Google Search Appliance Connectors
Deploying the Connector for SharePoint User Profiles

Google Search Appliance Connector for SharePoint User Profiles software version 4.1.1
Google Search Appliance software versions 7.4 and 7.6

January 2017
Table of Contents

About this guide

Overview of the GSA Connector for SharePoint User Profiles
  Automatic updates every 15 minutes
  Supported SharePoint versions
  Supported operating systems for the connector
  Supported authentication mechanisms
  Known connector limitation
  CPU and memory recommendation

Before you deploy the Connector for SharePoint User Profiles

Deploy the Connector for SharePoint User Profiles
  Step 1 Configure the search appliance
    Add the URL
    Add the IP address
    Create and configure a collection
    Set up security
  Step 2 Install the Connector for SharePoint User Profiles
    Windows Installation
    Command-line installation for Linux or Windows
    HTTPS configuration
  Step 3 Configure adaptor-config.properties variables
  Step 4 Run the Connector for SharePoint User Profiles

Uninstall the Google Search Appliance Connector for SharePoint User Profiles

Troubleshoot the Connector for SharePoint User Profiles
About this guide
This guide is intended for anyone who needs to deploy the Google Search Appliance Connector 4.1.1 for SharePoint User Profiles. The guide assumes that you are familiar with Windows or Linux operating systems and configuring the Google Search Appliance by using the Admin Console.

See the [Google Search Appliance Connectors Administration Guide](#) for general information about the connectors, including:

- What's new in Connectors 4?
- General information about the connectors, including the configuration properties file, supported ACL features, and other topics
- Connector security
- Connector logs
- Connector Dashboard
- Connector troubleshooting

For information about using the Admin Console, see the [Google Search Appliance Help Center](#).

For information about previous versions of connectors, see the [Connector documentation page](#) in the [Google Search Appliance Help Center](#).
Overview of the GSA Connector for SharePoint User Profiles

The Connector for SharePoint User Profiles enables you to crawl and index information about users in the SharePoint User Profile Service Application. Once the search appliance has indexed this information, it can use it in the expert search feature.

Expert search enables your users to find experts in your organization by searching on keywords. For detailed information about this feature, see the help page for Search > Search Features > Expert Search.

A single instance of the Connector for SharePoint User Profiles can have GSA index a single SharePoint web application. Each SharePoint web application can share the same SharePoint User Profile Service application.

The following diagram provides an overview of how the search appliance gets content (user profiles) from SharePoint through the connector. For explanations of the numbers in the process, see the steps following the diagram.

1. The Connector for SharePoint User Profiles starts communicating with the repository by presenting authentication credentials.
2. The repository sends Doc IDs of documents in the repository to the connector.
3. The connector constructs URLs from the Doc IDs and pushes them to the search appliance in a metadata-and-URL feed. Take note that this feed does not include the document contents.
4. The search appliance gets the URLs to crawl from the feed.
5. The search appliance crawls the repository according to its own crawl schedule, as specified in the GSA Admin Console. It crawls the content by sending GET requests for content to the connector.
6. The connector requests the content from the repository.
7. The repository sends the content to the connector.
8. The connector pushes the content to the search appliance for indexing.

**Automatic updates every 15 minutes**
After the initial process completes, the connector periodically informs the search appliance of new documents and changed documents, according to the value set in the connector configuration option `adaptor.incrementalPollPeriodSecs`. The default interval value is 15 minutes, but you can configure it to suit your needs. For more information, see “Common configuration options” in the Administration Guide.

**Supported SharePoint versions**
The Connector for SharePoint User Profiles 4.1.1 supports the following SharePoint versions:

- SharePoint 2016
- SharePoint 2013
- SharePoint 2010

**Supported operating systems for the connector**
The Connector for SharePoint User Profiles 4.1.1 must be installed on one of the following supported operating systems:

- Windows Server 2012
- Windows Server 2008 (32 and 64 bit)
- Windows Server 2003 (32 and 64 bit)
- Ubuntu
- Red Hat Enterprise Linux 5.0
- SUSE Enterprise Linux 10 (64 bit)
Supported authentication mechanisms
The Connector for SharePoint User Profiles 4.1.1 supports any authentication mechanism where a verified user ID is rendered.

