Internet Synchronization with the Microsoft Jet Database Engine: A Technical Overview

[originally from http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnacc2k/html/intrjet4.asp]

Michael Wachal
Microsoft Corporation

Revision Date: October 2005

For the latest information, see http://support.microsoft.com/support/default.asp.

Contents

Introduction

Internet synchronization was introduced in Jet database engine 3.5 as a way to exchange the data in a replicated database over an Internet or intranet connection. With the release of Jet database engine 4.0, several new features have been introduced to Internet synchronization. Among the new synchronization features in Jet 4.0 are:

Support of the HTTP 1.1 protocol, which eliminates the reliance on FTP for synchronization.
Performance enhancements to reduce transfer times.
A new type of replica visibility called "anonymous" for use with Internet replication.
The addition of several registry keys to control synchronizer timeouts.

Internet synchronization can also be used on a local area network (sometimes called an intranet) in place of standard indirect synchronization. Internet synchronization (unlike indirect synchronization) does not require a Synchronizer on the client computer to synchronize a database.

To initiate synchronization over the Internet, the client computer must make an HTTP connection to an Internet or intranet server. Depending on how the client computer and the server are configured, establishing a connection with the server may result in the display of a logon dialog box at the client computer. In this case, the synchronization will not occur unless a user at the client computer types the appropriate user name and password in the logon dialog box. Once connected, the client computer builds a message file containing the database changes that have occurred since the replicas were last synchronized, and uploads the message file to the drop box on the Internet or intranet server.

The Internet Synchronizer applies these changes to the base replica, unless you specify a replica other than the base replica by using Visual Basic® for Applications code.

> **Note** The base replica is determined by three criteria: it must be a full replica; the Synchronizer must manage it; and it must have the lowest Replica ID of all the managed replicas from the same replica set at that Synchronizer. The base replica is sometimes referred to as the gateway replica.

After these changes have been applied to the base replica, the Internet Synchronizer builds a message file containing the database changes from the base replica (or the replica specified in code), that have occurred since the client and server replicas were last synchronized, and places the message file in the drop box on the Internet or intranet server. The Internet server sends the name and location of the message file back to the client computer. The client computer then transfers the message file from the server, and all the changes specified within the message file are applied to the client replica.

New Functionality

Internet synchronization allows users of a replicated database to exchange updates by means of a series of message files transferred by using either the FTP or HTTP protocol. The protocol used for transfer of the message files is dependent on the combination of the Internet protocols supported on both the client and the server computers. If both the client and server support the HTTP 1.1 protocol, HTTP will be used for transfer of the message file; otherwise, FTP will be used. When using

HTTP 1.1, a client computer can now synchronize from behind a properly configured proxy server to a Synchronizer on the Internet. The reverse configuration, a Synchronizer behind a proxy server, has not been tested and is not supported by Microsoft. The use of a proxy server is not supported when using the FTP protocol. The following table shows the minimum requirements for Internet synchronization and the protocols that will be used by various Internet servers and clients.

		Server		
		IIS 2.0/3.0	**IIS 4.0/5.0/6.0**	**Netscape**
Client	IE 3.02	FTP	FTP	N/A
	IE 4.x/5.0/6.0	FTP	FTP/HTTP	HTTP

Encryption Settings: In Jet database engine 3.5, all message files transferred through the Internet were encrypted. The encryption process increases the amount of time required to complete Internet synchronization. The performance of Internet synchronization in Jet database engine 4.0 has been improved by using the encryption status of the source database to dictate the encryption status of the message files. If a database is encrypted, the message file created from it will be encrypted; otherwise, the message file will not be encrypted. If data security is a concern in your replicated applications, you will have to make sure that all of the databases in your replica set are encrypted prior to use for Internet synchronization.

Replica Visibility Types: In Jet database engine 3.5, there was only one type of replica called Global. Jet database engine 4.0 adds two new types of replica visibility: local (not discussed in this paper) and anonymous. Anonymous replicas are designed to limit the amount of data stored about the members of a replica set and help control synchronization topology. Because of this, an anonymous replica is an excellent choice for a client replica. Because of the limited information that is stored about anonymous members of a replica set, the **Synchronizer** window will not be cluttered with icons representing client replicas. Anonymous replicas can only synchronize with their parent replicas (that is, the member of the replica set that was used to create the anonymous replica) and that parent replica must be managed by Replication Manager.

