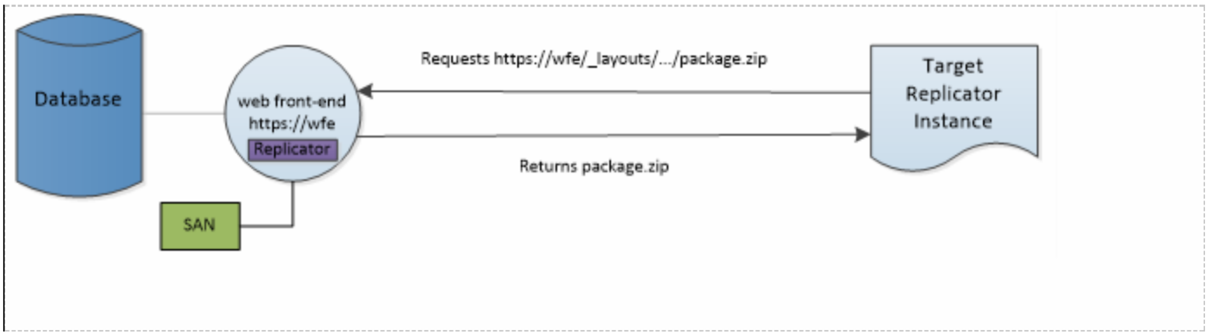
Metalogix® Replicator 7.4

September 2023

Secure Replication

This Knowledge Base article provides an overview of the advanced security configurations Replicator supports. Security configurations are applied at multiple levels within Replicator, SharePoint and IIS. Replicator relies upon the security that is configured within your SharePoint farm first and foremost.

The following diagram demonstrates the various areas that can be secured when replicating packages between two web applications:



This document will reference the above diagram while providing an overview of Secure Replication.

PowerShell

SharePoint

The first step to securing Replicator is to secure the SharePoint farm. The primary steps in securing a SharePoint farm are done through the configuration of secure connections and the use of least-privileged accounts.

Secure Connections

Secure connections can be configured for SharePoint by using the Hypertext Transfer Protocol Secure (HTTPS) option when creating or extending web applications. Another method to secure connections is to create a Virtual Private Network (VPN) connection between farms. These methods can be used separately or in tandem to enhance connection security.

Encrypting Transfers using HTTPS

The easiest method to secure SharePoint connections is through the use of the Hypertext Transfer Protocol Secure (HTTPS) which layers the HTTP protocol on top the Secure Socket Layer (SSL) and Transport Level Security (TLS) protocols. These protocols use system provided Windows functions to encrypts all inbound and outbound traffic for a web application at the Internet Information Services (IIS) level. Due to its unique design, Replicator leverages the security configuration of the underlying SharePoint platform. When the web application and its IIS web sites are configured to use HTTPS, all traffic to and from the web application is encrypted.

Replicator leverages this encryption through the use of the Binary Intelligent Transfer Service (BITS) as the transport layer between farms. After capturing an event on the source SharePoint farm, the content is packaged and then transferred using BITS. BITS transfers the package using the transfer protocol specified by IIS for the web application. When HTTPS is configured for the SharePoint web application this same level of encryption will be used by BITS to encrypt the transfer content.

This encryption and decryption of transfer content is handled entirely by IIS using the industry standards TLS and SSL. This provides administrators with a level of encryptions that is commonly understood with proven performance.

Encrypting Transfers using Secure VPN

Secure VPN solutions ensure all users and servers connected within a VPN have secure and encrypted access to each other. In a VPN environment all traffic sent through the secure VPN connection is automatically encrypted without requiring any changes in SharePoint or its underlying platform.

Secure VPN solutions allow network administrators to create a single comprehensive security solution for their clients without requiring specific changes and configuration in SharePoint. Replication Package transfers that are sent over the secure VPN connection are automatically encrypted by the VPN solution.

A whitepaper discussing MOSS 2007 in an SSL VPN environment, *How to Select an SSL VPN for Remote Access to Microsoft SharePoint Portal Server 2007*, can be downloaded from the Microsoft web site at http://download.microsoft.com/download/F/0/2/F0229C11-B47E-4002-A444-60207C6E11F5/SSL%20VPN%20for%20SharePoint-WP-200702.doc.

Least-Privilege Accounts

Least-privilege accounts is a security concept which provides each account in a network the minimum permissions required to perform required tasks. This concept all accounts, but for the purposes of this document the focus will be on SharePoint service accounts. The account privileges required by service accounts for SharePoint are discussed in the Microsoft Technet article found at http://technet.microsoft.com/en-us/library/hh377944.aspx. Least-privilege account requirements for Replicator will be discussed below.

