Table of Contents

1 Repstor custodian on-premise Installation ...... 4
   1.1 Environment Checklist................................................................. 4
   1.2 Custodian web install .................................................................... 4
   1.3 Run custodian installer (Installs Website Files) .................................... 6
   1.4 Installing Redis ............................................................................. 8
   1.5 Verify custodian URL and SSL connection ......................................... 8

2 Connect custodian to SharePoint ................. 9
   2.1 Register add-in with appregnew ......................................................... 9

3 Create Server-to-Server connection ............ 10
   3.1 Create S2S certificate ................................................................... 10
   3.2 Configure SharePoint with S2S Certificate ....................................... 11
   3.3 Configure Custodian with S2S certificate ......................................... 12

4 Install & Configure Provisioning Engine ...... 14
   4.1 Queues ......................................................................................... 14
   4.2 Provisioning engine service ............................................................ 15
   4.3 Generate custodian app file ............................................................. 16
   4.4 Enable Remote Site Collection provisioning (optional) ....................... 17
   4.5 Additional Settings ....................................................................... 17

5 Troubleshooting ............................................... 18
1 Repstor custodian on-premise
Installation

This document describes the installation of Repstor custodian in on-premise environments.

Before the installation complete the prerequisite steps. See Repstor Custodian On-Premise prerequisites document.

1.1 Environment Checklist

If any of the following checks fail, please read the prerequisites document to execute the correct configuration steps.

SharePoint Server

- March 2016 cumulative update installed or later
- Configuration for add-in support completed
  - add-in catalog is created (Central Admin -> Apps -> App Management -> Manage App Catalog). Select correct web application and ensure add-in catalog is created.
  - App URLs is configured (Central Admin -> Apps -> Configure App URLs). Ensure App domain and App prefix are completed.
  - App Management and Subscription Settings Service applications are created and started (Central Admin -> Application Management -> Manage service applications)
  - Custodian server
- IIS 8 installed (minimum)
- SSL certificate and custodian domain name are available (e.g. custodian.mycompany.com etc.)

1.2 Custodian web install

Ensure an IIS web application is available.

1. Run `inetmgr` from the Run dialog to open the IIS Manager.
   
   If this server is dedicated to custodian, you can use the Default Web Site which will be available.

2. If necessary, create a new website. Name your website CustodianWeb.

3. Select the correct website and in the Authentication section, disable everything except Windows Authentication.
4. In C:\Windows\System32\inetsrv\config\applicationHost.config, change the anonymousAuthentication section's overrideModeDefault from Deny to Allow.

This allows the anonymous access necessary to serve the custodian API.

5. Click Basic Settings and set the Physical Path to a new, empty folder:

6. Click OK.

7. To configure an SSL binding, Click Bindings.

8. In the Host name box type the correct host name.
9. If the server hosts multiple websites such as custodian and SharePoint, select the **Require Server Name Indication** check box.

10. In the **SSL certificate** drop-down, click the correct SSL certificate.

11. Click OK.

### 1.3 Run custodian installer (Installs Website Files)


2. Edit the file `Repstor.Sharepoint.Web.csproj.SetParameters.xml` in Notepad:

   ![Directory tree with RepstorCustodianWeb files]

3. Ensure the name of your IIS website matches the value in the SetParameters file:

   ![XML code in Notepad]
4. Open a powershell prompt as administrator and browse to the directory you unzipped to:

   ![Tasks](image)

   - Run as Administrator
   - Run ISE as Administrator
   - Windows PowerShell ISE
   - Windows PowerShell
   - Unpin this program from taskbar

5. Execute the command

   ```
   .\Repstor.Sharepoint.Web.csproj.deploy.cmd /Y
   ```

   ![Select Administrator](image)

   This installs the website files to your website directory. (Tip: instead of typing the full filename, enter `.\` followed by tab).

