Metalogix® Replicator 7.4

September 2023

Conflicts and Replicator

This Knowledge Base article details information about conflicts when replicating, as well as the best practices that should be implemented in order to keep conflicts at a minimum. Lastly, a detailed outline of the various conflict handling settings is provided here, describing what occurs with each configuration option, as well as where and how to monitor conflicts.

The examples in this document assume bidirectional replication is configured between two web applications, Corporate Portal and London Branch Portal. Connections are configured between these web applications as follows:

Description of conflicts

Conflict Settings

Best Practices

Description of conflicts

A conflict is detected when Replicator is applying an updated or changed list item and the contents of the event already contain an older item. The conflict is handled only on the web application where the event is being applied. They are handled according to settings defined locally on the inbound web application, on the replicator connection.

In the following scenario, Cora from Corporate updated an announcement at 1:01 PM (Eastern time). Lloyd from the London office updated the same announcement at 1:02 PM (Eastern time). The update from Corporate was sent to London, and the update from London was sent to Corporate.

On Corporate no conflict occurs because the update from London is the most recent change. On London, however, a conflict does occur because an update is sent from Corporate which is older than the update made on London. The way in which this conflict is handled depends on the conflict setting you have configured for the inbound connection on London.

Different conflict settings can be defined for each inbound connection.

Conflict Settings

You can customize the settings of each Replication Connection to deal with conflicts in a specific way. Conflict settings can be set to automatically resolve a conflict using Skip Event or Apply Event settings, or to manually resolve a conflict using the Generate Conflict setting.

When a conflict is detected:
- Skip Event – Do not apply inbound Events against matching content in local Web Application
- Apply Event – Apply inbound Events overwriting matching content in local Web Application
- Generate Conflict – Generate a report for inbound Events that match existing content. Pause replication until the conflict is resolved

Skip Event

Choosing Skip Event as the conflict setting for a replication connection means that in the event of a conflict, the inbound web application automatically keeps the most recent list item. The following is a depiction of how Skip Event functions:

If Skip Event has been set as the conflict setting for the Corporate to London Connection, then London Branch Portal⬚s change will be kept, as it is the most recent change. The conflict at London Branch Portal will therefore be automatically handled by keeping the most recent event.

After replication completes, both web applications have the item that was updated at 1:02 PM.

Apply Event

Choosing Apply Event as the conflict setting for a replication connection means that in the event of a conflict, the web application on the inbound server will automatically apply the inbound update or change, regardless of the time at which the change was made. This allows you to specify that the outbound web application is an authoritative source of content and will therefore automatically be applied.

The following is an example and depiction of how Apply Event functions:

If Apply Event has been set as the conflict setting for the Corporate to London connection, then the inbound change will be applied. The inbound conflict at London Branch Portal will therefore be automatically handled by applying the inbound event.

After replication completes, the London application is updated with the 1:01 PM update.
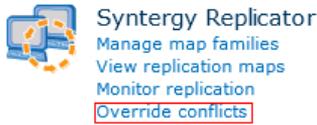
Generate Conflict

Choosing Generate Conflict as the conflict setting for a replication connection means that specified users must decide how to resolve the conflict. In the event of an inbound conflict, replication will be paused, the accounts specified for notifications on the inbound connection will receive an email notification, and a conflict report will be generated on the Monitor Conflicts page. The Monitor Conflicts page is accessed through **Site Settings** or the **Central Administration Application Management** page. The conflict must be resolved by choosing Accept or Reject in the email notification or on the Monitor Conflicts page.

Monitoring Conflicts

The Monitor Conflicts page is accessed through the following:

- **Site Settings** for the inbound site where the conflict was detected.

- **Central Administration Application Management** page for the inbound web application.

The Monitor Conflicts page displays conflict reports, which are only generated for connections with a conflict setting of Generate Conflict. This page displays all the details about the conflict. You must select Accept or Reject in order to resolve the conflict, so that replication can continue.

	Event Time	Event Type	Event Description	Status Message
Accept Reject	12/13/2011 12:03:33 PM	ListItemUpdate	Announcements/Fundraiser December 22, 2011	Attempting to replicate 'Fundraiser December 22, 2011 ' from Portal Map Family - / - Web Site. 'Announcements' contains a more recent copy of 'Fundraiser December 22, 2011 '.

Accept

In the example above, selecting Accept will apply the inbound package therefore behaving in the same manner as Apply Event.

Essentially you are manually applying the Apply Event setting.

Reject

Rejecting will reject the inbound package, keeping the most recently updated event therefore behaving in the same manner as Skip Event.

Essentially you are manually applying the Skip Event setting.

Receiving Conflict Notifications

When a conflict occurs, regardless of the conflict handling setting, we send email notifications to the individual(s) you specify.

Other Considerations

It is important to note that although it is a best practice to set your conflict handling settings to be the same for both outbound and inbound servers within a connection, you are not required to do so. Therefore, if you wanted conflicts handled differently on one server versus another, it is possible to do so by setting each server to a different setting.

You must think of conflicts as a uni-directional event. A conflict will only ever occur at one side, flowing in the direction of outbound to inbound with the conflict occurring on the inbound server. It is therefore the settings on the inbound server for conflict resolution that will be applied.

For More Information

For more information on configuring and monitoring conflicts, refer to the *Metalogix Replicator Reference Guide*.

Best Practices

There are certain practices which can be put into effect in order to minimize the number of conflicts that occur.

Versioning

Turning on the SharePoint versioning setting for your lists and libraries is a safe-guard against possible conflicts. In the event that a conflict does occur, you will always have a history of what occurred to the document.

Replication Scheduling

Setting the Replication Schedule of your Map Families to 'Immediate' is the best practice in order to diminish the number of conflicts that occur. When this is not done, replication packages are backlogged for later replication, allowing for the possibility of a criss-cross in updated versions once the changes are replicated this in turn causes a conflict. If you cannot use immediate replication, then selecting the shortest possible interval, which will reduce the likelihood of a conflict.

Replication Schedule

If Manually is selected, you must use Replicate Now on Manage Map Families to start replication.

Replicate Changes:
- ⦿ Immediately
- ○ Every
- ○ Daily
- ○ Weekly
- ○ Monthly
- ○ Manually

Please note that there is still a risk of conflicts occurring when using 'immediately' as your replication schedule setting. However, the risk lies mainly with backlog and network speed issues. Choose your settings based on your network and farm needs.

Documentation Management

Good and consistent documentation policies will help reduce the risk of conflicts occurring. Checking documents in and out, and limiting permissions while documents are checked-out, significantly reduces these risks.