Replicator

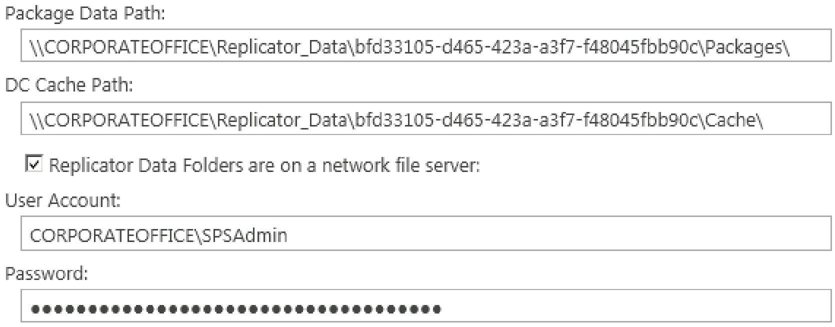
The process of securing Replicator builds upon the security which has already been configured for SharePoint. The first step in ensuring a secure environment for replication is done by requiring farm administration privileges to configure Replicator. This ensures that only designated administrators can alter the configuration of your SharePoint and Replicator environments. Additional security is provided through the configuration of the Replicator data folders, encrypted zip files, firewalled connections and least-privilege accounts.

Replicator Services

The Replicator service runs under the SharePoint Central Administration (SP CA) Application Pool account. The Replicator service must run under the SP CA application pool account and can't be replaced with another account. However, to increase security you could create separate application pool accounts for each web application which would result in the application pool account for the content web applications being different than the application pool account for the SP CA application pool account. This will work fine provided you follow the instruction in the *Metalogix Replicator Advanced Installation Guide* under Access Requirements.

Replicator Data Folders

When configuring Replicator during the initial setup, a file share is created to store inbound and outbound replication packages. The permissions on both the share and the physical folder location should be modified to limit access to the SharePoint access account and authorized administrators. This can be further secured by removing the SharePoint access account and using a separate storage access account. This account is identified at the Configure Web Application level, under Replicator Data Folders.



Package Data Path:

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

DC Cache Path:

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

☑ Replicator Data Folders are on a network file server:

User Account:

CORPORATEOFFICE\SPSAdmin

Password:

●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●

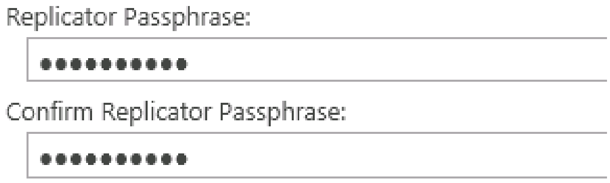
In the diagram at the beginning of this document, this security setting is applied on both the source and target web applications, securing the creation of replication packages on both ends. Furthermore, the data folders are commonly located on a network drive, like a SAN.

Connections

Replication functionality requires that each web application in a pair needs to have a connection created to the other one. Without a connection going each way there is no data access. This is clearly demonstrated in the above diagram, where we have two web applications connected with two connections, one in each direction, allowing for the transfer and reception of packages from both sides. Replicator also offers users the ability to secure their connections through the use of a passphrase, set up at the Web Application Configuration level, and applied for security settings at the Connection Configuration level.

The exception to this rule is when your connections are set up in firewalled mode. Since the server outside the firewall cannot connect to the server inside the firewall, Replicator only requires a single connection. In these cases, you must set a passphrase on the web application outside the firewall and specify it when creating the connection on the web application inside the firewall. This passphrase confirms that the farm administrator creating the connection is authorized by a farm administrator on the other farm.

1. Set a passphrase at the web application level, under Advanced Settings.



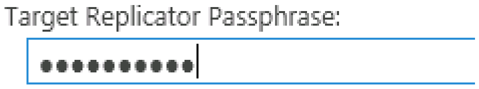
Replicator Passphrase:

●●●●●●●●●●

Confirm Replicator Passphrase:

