you selected. If you want to add the same LDAP connection to multiple SharePoint web applications, you will need to repeat the same configuration steps (4-5-6) for each SharePoint web application.

---

## Configuration Storage

Configuration settings are stored in the web application properties collection with the key "PingClaimsProviderConfig". The configuration is stored in JSON format in plain text (unencrypted).

```
$webApp = Get-SPWebApplication <web app URL>  
$webApp.Properties["PingClaimsProviderConfig"]
```

# Diagnostic Logging

Verbose tracing can be enabled for the Ping Identity People Picker on the Diagnostic Logging page of the Monitoring section in Central Administration.

1. Go to Central Administration >> Monitoring >> Reporting >> Configure diagnostic logging
2. Select the Custom Claims category

## Diagnostic Logging

### Event Throttling

Use these settings to control the severity of events captured in the Windows event log and the trace logs. As the severity decreases, the number of events logged will increase.

You can change the settings for any single category, or for all categories. Updating all categories will lose the changes to individual categories.

Select a category

Category	Event Level	Trace Level
<input type="checkbox"/> All Categories		
<input type="checkbox"/> Access Services		
<input type="checkbox"/> Access Services 2010		
<input type="checkbox"/> Business Connectivity Services		
<input type="checkbox"/> Document Conversions		
<input type="checkbox"/> Document Management Server		
<input type="checkbox"/> eApproval		
<input type="checkbox"/> Education		
<input type="checkbox"/> Excel Services Application		
<input type="checkbox"/> InfoPath Forms Services		
<input type="checkbox"/> Office Automation Services		
<input type="checkbox"/> Office Services Infrastructure		
<input type="checkbox"/> PerformancePoint Service		
<input checked="" type="checkbox"/> Ping Identity People Picker		
<input checked="" type="checkbox"/> Custom Claims	Information	Verbose
<input type="checkbox"/> Search		
<input type="checkbox"/> Secure Store Service		

3. (Optional) Select SharePoint Foundation >> Monitoring to enable monitored scopes that will show LDAP queries.

<input type="checkbox"/> Marketplace Web Service	Information	Medium
<input type="checkbox"/> Micro Trace	Information	Medium
<input checked="" type="checkbox"/> <b>Monitoring</b>	Information	<b>Verbose</b>
<input type="checkbox"/> Network Usage	Information	Medium
<input type="checkbox"/> Object Cache	Information	Medium

4. Select Verbose as the least critical event to report to the trace log

Least critical event to report to the event log

Least critical event to report to the trace log

5. Use the ULS Viewer app to monitor the ULS logs. You can use the following filters to see just the output from the custom claims provider

Field	Operation	Value	And/Or
Product	Equals	Ping Identity People Picker	Or
Message	Contains	LdapQuery	And

You can download the ULS Viewer tool from Microsoft here: <https://www.microsoft.com/en-us/download/details.aspx?id=44020>

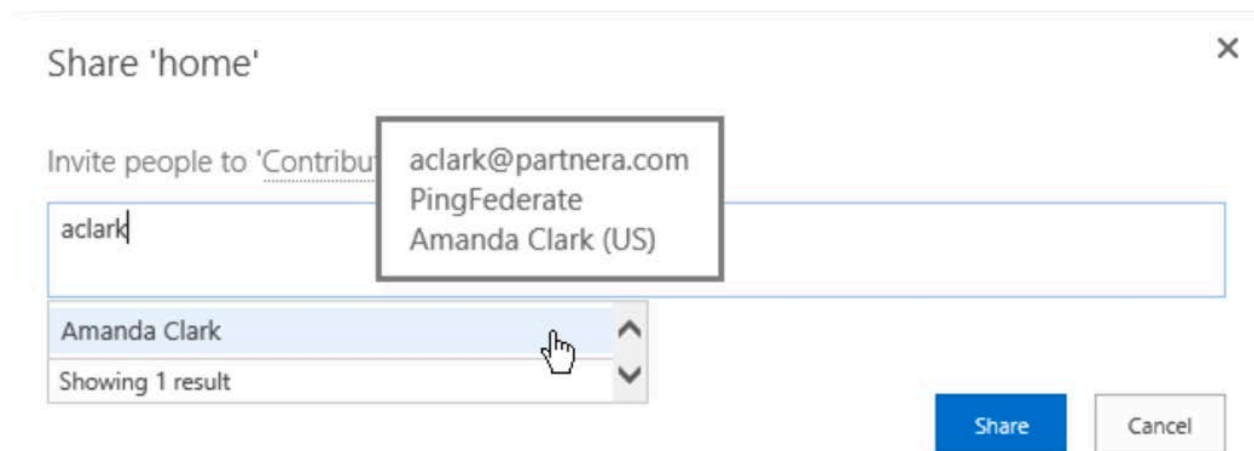
# Supported Search Attributes with Examples

