

# Metalogix® Replicator 7.4

September 2023

## Firewall Replication

Replicator supports one way and bidirectional replication between any pair of web applications where one of the web applications can communicate with the other using HTTP or HTTPS. In a firewalled environment, one of the web applications is behind a firewall and cannot be accessed by the other web application. Replicator requires that the web application behind the firewall must be able to communicate with the other.

Configuring Replicator for firewalled replication is almost the same as configuring non-firewalled replication. The only change is how you configure your Replication Connections between web applications. This article describes the steps you must perform to configure Metalogix Replicator for firewalled replication.

Operationally, Replicator changes its behavior in firewalled replication environments. Since only the web application inside the firewall can communicate with the other, its instance of Replicator manages all communication and transfers for replication. Instead of the Replicator instance outside of the firewall downloading packages from the web application inside the firewall, the Replicator instance inside the firewall uploads packages to the instance outside the firewall using BITS Server Extensions.

[Prerequisites](#)

[Configuration Overview](#)

## Prerequisites

The following sections describe the tasks you must perform on each server running the SharePoint Web Application service, including all web front-end servers. These steps can be performed before or after installing Replicator.

## Windows Server 2008 R2

1. For each web application server in the farm outside the firewall, install BITS IIS Server Extension. For instructions, see <http://technet.microsoft.com/en-us/library/cc753301.aspx>.
2. For each web application server in the farm outside the firewall, install IIS Hotfix 2587894 from <http://support.microsoft.com/kb/2587894>.

## Windows Server 2008

1. For each web application server in the farm outside the firewall, install BITS Server Extensions. For instructions, see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa363130.aspx>.
2. For each web application server in the farm outside the firewall, install IIS Hotfix 2587894 from <http://support.microsoft.com/kb/2587894>.

## Windows Server 2003

1. For each web application server on the farms inside and outside of the firewall, install the Microsoft components required by Replicator for Windows Server 2003. These components are described in the *Metalogix Replicator Quick Start Deployment Guide*.
2. For each web application server in the farm outside the firewall, install BITS Server Extensions. For instructions, see <http://technet.microsoft.com/en-us/library/cc740133%28WS.10%29.aspx>.

## Configuration Overview

The configuration for firewalled replication only affects how you set up your Replication Connections between web applications. All other aspects of configuring and managing Replicator are unchanged. For the complete steps required to configure replication, see the *Metalogix Replicator Quick Start Deployment Guide*.

When you create a connection from the web application inside the firewall and select the Firewalled replication mode, Replicator automatically creates a connection for the other web application. Since the other web application cannot communicate with the web application inside the firewall, the automatically created connection does not require any credentials for the web application inside the firewall.

The following sections highlight the specific steps you must perform to configure firewalled replication depending on your replication scenario.

## Configuring One Way Replication with the Source behind a Firewall

In this scenario, the target Replicator instance (Extranet Portal) cannot download packages from the source web application (Corporate Portal) because of the firewall. The source Replicator instance must upload files to target using the server extensions.

To configure Replicator for this scenario:

1. Enable the web application on the inside of the firewall.

2. Set a passphrase for the web application outside the firewall under **Advanced Settings** before enabling the web application. If the web application was already enabled, then set the passphrase, disable, and then re-enable.
3. On the web application inside the firewall, create a Replication Group for one way replication. This group cannot exist on the other web application.
4. On the web application inside the firewall, create a Replication Connection to the other web application. The connection must have the following settings:
  - a. Under **Target Web Application** enter the passphrase which was set for the web application in step 1.
  - b. Under **Selected Replication Groups**, select the group you created in step 3.
  - c. Under **BITS Transport Settings** and **Replication Mode**, select **Firewalled**.

By specifying the firewalled replication mode, Replicator automatically creates a Replication Connection on the other web application for replication.

5. On the web application inside the firewall, create a Replication Map Family that specifies the SharePoint changes you want to replicate. Configure the map family to use the group created in step 3.

After completing these steps, changes made to the web application inside the firewall are replicated to the other web application.

## Configuring Bidirectional Replication with a Firewall

In this scenario, the Replicator instance outside the firewall (London Branch Portal) cannot download packages from the web application inside the firewall (Corporate Portal). Nor can it inform the Replicator instance inside the firewall that packages are available for download. The firewalled Replicator instance must upload files to the other instance using the server extensions and must also regularly poll the web application outside the firewall for available packages.

To configure Replicator for this scenario:

1. Enable the web application on the inside of the firewall.
2. Set a passphrase for the web application outside the firewall under **Advanced Settings** before enabling the web application. If the web application was already enabled, then set the passphrase, disable, and then re-enable.
3. On the web application inside the firewall, create a Replication Group for bidirectional replication. You can also use the preconfigured Worldwide Connections group.
4. On the web application outside the firewall, create a Replication Group with the same name as the one created in step 3.
5. On the web application inside the firewall, create a Replication Connection to the other web application. The connection must have the following settings:

- a. Under **Target Web Application** enter the passphrase which was set for the web application in step 1.
- b. Under **Selected Replication Groups**, select the group you created in step 3.
- c. Under **BITS Transport Settings** and **Replication Mode**, select **Firewalled**.