   ![Administrator: Windows PowerShell](image)

   The output should look as follows:
1.4 Installing Redis

1. Download and run the latest Redis installer from
   https://github.com/MSOpenTech/redis/releases

2. Ensure that the “Set the Max Memory limit” is checked during the installer.

   ![Set the Max Memory limit]
   
   Max Memory: 100 MB

1.5 Verify custodian URL and SSL connection

1. Open your web browser and enter the correct URL for your website (see pre-requisites
   for configuring custodian URL/DNS):

   ![Repstor custodian]
   
   ![https://custodian.repstor.com/Error]

   You must see if your SSL certificate is valid. Additionally, you will be redirected to a
   blank Error page – this is normal since the request did not originate from SharePoint.
   However, this confirms that the address is correct, and SSL is configured correctly.

   If you are installing custodian on a SharePoint front-end server, ensure that the pre-existing
   SharePoint URL is unaffected.
2 Connect custodian to SharePoint

After the custodian server is installed, configure it to connect to SharePoint. This involves registering the app with SharePoint and setting up a server-to-server trust with SharePoint to allow communication.

2.1 Register add-in with appregnew

1. Browse to the SharePoint URL at /_layouts/15/appregnew.aspx and enter the following values:

   **App Id**: 81a5429e-0186-4684-bd22-f4e6e4e1bc4a (you can use any generated GUID, but Repstor consistently use this one to avoid confusion)

   **App Secret**: <click Generate>

   **Title**: Repstor custodian

   **App Domain**: custodian.mycompany.com (enter your own custodian server url as tested in the previous step)

   **Redirect URI**: Same as App domain, but with https://

2. Click the Create to view a summary.

   **CAUTION** Ensure that you note down all details by saving to a text file for later use. The App Secret cannot be retrieved after you close this summary page.
3 Create Server-to-Server connection

The server-to-server connection is what allows custodian to access SharePoint, by configuring SharePoint to trust requests signed with a digital certificate.

3.1 Create S2S certificate

Note If you already have a certificate and private key that you wish to use, skip this step.

1. To generate a key, first download and install OpenSSL from http://gnuwin32.sourceforge.net/packages/openssl.htm

2. Open a command window and cd to C:\Program Files (x86)\GnuWin32\bin

3. Execute the command below. Input the relevant details when prompted.
   
   openssl req -x509 -newkey rsa:2048 -keyout s2s.pem -out s2s.cer -days 3650 -passin "pass:P@ssword1" -passout "pass:P@ssword1" -config "C:\Program Files (x86)\GnuWin32\share\openssl.cnf"

4. Export the public key:

   The SSL certificate is saved in the C:\Program Files (x86)\GnuWin32\bin

   openssl pkcs12 -export -in "s2s.cer" -inkey "s2s.pem" -out "s2s.pfx" -passin "pass:P@ssword1" -passout "pass:P@ssword1" -CSP "Microsoft RSA SChannel Cryptographic Provider"

   (the final parameter, -CSP, allows us to explicitly specify the provider. Some providers are not supported in token-signing applications and will result in an **Invalid provider type specified** error in the custodian logs)
3.2 Configure SharePoint with S2S Certificate

1. To register the certificate public key as a trusted root authority. Open SharePoint Management Shell as Administrator and execute the following:

```powershell
$path = "C:s2s.cer"
New-SPTrustedRootAuthority -Name "Custodian S2S Certificate" -Certificate $certificate
```

2. To register the token issuer, equivalent to registering custodian as being trusted to access SharePoint with the s2s certificate.

   The issuerId value must be the same as the App Id as entered on the appregnew.aspx page.

   Execute the following:

```powershell
$realm = Get-SPAuthenticationRealm
$issuerId = "81a5429e-0186-4684-bd22-f4e6e4elbc4a"
$fullIssuerId = $issuerId + '@' + $realm
New-SPTrustedSecurityTokenIssuer -Name "Custodian S2S Cert" -Certificate $certificate -RegisteredIssuerName $fullIssuerId -IsTrustBroker
```

   The above will take up to 24 hours to take effect in the SharePoint system, but should work immediately if SharePoint is restarted.

3. A reminder to renew the certificate before expiry date. The certificate has an expiry date, which has been set to 10 years.

SharePoint over HTTP
If SharePoint is running over HTTP, and not HTTPS, then you must explicitly enable OAuth to work over HTTP.