This solution is currently enabled to search for the following LDAP attributes:

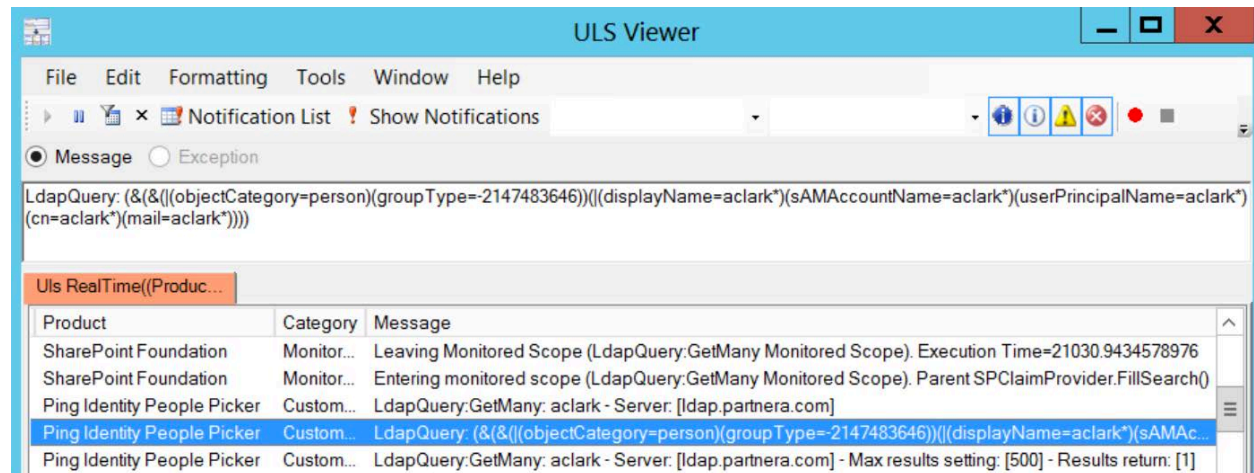
cn  
displayName  
mail  
sAMAccountName  
userPrincipalName

## Search by User

Here is an example of a successful search for a user by username (sAMAccountName):



This is the corresponding log entry for the successful search:



## Search by Group

Here is an example of a successful search for a group by the group's name (cn, sAMAccountName):

## Share 'home'



Invite people to 'Contribute'

Group1

PingFederate  
CN=Group1,CN=Users,DC=partnera,DC=com

PARTNERA\Group1

Showing 1 result

Share Cancel

This is the corresponding log entry for the successful search:

ULS Viewer

File Edit Formatting Tools Window Help

Notification List Show Notifications

Message Exception

LdapQuery: (&((!(objectCategory=person)(groupType=-2147483646))((displayName=Group1\*)(sAMAccountName=Group1\*)(userPrincipalName=Group1\*)(cn=Group1\*)(mail=Group1\*))))

	Product	Category	Message
2.86	Ping Identity People Picker	Custom...	LdapQuery:GetMany: Group1 - Server: [ldap.partnera.com]
2.86	Ping Identity People Picker	Custom...	LdapQuery: (&((!(objectCategory=person)(groupType=-2147483646))((displayName=Group1*)(sAMAccountName=Group1*)(userPrincipalName=Group1*)(cn=Group1*)(mail=Group1*))))
3.85	Ping Identity People Picker	Custom...	LdapQuery:GetMany: Group1 - Server: [ldap.partnera.com] - Max results setting: [500] - Results returned: [1]
3.85	SharePoint Foundation	Monitor...	Leaving Monitored Scope (LdapQuery:GetMany Monitored Scope). Execution Time=990.6756305615

# Instructions to Uninstall (Rollback) the solution

The following steps can be used to remove the Custom Claims Provider (People Picker) solution:

1. In Central Administration disable the Trusted Identity provider from the web application.
  - This step must be completed for each web application that is using that Trusted Identity provider (also known as the Partner STS or Trusted Identity Token Issuer).

## Edit Authentication

### Claims Authentication Types

Choose the type of authentication you want to use for this zone.

Negotiate (Kerberos) is the recommended security configuration to use with Windows authentication. If this option is selected and Kerberos is not configured, NTLM will be used. For Kerberos, the application pool account needs to be Network Service or an account that has been configured by the domain administrator. NTLM authentication will work with any application pool account and with the default domain configuration.

