

Metalogix® Replicator 7.4

September 2023

Using Replicator with Claims-Based Authentication

This article describes the steps you must perform to configure Metalogix Replicator with SharePoint 2010 and 2013 Web Applications using Claims-based Authentication or Anonymous Access.

[Configuring Claims-based Windows Authentication Web Applications](#)

[Configuring Forms-based, Mixed Mode Authentication, or Anonymous Access Web Applications](#)

Configuring Claims-based Windows Authentication Web Applications

Web applications using only claims-based Windows-only authentication can be configured for replication using the steps described in the Metalogix Replicator documentation.

Note that the account you specify must have read and write access to the Replicator Data Folders on the Target Web Application.

For more information on creating a Replication Connection, see the *Metalogix Replicator Reference Guide*.

Configuring Forms-based, Mixed Mode Authentication, or Anonymous Access Web Applications

For claims-based authentication, Metalogix Replicator requires a web application or web application extension configured using only Windows authentication. If you have a web application using forms-based authentication, a combination of claims-based authentication types, or Anonymous Access, then you must perform the following tasks to extend the web application for Replicator:

1. Extend the web application.
2. Configure Replicator Data Folders.
3. Configure the extension site.

1. Extend the Web Application

- In SharePoint Central Administration, select **Application Management** and then **Manage Web Applications**.
- Select the web application and click **Extend**.
- In the Extend Web Application form, enter settings for the extension. For example, if your forms-based web application uses port 80, then configure the extension to use port 8080. Give the extension a unique name to make it easier to identify later. For example, you could name the extension for an extranet site, "Extranet NTLM".
- Under Claims Authentication Types, select **Enable Windows Authentication, Integrated Windows authentication, and NTLM**. Do not select any other options under Claims Authentication Types.

Claims Authentication Types

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

Enable Windows Authentication

Integrated Windows authentication

NTLM

- Click OK to create the extension.

2. Configure Replicator Data Folders

- On the SharePoint Central Administration page, select **Application Management**.
- On the Application Management page, under Metalogix Replicator, select **Configure Web Application**.
- Scroll to the bottom of the Configure Web Application page and expand **Replicator Data Folders**.
- Ensure the account you selected in step 2 has permission to both read from and write to each of the Replicator Data Folders. Also ensure that account is specified on this page.

Package Data Path:

\\EXTRANET\Replicator_Data\bfd33105-d465-423a-a3f7-f48045fbb90c\Packages\

DC Cache Path:

\\EXTRANET\Replicator_Data\bfd33105-d465-423a-a3f7-f48045fbb90c\Cache\

Replicator Data Folders are on a network file server:

User Account:

EXTRANET\SPSAdmin

Password:

.....

- Note the paths and the user account. We will use this information to configure IIS virtual directories later.
- If you have not previously enabled this web application for replication, then do that now. This creates the Replicator Data Folders.

3. Configure the Extension Site

- a. Start Internet Information Services (IIS) Manager.
- b. Expand the site's folder, then **_layouts, Metalogix, and Replicator**. You will see an Images folder under the Replicator folder.
- c. Right-click on the Replicator folder and select **Add Virtual Directory**.
- d. In the Add Virtual Directory dialog:
 - For Alias field, enter **Import**.
 - For Physical Path, enter the Import Path from the Configure Web Application page.
- e. Click **Connect as**.
- f. In the Connect As dialog:
 - Select **Specific user**.
 - Click **Set** and enter the user account information from the Configure Web Application page. If the user account included a domain, then you must also include it here, for example EXTRANET\spadmin.
 - Click **OK** twice to return to the Add Virtual Directory dialog.
- g. Click **Test Settings** to validate the virtual directory settings you have entered.
- h. If both tests pass, then click **Close** to return to the Add Virtual Directory dialog and then click **OK** to create the virtual directory.
- i. Repeat steps 7 through 12 to create a virtual directory named **Export**, using the Export Path value from the Configure Web Application page.
- j. Restart the site for the extended web application.

The web application extension is now fully prepared for Replicator. You can proceed to configure Replicator as described in the Metalogix Replicator documentation.

When you create the Replication Connection for your web applications, **connect to the NTLM-only web application extension**.

Remapping Domains and User Accounts

Web applications using claims-based authentication translate user accounts into claims identities. Each NTLM identity is prefixed with one of the following tokens:

Authentication Type	Token Prefix	Example Identity
Classic	<i>none</i>	DOMAIN\username

Authentication Type	Token Prefix	Example Identity
Claims-based Windows	i:0#.w	i:0#.w DOMAIN\username
Forms-based	i:0#.f <MembershipProviderName>	i:0#.f sqlmember username

For more information on remapping domains and user accounts, see *SKB 1100224, User and Domain Remapping* in the Metalogix Knowledge Base.

Domain Remapping for Inbound Packages

When configuring domain on the Replicator Configure Web Application page, you must specify this prefix before the domain. For example, if the Corporate Portal web application uses claims-based authentication with Windows authentication and we want to remap all inbound changes to the CORPORATE domain, then we would configure the web application as follows:

Enable domain remapping:

Yes No

Remap domain names in inbound Packages to:

i:0#.w|CORPORATE

Remap unknown inbound user accounts to:

Site Collection Owner System Account

Enable user remapping table:

Yes No

In this example, changes made by LONDON\paul would be remapped to CORPORATE\paul when they are applied on the Corporate Portal.

Since forms-based authentication accounts do not have a domain, you cannot use domain remapping with web applications using forms-based authentication. You can use user remapping in these situations.

User Remapping for Inbound Packages

When configuring user remapping, you must specify the appropriate prefix with each user in the remapping table. The following examples show how you can specify entries in a user remapping table for various scenarios:

To remap inbound changes from the claims-based CORPORATE\susan account to a generic, forms-based support account on the Extranet Portal, we would use the following remapping on the Extranet Portal:

```
<User OldUser="i:0#.w|CORPORATE\susan" NewUser="i:0#.f|sqlmember|support"/>
```

Alternatively, if in the previous example, the outbound web application was using classic authentication, then there would not be a token prefix and we could specify the mapping as follows:

```
<User OldUser="CORPORATE\susan" NewUser="i:0#.f|sqlmember|support"/>
```

Applies To

- Metalogix Replicator for SharePoint version 4.1, builds 3375.151 and higher
- Metalogix Replicator for SharePoint version 5.0

Keywords

Replicator; authentication; Claims-based authentication; Forms-based; CBA; FBA