Within the SharePoint Management Shell, run the following:

```powershell
$serviceConfig = Get-SPSecurityTokenServiceConfig
$serviceConfig.AllowOAuthOverHttp = $true
$serviceConfig.Update()
```

See the following URL for more information;

**Note** whilst SharePoint can be configured to work over HTTP, the custodian server **must** be HTTPS.

### 3.3 Configure Custodian with S2S certificate

Configure the custodian web application to use the certificate private key to encode requests. Import the certificate and its private key to the certificate store on the local machine.

**Note** Referencing the private key directly by using the path and password is no longer recommended.

#### Configure certificate by importing it to the local machine

Ensure that both the certificate and its private key (the .cer and .pfx files) are imported to the LocalMachine location, in the Personal store, **with the private key**. You will know the private key has been imported if the certificate icon shows the key symbol. You grant access to the custodian app pool identity using the following steps:

- a. Right-click the certificate and select All Tasks
- b. Select Manage Private Keys
- c. Add the custodian app pool identity. Note that if the custodian app pool uses the identity 'ApplicationPoolIdentity', then you should add the identity with following format:

  `IIS AppPool\custodian`

  where `custodian` is the name of the app pool.

#### Configure certificate using private key on disk

**Note** This method of configuring the certificate is only supported **before** .NET 4.6 and is no longer recommended.

1. Run Notepad as administrator and open the web.config file from the installation folder of the custodian web application. There are a few values to configure:
2. Set ClientSecret to the value configured on the appregnew.aspx page;

3. Set ClientSigningCertificatePath to the path of the private key on the local machine (ensure the identity of the custodian app pool has read access to it);

4. Set ClientSigningCertificatePassword to the password of the private key file;

Configure logging

Set the log file location. This can be useful for troubleshooting installation problems.
4 Install & Configure Provisioning Engine

4.1 Queues

1. Create two MSMQ queues: ‘custodian’ and ‘custodianeadd’.
2. Grant full access to the app pool identity under which custodian is running.
3. Open Computer Management and browse to MSMQ. Right-click and create the two queues:

When setting up the MSMQ Queues for custodian does not require selecting the transactional option.

**Note** You should assign full permissions to the custodian web application app pool identity:
4.2 Provisioning engine service


2. Copy the files to a new folder under C:\Program Files\Repstor\Provisioning Engine (Or a location of your choice).

3. Open a command prompt as administrator and execute the following command to create the provisioning engine windows service:

   ```
   sc create repstor_provisioning binPath= "C:\Program Files\Repstor\Provisioning Engine\Repstor.Sharepoint.Tasks.Server.exe" DisplayName= "Repstor Provisioning Engine" start= auto
   ```

   Open Windows Services and view properties for the new service:
4. Ensure the account under the Log On tab has full permissions to the custodian queue.
5. Start the service.

### 4.3 Generate custodian app file

1. Generate an app file (.app) to add to the SharePoint app catalog. This is custom to every on-premise environment, to match the custodian site URL and Client ID. The Repstor app generator can be used to produce it.
2. Navigate to [https://custodian-appgen.azurewebsites.net](https://custodian-appgen.azurewebsites.net) and enter your URL and Client ID (81a5429e-0186-4684-bd22-f4e6e4e1bc4a):

```
Custodian Url: https://custodian.mycompany.com
Client Id: 81a5429e-0186-4684-bd22-f4e6e4e1bc4a

[Download App File]
```

3. Download the app file.
4. Navigate to the SharePoint App Catalog site, and upload the app file. The App Catalog must already be created during the prerequisites. You can find it in **Central Admin -> Apps -> Manage App Catalog**.
When the app is uploaded to the app catalog library, it is available to install on SharePoint sites.

### 4.4 Enable Remote Site Collection provisioning (optional)

If you are using custodian to provision Site Collections, then you will need to enable remote site collection provisioning. This involves a few simple steps:

1. Ensure SharePoint is on at a minimum the March 2016 cumulative update.
3. Enable Remote Site Collection Provisioning for your web application
4. Create (or nominate an existing) site collection which will be designated as the admin site for managing site collection creation, and set its AdministrationSiteType property to TenantAdministration.


### 4.5 Additional Settings

For on-premise installation of custodian, you must add the following keys in the relevant location.