Basic authentication method passes users' credentials over a network in an unencrypted form. If you select this option, ensure that Secure Sockets Layer (SSL) is enabled.

Enable Windows Authentication

Integrated Windows authentication

NTLM

Basic authentication (credentials are sent in clear text)

Enable Forms Based Authentication (FBA)

ASP.NET Membership provider name

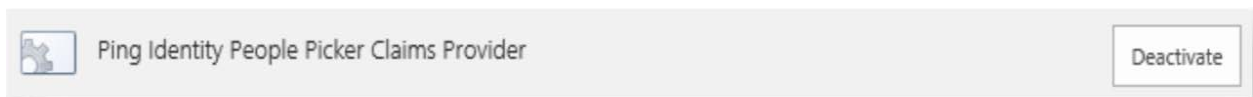
ASP.NET Role manager name

Trusted Identity provider

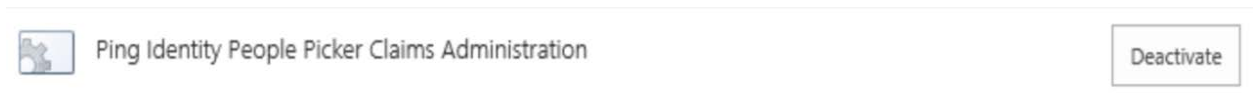
Trusted Identity Provider

PingFederate

2. In Central Administration >> System Settings >> Farm Features >> deactivate the Ping Identity People Picker Claims Provider farm feature.



3. In Central Administration >> Site Settings >> Site Features >> deactivate the Ping Identity People Picker Claims Administration site feature.



- In Central Administration >> System Settings >> Farm Solutions >> retract the pingidentity.sharepoint.ppclaimsprovider.wsp solution.

---

**Note:** The SharePoint Administration service must be running in order for this retraction to be successful.

---

## Solution Properties

[Retract Solution](#) [Back to Solutions](#)

Name:	pingidentity.sharepoint.ppclaimsprovider.wsp
Type:	Core Solution
Contains Web Application Resource:	No
Contains Global Assembly:	Yes
Contains Code Access Security Policy:	No
Deployment Server Type:	Front-end Web server
Deployment Status:	Deployed
Deployed To:	Globally deployed.

- In Central Administration >> System Settings >> Farm Solutions >> remove the pingidentity.sharepoint.ppclaimsprovider.wsp solution.



# Solution Properties

[Deploy Solution](#) [Remove Solution](#) [Back to Solutions](#)

Name:	pingidentity.sharepoint.ppclaimsprovider.wsp
Type:	Core Solution
Contains Web Application Resource:	No
Contains Global Assembly:	Yes
Contains Code Access Security Policy:	No
Deployment Server Type:	Front-end Web server
Deployment Status:	Not Deployed

6. Open SharePoint 2013 Management Shell as an Administrator
7. Make a backup copy of your configuration settings for your existing Trusted Identity Token Issuer. For example: use this command to produce a file called partnersts.txt that contains your list of token issuers and their settings:  
`Get-SPTrustedIdentityTokenIssuer >partnersts.txt`
8. Use this command to delete your current Trusted Identity Token Issuer:  
`Remove-SPTrustedIdentityTokenIssuer -Identity '<PartnerSTS>'`  
Replace <PartnerSTS> with the Name of your Trusted Identity Token Issuer.
9. Use PowerShell to recreate your SP Trusted Identity Token Issuer (without setting the default claims provider). You can refer to the partnersts.txt to review what settings you used previously.
10. In Centralt Administration reconfigure the web application to use the newly created SPTrustedIdentityTokenIssuer.
11. (Optional) For a complete cleanup, you may also wish to remove the People Picker configuration settings that were stored for each web application that you configured to use the People Picker. This can be done by running the following commands via the SharePoint 2013 Management Shell for each web application:
  - Identify the web application by replacing <web app URL> with the SharePoint Web Application's URL  
`$webApp = Get-SPWebApplication <web app URL>`
  - To view the settings associated for the web application:  
`$webApp.Properties['PingClaimsProviderConfig']`
  - To remove the settings associated for the web application:  
`$webApp.Properties.Remove['PingClaimsProviderConfig']`

## SharePoint Log Location

The default log directory will be similar to this path: C:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\15\LOGS

If the Sharepoint admin has changed the default log path, you can find it by going to Central Admin >> Monitoring >> Reporting >> Configure diagnostic logging >> scroll down to Trace Log - the Path configured here is where your Sharepoint Logs are being stored.