Customized Timeout Values: Five new registry keys have been added to allow you to customize the timeout values for many of the processes of the Internet Synchronizer. The default settings for these keys allow the most flexibility and error recovery during Internet synchronization. You may be required to modify these settings to get an optimum configuration for your replicated application. The client program will be unavailable during Internet synchronization, including during the periods of time that it is waiting for a timeout to occur. The Jet database engine creates these keys in the following location in the Windows® Registry:

HKEY_Local_Machine\Software\Microsoft\Jet\4.0\Transporter\

These timeouts are stored in the Windows Registry as hexadecimal DWORD values and can only be changed by using a registry editor such as Regedit or Regedt32.

The names and default values are as follows.

Key Name	**Default Value (sec)**	**Description**
Timeout_Internet_Client	3600	Determines the length of time the client (Access, Replication Manager, or the Synchronizer) will wait for a return message from the server once the initial message has been sent.
Timeout_Internet_Connect	120	Determines the length of time the client will wait to get an FTP connection to the Internet server. If you are using FTP to synchronize and you have a busy server, increasing this value may increase the chance of a successful synchronization.
Timeout_Synch	60	Determines the amount of time the Internet Synchronizer will wait for the target database if another Synchronizer is using it. The higher this value, the more pending synchronizations can be waiting on the Internet server.
Timeout_Synch_Internet_Server	3600	Synonymous to Timeout_Internet_Client, but is set on the server and affects the Internet Synchronizer.
Timeout_Synch_Lock	60	Determines the amount of time the Synchronizer will wait to obtain a Jet lock. If you get frequent synchronization failures due to contention or locking problems, try increasing this value.

Preparing for Internet Synchronization

Before you can synchronize over the Internet, you must properly configure your Internet server and the Replication Manager. If you are new to the Internet, here is the easiest way to configure everything.

1. Set up your Internet server with an operating system and server software. For example, you can use Microsoft® Windows Server 2003 family with Microsoft Internet Information Services (IIS) 6.0.

Note You can also use Windows NT 4.0 with IIS 4.0 or Windows 2000 Server with IIS 5.0.

2. Install Microsoft Access 2000, Access 2002, or Access 2003 on the same computer. Install Microsoft Replication Manager on the same computer. Replication Manager is included as part of the Microsoft Office 2000 Developer product (MOD 2000) or Microsoft Office XP Developer (MOD XP) product.

   Note The Replication Manager runs on Intel server platforms only, and supports the Microsoft Internet Explorer and Netscape server platforms.

   Note Replication Manager is not available as part of Microsoft Visual Studio Tools for the Microsoft Office System (Visual Studio Tools for Office). For more information about Visual Studio Tools for Office, see Microsoft Knowledge Base Article – 828089: INFO: Migrating from Microsoft Office XP Developer. Replication Manager 4.0, included with Microsoft Office 2000 Developer Edition and Microsoft Office XP Developer Edition, works to configure Internet synchronization for Access 2003 because it uses the same Jet 4.0 database engine as Access 2000 and Access 2002. Users who want to configure Internet replication will need to get Replication Manager from the Office 2000 Developer Edition or Office XP Developer Edition.

3. Create a replica on the Internet server computer, and manage it using the Replication Manager. This will "stamp" the replica with information about the Internet server's HTTP address and other internal system information.
4. Create a copy of the replica, and distribute this copy to your users. When they open the replica in Microsoft Access and synchronize, they will be able to synchronize back to the replica on the Internet server by using the automatically configured HTTP address.

This paper describes configuring your Internet server, configuring Microsoft Replication Manager 4.0, and creating and distributing the replica set. For more information about installing Microsoft Access 2000, Access 2002, or Access 2003, see the documentation provided with your product.

Configuring Your Internet/Intranet Server

The first step in preparing for Internet synchronization is to configure your Internet or intranet server. The following section details the steps for configuring Internet Information Services (IIS) 6.0 on Windows Server 2003 family.