"Custodian.ClientId"="81a5429e-0186-4684-bd22-f4e6e4e1bc4a"

"Custodian.CustodianUrlBase"="https://[Custodian Url]/Matter/Create?SPHostUrl=

"Custodian.HostUrl"="[SP Host Url]"

"Custodian.ServiceUrl"="[Custodian Url]"

"CRLSync.ReposServer"="[Custodian Url]/api (or [Repositories Server Url]/api in the case of a dedicated repositories server)"

The location for these keys is

**Computer\HKEY_LOCAL_MACHINE\SOFTWARE \Repstor\Repstor affinity** - for 64 Bit Office.

**Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Repstor\Repstor affinity** - for 32 Bit Office.
5 Troubleshooting

• When adding the app under Site Contents, the app doesn't add and says “we're adding your app” indefinitely – confirm these services are running: App Installation Service, SharePoint Timer Service, SharePoint Central Administrator Service

• “Keyset does not exist” error – web application user identity does not have access to the server-to-server certificate specified in the web.config. You should give that user access. See also: http://stackoverflow.com/questions/602345/cryptographicexception-keyset-does-not-exist-but-only-through-wcf

• “Invalid Issuer” error – you have not correctly configured SharePoint such that the certificate is a trusted token issuer for the correct client ID (81a5429e-0186-4684-bd22-f4e6e4e1bc4a). Review the instructions on the following page and note that anywhere the guid “11111111-1111-1111-1111-111111111111” is mentioned, it should be replaced with the custodian client ID. https://msdn.microsoft.com/en-us/library/office/fp179901(v=office.15).aspx#Configure2 http://msdn.microsoft.com/en-us/library/office/jj860570(v=office.15).aspx#ConfigureSP

• “Sorry, this site does not support apps but you can still acquire them and add them on other sites.” This error can appear if any of the SharePoint app support steps have been skipped or completed incorrectly. You will need to review steps from the section “Initial SharePoint configuration for app support”. Some common omissions are:
  o Has an App Management Service been created? (Central Admin, Application Management, Manage service applications)
  o Is the User Profile Service running under Central Admin -> Application Management -> Manage services on server?
  o Under Central Admin -> Application Management -> Manage service applications, are the User Profile Service Application and App Management Service running?
  o Does the User Profile Service Application have at least one user profile created?
  o Has the isolated apps domain been registered by running Set-SPAppDomain, and the app prefix set by running Set-SPAppSiteSubscriptionName?
  o Has the Subscription Settings Service been enabled via relevant Powershell commands?

• “Sorry, something went wrong” “an unexpected error occurred”. This can happen when attempting to install an app as the system account. This can be confirmed by inspecting the ULS logs.

• “Error in step 'Applying reusable workflows to lists.' Step will be skipped, provisioning will continue. Operation is not valid due to the current state of the object.” – this can be caused by a reusable workflow in an invalid state. Try opening the workflow in SharePoint designer, re-save, and re-publish it.

• App does not appear in app catalog. In this case, ensure the user is both a Farm Administrator and a Site Collection Administrator (but not the System Account).
• ‘Sorry this app is not supported on your server’ - Check that the service applications are running as described in the custodian pre-requisites document. Also check that the User Profile service is running and user profiles have been imported.

• Custodian fails to load and the logs contain a “403 forbidden” error: This can occur when SharePoint is running over http (non-SSL). To permit web services over HTTP, run the following commands:

```powershell
$serviceConfig = Get-SPSecurityTokenServiceConfig
$serviceConfig.AllowOAuthOverHttp = $true
$serviceConfig.Update()
```

• Custodian fails to load and the following error appears in the logs: “An internal error occurred” “System.Security.Cryptography.X509Certificates.X509Utils._LoadCertFromFile” This may mean that the advanced setting “Load User Profile” should be set to True in the app pool advanced settings.

• Custodian displays in IE7 compatibility mode
It is possible that group policy (or other environmental settings) cause web pages to display in IE7 compatibility mode by default. This can be overridden by adding an HTTP response header in IIS as follows:

```
X-UA-Compatibe="!IE=11"
```