Known connector limitation
Supports one connector instance per User Profile Service Application instance.

CPU and memory recommendation
The recommended configuration for the Connector for SharePoint User Profiles is 4 GB RAM and 4 core CPU.
Before you deploy the Connector for SharePoint User Profiles

Before you deploy the Connector for SharePoint User Profiles, ensure that your environment has all of the following required components:

- GSA software version 7.2.0.G.264 or higher
  To download GSA software, visit the Google for Work Support Portal (password required).
- Java JRE 1.7u9 or higher installed on computer that runs the connector.
  If you want to use the DH (Diffie-Hellman) style of encryption and you are running the GSA with 2048-bit encryption, JRE 1.7u80 or 1.8.0_20 is required.
- Connector for SharePoint User Profiles 4.1.1 JAR executable
  For information about finding the JAR executable, see Step 2 Install the Connector for SharePoint User Profiles.
- User account for the connector, with Full Control permissions to SharePoint User Profile Service Application
- If running the connector on Windows Server 2008, Windows Server 2008 R2 or Windows Server 2012 machine, specify the LAN Manager Authentication Level Policy.

Optionally, configure the search appliance for the authentication method in use (typically LDAP for Active Directory). For detailed information about configuring authentication, see Managing Search for Controlled Access-Content.
Deploy the Connector for SharePoint User Profiles

Because the Connector for SharePoint User Profiles is installed on a separate host, you must establish a relationship between the connector and the search appliance.

To deploy the Connector for SharePoint User Profiles, perform the following tasks:

1. **Configure the search appliance**
2. **Install the Connector for SharePoint User Profiles**
3. Optionally, **configure adaptor-config.properties variables**
4. **Run the Connector for SharePoint User Profiles**

**Step 1 Configure the search appliance**

For the search appliance to work with the Connector for SharePoint User Profiles, the search appliance needs to be able to crawl information about users in the SharePoint User Profile Service Application via connector and accept feeds from the connector. Once indexed by the search appliance, SharePoint User Profile information has to reside in a collection that contains only profile information.

To set up these capabilities, perform the following tasks by using the search appliance Admin Console:

1. **Add the URL** provided by the connector to the search appliance's follow patterns.
2. **Add the IP address** of the computer that hosts the connector to the list of Trusted IP addresses so that the search appliance will accept feeds from this address.
3. **Create and configure a collection** for user profile information.
4. **Set up security**.

**Add the URL**

To add the URLs provided by the connector to the search appliance's crawl configuration follow patterns:

1. In the search appliance Admin Console, click **Content Sources > Web Crawl > Start and Block URLs**.
2. Under **Follow Patterns**, add the URL that contains the hostname of the machine that hosts the connector and the port where the connector runs.
   For example, you might enter `http://connector.example.com:5678/doc/` where `connector.example.com` is the hostname of the machine that hosts the connector.
   By default the connector runs on port 5678.
3. Click **Save**.
Add the IP address
To add the IP address of the computer that hosts the connector to the list of trusted IP addresses:

1. In the search appliance Admin Console, click Content Sources > Feeds.
2. Under List of Trusted IP Addresses, select Only trust feeds from these IP addresses.
3. Add the IP address for the connector to the list.
4. Click Save.

Create and configure a collection
To create and configure a collection for user profile information:

1. In the search appliance Admin Console, click Index > Collections.
2. In the Create New Collection section, enter a unique name for the new collection.
3. For Initial Configuration, select Empty and click Create.
4. In the Current Collections section, click Edit for the newly-created user profile collection.
5. In the Include Content Matching the Following Patterns box, add the URL pattern for the connector, for example http://connector.example.com:5678/doc/.
6. Configure the default_collection to exclude user profile documents. In the Current Collections section, click Edit for default_collection.
7. In the Do Not Include Content Matching the Following Patterns box, add the URL pattern for the connector (see step 5).
8. Click Save.