For Internet or intranet synchronization to be successful, you will need two directories (folders) managed by your Internet server. The first directory should be part of the HTTP service. This directory is used to house the copy of the Internet Synchronizer program (mstrai40.exe) that handles the exchange of information with Internet or intranet replicas that are requesting synchronization. Because the Synchronizer will be running in this folder, it must have read and execute permissions enabled for it in the HTTP service. Either create your own new directory in IIS 6.0 or use an existing directory, such as the Scripts directory if you are using IIS 4.0 or IIS 5.0. The second directory will be used as the Internet drop box. This directory serves as the exchange point for the message files that hold the database changes from each replica involved in the synchronization. Because both the Synchronizer and the remote replica will be using this directory, it needs both read and write permissions enabled on the server. Because Jet database engine 4.0 supports the HTTP 1.1 protocol, the FTP service, the HTTP service, or both can manage this drop box. For maximum flexibility, you will want to make your Internet drop box available to both the FTP and the HTTP service.

Note For this to be properly configured in Replication Manager, you must have identically named Virtual Directories in both the FTP and HTTP services pointing to the same directory on your physical hard disk. This is explained in more detail in the configuration steps later in this paper.

The following examples for configuring an Internet or intranet server are specific to IIS 6.0. They also can be applied to IIS 4.0 or IIS 5.0 with minor changes in the menu names. The steps to configure your Internet or intranet server may be different. Microsoft Access support engineers do not directly support the configuration of Internet or intranet servers. If you have questions regarding the configuration of an Internet or intranet server, contact the manufacturer of that server. For questions about Microsoft Internet servers, visit our support site at http://support.microsoft.com/ and choose the most appropriate option for support.

Microsoft Internet Information Services 6.0 for Windows Server 2003 Family

You can configure IIS 6.0 by using the Internet Information Services Manager.

For more information about how to install and set up IIS and the FTP server in Windows Server 2003, see Microsoft Knowledge Base Article – 323384: How To Set Up an FTP Server in Windows Server 2003.

For the purpose of this example, you create the Scripts directory for the location of the Internet Synchronizer, and then you create a directory named Drop box to be used as the Internet drop box.

1. Create a directory called "Drop box" on your Internet server under the C:\InetPub\ folder so that the final path to your directory will be C:\InetPub\Drop box.
2. Create a directory called "Scripts" on your Internet server under the C:\InetPub\ folder so that the final path to your directory will be C:\InetPub\Scripts.

   Note The Scripts directory is created by default when IIS 5.0 or IIS 4.0 is installed.

3. Click **Start**, point to **Administrative Tools**, and then click **Internet Information Services (IIS) Manager**.
4. Expand the Computer icon for your computer name. Check to make sure both the **Default FTP Site** and the **Default Web Site** are running. If they are listed as **Stopped**, select the site and click the **Start** button. The **Start** button looks like the play button on a VCR and is on a toolbar near the top of the console. See Figure 1.

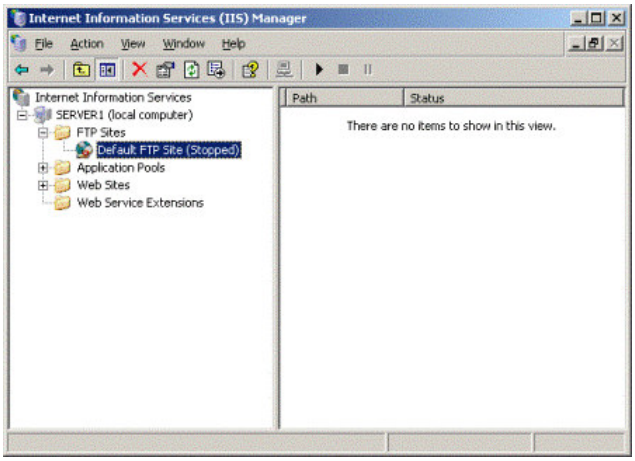


Figure 1. Expanded Internet Information Services folder

5. Click the **Default Web Site** to select it. Drop down the **Action** list, point to **New**, and then click **Virtual Directory**. See Figure 2.