By specifying the firewalled replication mode, Replicator automatically creates a Replication Connection on the other web application for replication.

6. On the web application outside the firewall, edit the automatically created Replication Connection. Under **Selected Replication Groups**, select the group you created in step 3.
7. On either web application, create a Replication Map Family that specifies the SharePoint changes you want to replicate. Configure the map family to use the group created in step 3. Since the group exists for both web applications, Replicator automatically configures the other web application to use the same map family for bidirectional replication.

After completing these steps, changes made to either web application are replicated to the other web application.

## Configuring One Way Replication with the Target behind a Firewall

In this scenario, the Replicator instance outside the firewall (London Branch Portal) cannot inform the Replicator instance inside the firewall (Corporate Portal) that packages are available for download. The firewalled Replicator instance must regularly poll the web application outside the firewall for available packages.

To configure Replicator for this scenario:

1. Enable the web application on the inside of the firewall.
2. Set a passphrase for the web application outside the firewall under **Advanced Settings** before enabling the web application. If the web application was already enabled, then set the passphrase, disable, and then re-enable.
3. On the web application inside the firewall, create a Replication Connection to the other web application. The connection must have the following settings:
  - a. Under **Target Web Application** enter the passphrase which was set for the web application in step 1.
  - b. Under **Replication Groups**, clear all groups from **Selected Replication Groups**.
  - c. Under **BITS Transport Settings** and **Replication Mode**, select **Firewalled**.

By specifying the firewalled replication mode, Replicator automatically creates a Replication Connection on the other web application for replication.

4. On the web application outside the firewall, create a Replication Group for one way replication.

5. On the web application outside the firewall, edit the automatically created Replication Connection. Under **Selected Replication Groups**, select the group you created in step 3.
6. On the web application outside the firewall, create a Replication Map Family that specifies the SharePoint changes you want to replicate. Configure the map family to use the group created in step 3.

After completing these steps, changes made to the web application outside the firewall are replicated to the other web application.

After completing these steps, Replicator is configured to replicate changes made to your SharePoint web applications. No other Replicator configuration and maintenance activities are affected by the firewall.

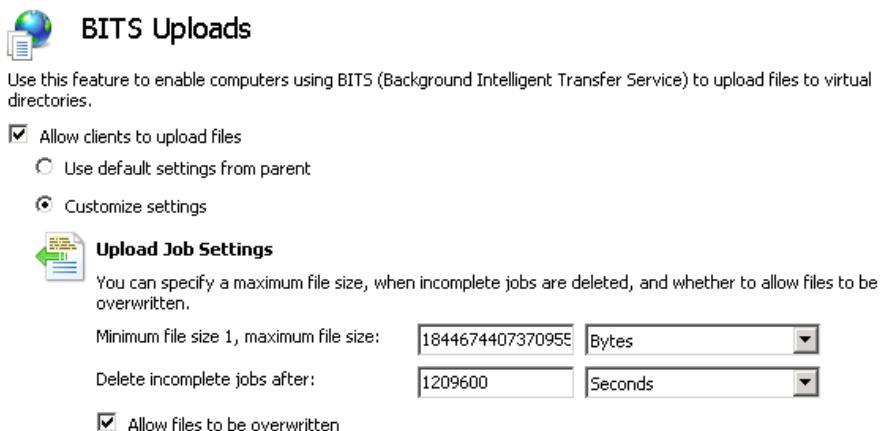
## Verifying IIS BITS Upload Settings

When you enable any web application on a server where BITS Server Extensions are installed, Replicator automatically configures the Replicator Import data folder for BITS Uploads. You can verify these settings as follows.

## Windows 2008 R2 and Windows 2008

To verify the web application has the correct BITS Upload settings:

1. Open Internet Information Services (IIS) Manager.
2. In the Connections tree, expand the site corresponding to the web application that was enabled for replication. Then expand the \_layouts, Synergy and Replicator folders.
3. Select the Import folder and then double click BITS Uploads in the main window. This opens the BITS Uploads settings for the Replicator Import Data Folder.
4. In the BITS Uploads settings, verify the following options are selected:
  - Allow clients to upload files.
  - Allow files to be overwritten.



5. If you change any of the BITS Uploads settings or any other IIS settings for this site, then you must stop and restart the site.

## Windows 2003

To verify the web application has the correct BITS Upload settings:

1. Open Internet Information Services (IIS) Manager.
2. Select the Web Sites folder in the Internet Information Services tree. In the main window, note the identifier for the web site you enabled for replication.
3. Open a Command Prompt window and run the following command in the window:

```
C:\Windows\System32\cscript.exe C:\Inetpub\AdminScripts\adsutil.vbs get  
w3svc/<identifier>/root/_layouts/Syntergy/Replicator/Import/BITSAllowOverwrites
```

If this command returns an integer value, then BITS uploads are configured properly for the Replicator Import data folder. If an error or any other value is returned, then verify that the prerequisite software listed earlier in this document is installed correctly and then disable and re-enable replication for this web application.

### Applies To

- Metalogix Replicator for SharePoint version 4.x, build 3375.151 and higher