Set up security
For information about setting up security, see “Enable connector security” in the Administration Guide.
Step 2 Install the Connector for SharePoint User Profiles

This section describes the installation process for the Google Search Appliance Connector for SharePoint User Profiles on the connector host computer. This connector version does not support installing the connector on the Google Search Appliance.

You can install the Connector for SharePoint User Profiles on any host running one of the supported operating systems.

As part of the installation procedure, you need to edit some configuration variables in the configuration file. Take note that you can encrypt the value for `sharepoint.password` before adding it to the file by using the Connector Dashboard or standalone command line program, as described in “Encode sensitive values,” in the Administration Guide.

Windows Installation

To install the Connector for SharePoint User Profiles on Windows:

1. Log in to the computer that will host the connector by using an account with sufficient privileges to install the software.
2. Start a web browser.
   Download the `exe` file by clicking on Microsoft SharePoint User Profiles in the Windows Installer table.
   You are prompted to save the single binary file, `spup-install-4.1.1.exe`.
4. Start installing the file by double clicking `spup-install-4.1.1`.
5. On the Introduction page, click Next.
6. On the GSA Hostname and other required configuration values page, enter values for the following options:
   a. **GSA Hostname or IP address** of the GSA that will use the connector.
      For example, enter `yourgsa.example.com`
   b. **SharePoint Server**.
      For example, enter `http://yoursharepoint.example.com/`
   c. **Adaptor port number** for any crawlable documents this connector serves.
      Each instance of a Connector on same machine requires a unique port. The default is 5778.
d. **Server dashboard port** for the Connector Dashboard. The value is the port on which to view web page showing information and diagnostics about the connector. The default is 5779. You can edit this value and set it to any value that is different from the Adaptor port number (server.port).

e. Enter the **Maximum Java Heap size (in megabytes)**. Default is 1024.

f. Whether or not to run the connector after the installer finishes.

7. Click **Next**.

8. On the **Choose Install Folder** page, accept the default folder or navigate to the location where you want to install the connector files.

9. Click **Next**.

10. On the **Choose Shortcut Folder**, accept the default folder or select the locations where you want to create product icons.

11. To create icons for all users of the Windows machine where you are installing the connector, check **Create Icons for All Users** and click **Next**.

12. On the **Pre-Installation Summary page**, review the information and click **Install**. The connector installation process runs.

13. On the **Install Complete** page, click **Done**. If you selected the option to run the connector after the installer finishes, the connector starts up in a separate window.

When SharePoint and the current user domain is the same or from the same domain hierarchy, Windows operating systems automatically use the credentials of the person currently signed on to Windows.

If not, you need to specify a username and password. For example, suppose that you run the connector from a corporate domain such as @mycompany.com against a SharePoint instance from another domain, such as GSA-CONNECTORS. In this case, you need to specify user credentials for GSA-CONNECTORS domain.

14. If the adaptor needs to use Live Authentication to connect to SharePoint, then add these additional configuration options to **adaptor-config.properties**:

```
sharepoint.username=AdaptorUser Live Authentication Id
sharepoint.password=uS3R_passWoRD
sharepoint.useLiveAuthentication=true
```
15. If the adaptor needs to use ADFS Authentication to connect to SharePoint, then add these additional configuration options to `adaptor-config.properties`:

```properties
sharepoint.username=AdaptorUser@yourdomain.com
sharepoint.password=uS3R_passWoRD
sharepoint.sts.endpoint=https://adfs.example.com/adfs/services/trust/2005/usernamemixed
sharepoint.sts.realm=urn:myserver:sharepoint or https://yoursharepoint.example.com/_trust
```

Command-line installation for Linux or Windows
The following procedure gives the steps for installing the Connector for SharePoint User Profiles on Linux. Take note that if you prefer not to use the Windows installer, you can also follow this procedure to install the Connector on Windows.