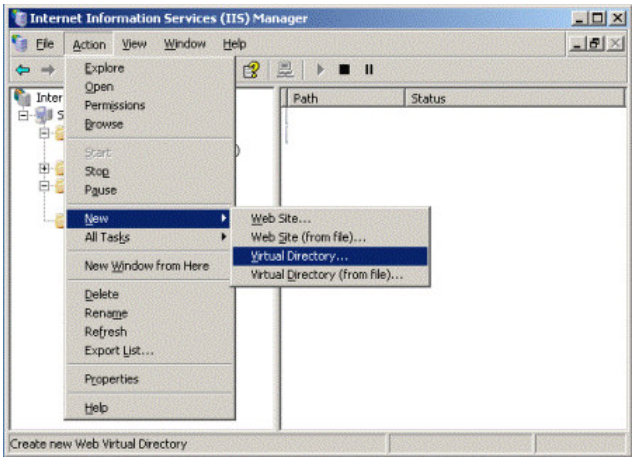


Figure 2. Locating the Virtual Directory

6. A wizard walks you through creating a Virtual Directory. Add the folder that you created in step 1 (C:\InetPub\Drop box) to the Default Web Site.
   a. On the first page of the wizard, click Next.
   b. On the second page of the wizard, type **Drop box** in the **Alias** box, and then click **Next**.
   c. On the third page of the wizard, enter the path to the Drop box directory you created in step 1, or click **Browse**, select the directory, and then click **Next**.
   d. On the fourth page of the wizard, select the **Read** and **Write** check boxes. Make sure that both **Run scripts** and **Execute permissions** are disabled, and then click **Next**.
   e. On the last page of the wizard, click **Finish**.
7. Repeat steps 5 and 6 (including substeps) to create another virtual directory with the alias "Scripts" that maps to the Scripts directory you created in step 2.

   Note The Scripts directory is created and managed by default when IIS 5.0 or IIS 4.0 is installed.

8. Select the Scripts directory in the Internet Information Services (IIS) Manager, and then click **Properties** on the toolbar. See Figure 3.

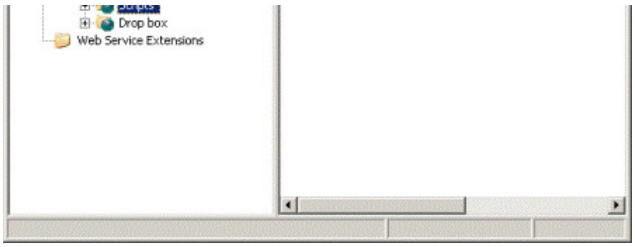


Figure 3. Locating Scripts directory in IIS Manager

9. In the **Scripts Properties** dialog box, click the **Directory Security** tab, and then click **Edit** under **Authentication and access control**.
10. Make sure that **Enable anonymous access** is selected, and then click **OK**.
11. In the **Scripts Properties** dialog box, click the **Virtual Directory** tab, make sure the **Execute** permissions are set to **Scripts and Executables**, and then click **OK**.

    Note You will get an IIS Manager message that asks if you are sure you want to do this. For information about security concerns, see the "Securing the Internet Server" section later in this paper.

12. If you want maximum flexibility for Internet synchronization, like support of Internet Explorer 3.02 clients, you need to create an FTP alias for the same Drop box that was configured for HTTP. Click once on the **Default FTP Site** to select it, and then click **Properties**.
13. In the **Default FTP Site Properties** dialog box, click the **Security Accounts** tab.
14. Click to select the **Allow anonymous connections** check box, and then click **OK**.

    Note For information about security concerns, see the "Securing the Internet Server" section later in this paper.

15. With the **Default FTP Site** still selected, drop down the **Action** list, point to **New**, and then click **Virtual Directory**.
16. Using the wizard again, add a Virtual Directory for the Drop box folder that you created in step 1 (C:\InetPub\Drop box) to the **Default FTP Site**.
    a. On the first page of the wizard, click **Next**.
    b. On the second page of the wizard, type **Drop box** in the **Alias** box, and then click **Next**.
    c. On the third page of the wizard, enter the path to the Drop box folder that you created in step 1; or click **Browse**, select the directory, and then click **Next**.
    d. On the fourth page of the wizard, click to select the **Read** and **Write** check boxes, and then click **Next**.
    e. On the final page of the wizard, click **Finish**.