●●●●●●●●●●

2. Apply the passphrase when creating a firewalled connection, under Target Web Application.

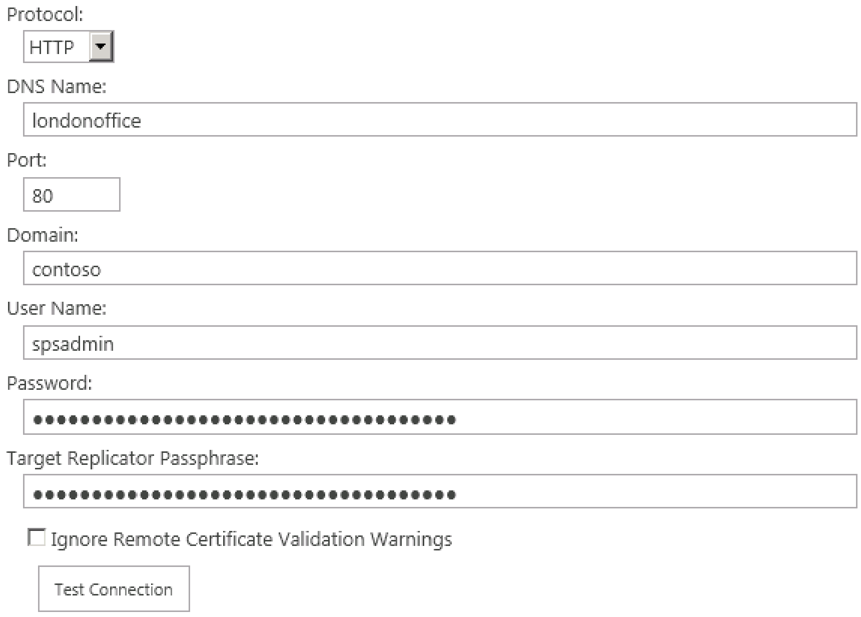


Target Replicator Passphrase:

●●●●●●●●●●

3. Finally, when setting up Replicator, the account specified on the connection configuration page is the only account with permission to download packages from the target web application. This ensures that packages are only downloaded by the allotted account and

cannot be downloaded by others.



Protocol:
HTTP

DNS Name:
londonoffice

Port:
80

Domain:
contoso

User Name:
spsadmin

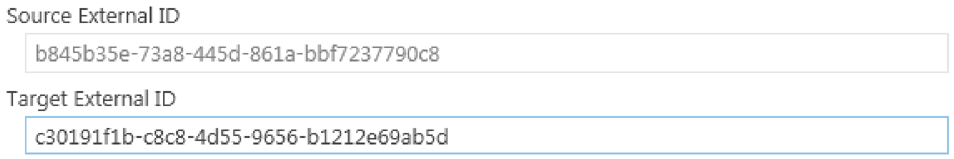
Password:
●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●

Target Replicator Passphrase:
●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●

□ Ignore Remote Certificate Validation Warnings

Offline Replication

When setting up a connection to Transport in offline mode, replicator restricts replication to a specific target using an ID field. This ensures that once replication is brought back online, only the specified target will be able to receive packages during the import procedure.



Source External ID
b845b35e-73a8-445d-861a-bbf7237790c8

Target External ID
c30191f1b-c8c8-4d55-9656-b1212e69ab5d

Packages

As changes are made in SharePoint, Replicator captures these as events and extracts the changes into Replication Packages. These packages are stored on disk as zip files that contain proprietary wrappers that further protect the SharePoint changes from being read.

Farm administrators can specify passwords that will be used to encrypt these packages, ensuring another layer of security. The encrypted zip files are stored in the Replicator Data Folders, transferred to target servers, and then decrypted and applied on the target web applications.

PowerShell

Replicator also allows for controlling and resetting of passwords through PowerShell. The following commands are for users who change their passwords regularly for security purposes. They give you a way to update Replicator with the new passwords in conjunction with the automated process you have for changing passwords.

For more information about the following commands, see the *Metalogix Replicator Command-line Reference*.

Replicator Data Folders

You can use the following command to set up the password for your data folders, configured at the web application level:

Example:

```
PS>Set-ReplicatorWebAppConfig "http://corporateoffice"

                                        -remotepassword pa55w0rd
```

Connection Password

You can use the following command to set up the target passwords for your connections:

Example:

```
PS>Update-ReplicatorConnection -Url http://corporateoffice
-ConnectionName "Corporate to London Connection"
-TargetDomain londonoffice -TargetUserName spadmin -TargetPassword pa55w0rd
```

Service Password

You can use the following command to set up the password for your Replicator account:

Example:

```
PS> Update-ReplicatorAccount -VirtualDirectoryAccount true
-Url http://corporateoffice
-UserAccount corporateoffice\spadmin -Password p4ssw0rd -NewPassword pa55w0rd
```