To install the connector:

2. Create a directory on the host where the connector will reside. For example, create a directory called `sharepointup-connector_411`.
3. Copy the Connector for SharePoint User Profiles 4.1.1 JAR executable to the directory.
4. Create an ASCII or UTF-8 file named `adaptor-config.properties` in the directory that contains the connector binary.
5. Provide the following configuration (replacing bolded items with your real configuration) within the file:

```properties
gsa.hostname=yourgsa.example.com or IP address
sharepoint.server=http://yoursharepoint.example.com/
```

where the value of `yoursharepoint.example.com` is a fully-qualified domain name. If it is not a fully-qualified domain name, then you must set DNS override on the connector host.
6. **Linux**: Add these additional configuration options to `adaptor-config.properties`:

   ```
   sharepoint.username=YOURDOMAIN\ConnectorUser
   sharepoint.password=user_password
   ```

   **Windows**: When SharePoint and the current user domain is the same or from same domain hierarchy, Windows operating systems automatically use the credentials of the person currently signed on to Windows.

   If not, you need to specify a username and password. For example, suppose that you run the connector from a corporate domain such as @mycompany.com against a SharePoint instance from another domain, such as GSA-CONNECTORS. In this case, you need to specify user credentials for GSA-CONNECTORS domain.

7. Create an ASCII or UTF-8 file named `logging.properties` in the same directory that contains the connector binary and add the following content:

   ```
   handlers = java.util.logging.FileHandler
   .level = WARNING
   com.google.enterprise.adaptor.level = INFO
   com.google.enterprise.adaptor.sharepoint.level = INFO
   java.util.logging.FileHandler.formatter=com.google.enterprise.adaptor.CustomFormatter
   java.util.logging.FileHandler.pattern=logs/spup-adaptor.%g.log
   java.util.logging.FileHandler.limit=104857600
   java.util.logging.FileHandler.count=20
   ```

8. Create a folder named `logs` in the same directory.

   **Windows**: When SharePoint and the current user domain is the same or from the same domain hierarchy, Windows operating systems automatically use the credentials of the person currently signed on to Windows.

   If not, you need to specify a username and password. For example, suppose that you run the connector from a corporate domain such as @mycompany.com against a SharePoint instance from another domain, such as GSA-CONNECTORS. In this case, you need to specify user credentials for GSA-CONNECTORS domain.
9. Get a SharePoint certificate to add it as a trusted host for the connector by performing the following steps:
   a. Navigate to SharePoint in a browser.
      A warning page appears with a message such as "This Connection is Untrusted." This message appears because the certificate is self-signed and not signed by a trusted Certificate Authority.
   b. Click, "I Understand the Risks" and "Add Exception."
   c. Wait until the "View..." button is clickable, then click it.
   d. Change to the "Details" tab and click "Export...".
   e. Save the certificate in your connector's directory with the name "sharepoint.crt".
   f. Click Close and Cancel to close the windows.

10. To allow the connector to trust SharePoint, enter the following command:

    ```bash
    keytool -importcert -keystore cacerts.jks -storepass changeit
    -file sharepoint.crt -alias sharepoint
    ```

11. When prompted Trust this certificate?, answer yes.

12. If the adaptor needs to use Live Authentication to connect to SharePoint, then add these additional configuration options to `adaptor-config.properties`:

    ```properties
    sharepoint.username=AdaptorUser Live Authentication Id
    sharepoint.password=uS3R_passWoRD
    sharepoint.useLiveAuthentication=true
    ```

13. If the adaptor needs to use ADFS Authentication to connect to SharePoint, then add these additional configuration options to `adaptor-config.properties`:

    ```properties
    sharepoint.username=AdaptorUser@yourdomain.com
    sharepoint.password=uS3R_passWoRD
    sharepoint.sts.endpoint=https://adfs.example.com/adfs/services/trust/2005/username\mixed
    sharepoint.sts.realm=urn:myserver:sharepoint or https://yoursharepoint.example.com/_trust
    ```
HTTPS configuration
If SharePoint is configured to use HTTPS, get a SharePoint certificate to add it as a trusted host for the connector by performing the following steps:

1. Navigate to SharePoint in a browser.
   A warning page appears with a message such as "This Connection is Untrusted."
   This message appears because the certificate is self-signed and not signed by a trusted Certificate Authority.
2. Click, "I Understand the Risks" and "Add Exception."
3. Wait until the "View..." button is clickable, then click it.
4. Change to the "Details" tab and click "Export...".
5. Save the certificate in your connector's directory with the name "sharepoint.crt".
6. Click Close and Cancel to close the windows.
7. To allow the connector to trust SharePoint, enter the following command:

   keytool -importcert -keystore cacerts.jks -storepass changeit
   -file sharepoint.crt -alias sharepoint

8. When prompted Trust this certificate?, answer yes.

Step 3 Configure adaptor-config.properties variables
Optionally, you can edit or add additional configuration variables to the adaptor-config.properties file. The following table lists the most important variables that pertain to the SharePoint User Profiles connector, as well as their default values. See also “Common configuration options" in the the Administration Guide.

<table>
<thead>
<tr>
<th>Variables</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>server.dashboardPort</td>
<td>Port on which to view web page showing information and diagnostics.</td>
<td>The Windows installer sets this value to 5779. If you use the command-line installer, this value defaults to 5679 for all adaptors. You can edit this value and set it to any value that is different from server.port.</td>
</tr>
<tr>
<td>server.port</td>
<td>Unique value for the retriever port.</td>
<td>The Windows installer sets this value to 5778. If you use</td>
</tr>
<tr>
<td>parameter</td>
<td>Description</td>
<td>default</td>
</tr>
<tr>
<td>--------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>adaptor.namespace</td>
<td>Namespace used for ACLs sent to GSA.</td>
<td>Default</td>
</tr>
<tr>
<td>profile.setacl</td>
<td>Whether user profile information is considered restricted to authenticated users or public.</td>
<td>True</td>
</tr>
<tr>
<td>profile.mysitehost</td>
<td>SharePoint Web application URL hosting my sites for users.</td>
<td>Virtual server</td>
</tr>
</tbody>
</table>

### Step 4 Run the Connector for SharePoint User Profiles

After you install the Connector for SharePoint User Profiles, you can run it by using `cmd.exe` on the host machine:

```bash
java -Djava.util.logging.config.file=logging.properties -jar adaptor-sharepoint-user-profile-4.1.1-withlib.jar
```

Verify that the connector has started and is running by navigating to the Connector Dashboard at `http://<CONNECTOR_HOST>:<nnnn>/dashboard` or `https://<CONNECTOR_HOST>:<nnnn>/dashboard`

where `<nnnn>` is the number you specified as the value for the `server.dashboardPort` in the configuration file.

To run the connector as a service, use the Windows service management tool or run the `prunsrv` command, as described in “Run a connector as a service on Windows” in the Administration Guide.
Uninstall the Google Search Appliance Connector for SharePoint User Profiles

If you have created a Windows Service for the Connector for SharePoint User Profiles, before you uninstall the connector, you must remove the Windows Service.

To stop and remove the Windows Service, execute the following command:

```bash
prunsrv //DS//adaptor-sharepoint-user-profile
```

To uninstall the Connector for SharePoint User Profiles on Windows:

1. Navigate to the SharePoint User Profiles connector installation folder, `GSA_SPUP_Adaptor_installation`.
2. Click `Uninstall_GSA_SPUP_Adaptor.exe`. The `Uninstall GSA_SPUP_Adaptor` page appears.
3. Click **Uninstall**. Files are uninstalled.
4. Click **Done**.
Troubleshoot the Connector for SharePoint User Profiles
For information about troubleshooting the Connector for SharePoint User Profiles, see “Troubleshoot Connectors,” in the Administration Guide.