When setting up Microsoft Jet 4.0 Internet replication on a computer running Microsoft Windows Server 2003 with IIS 6.0, there are several additional required configuration steps:

NTFS Permissions
MIME Types
Web Service Extensions

NTFS Permissions

The following are some NTFS permissions that you should set or verify for the two directories in Windows Server 2003:

C:\InetPub\Scripts

No change is required. **Read & Execute** permission is assigned by default to the Users group.

C:\InetPub\Drop box

Assign **Write** permission to the Users group; by default this permission is not granted to users on Windows Server 2003

Folder containing the hub replica

No change is required. **Read & Execute** permission is assigned by default to the Users group.

To access NTFS and sharing permission settings

1. Right-click the particular folder and select **Properties**.
2. Click the **Security** tab.
3. Select the Users (machine name\Users) group and assign permissions.
4. If the folder is shared, click the **Sharing** tab. It is not required that you share the folder.
5. Click the **Permissions** button.
6. Select the **Everyone** group, and assign permissions.

MIME Types

Add the following file extensions and specify a MIME type of "Application/octet-stream" (no quotation marks) for each extension:

.msg
.tmp

Note The new MIME types can be added at the server or the Web site level.

To access the IIS MIME server settings, follow one of these sets of steps:

To add MIME types to the server

1. Click **Start**, point to **Administrative Tools**, and then click **Internet Information Services (IIS) Manager**.
2. To add the new MIME types to the server, right-click the server name and select **Properties**.
3. Click **MIME Types**.
4. Click **New**.
5. Enter the extension and MIME type for the first new file extension.
6. Repeat the previous two steps for the second new file extension.

To add MIME types to the Web site

1. Click **Start**, point to **Administrative Tools**, and then click **Internet Information Services (IIS) Manager**.
2. To add the new MIME types to the Web site, expand the Web Site folder beneath the server name.
3. Right-click the appropriate site, or the Default Web Site if there are no other sites, and select **Properties**.
4. Click the **HTTP Headers** tab.
5. Click **MIME Types**.
6. Click **New**.
7. Enter the extension and MIME type for the first new file extension.
8. Repeat the previous two steps for the second new file extension.

Web Service Extensions

Change the status for the following Web service extensions:

All Unknown CGI Extensions
WebDAV status

To change the Web Services Extensions settings

1. Click **Start**, point to **Administrative Tools**, and then click **Internet Information Services (IIS) Manager**.
2. Click the Web Service Extensions folder beneath the server name.
3. Select **All Unknown CGI Extensions** in the Web Service Extension column.
4. If the Status is Prohibited, click the **Allow** button to the left of the extensions list. If you do this, you will see an IIS Manager message, asking if you want to allow all unknown CGI extensions. Click **Yes**. For more information, see the "Securing the Internet Server" section later in this paper.
5. Select the **WebDAV** extension.
6. If the Status is Prohibited, click the **Allow** button to the left of the extensions list.

You have now added the required directories to your HTTP and FTP services to use Internet or intranet synchronization. From here, you need to configure the Microsoft Replication Manager. To do so, see the "Configuring Microsoft Replication Manager 4.0" section later in this paper.

Microsoft Personal Web Server 4.0 for Windows 95/98

Internet synchronization is not supported by Microsoft Personal Web Server 4.0 on Windows 95 and Windows 98 because it does not support the FTP service and you cannot set Write permissions on an HTTP directory. For Internet synchronization to be successful, you must be able to send a message file to either an FTP or HTTP drop box.

Configuring Microsoft Replication Manager 4.0

To configure Microsoft Replication Manager 4.0 on your Internet server for use with Internet replication, follow these steps:

1. Install Microsoft Replication Manager 4.0 on your Internet server.
2. Start Microsoft Replication Manager 4.0.
3. If this is the first time you have run Microsoft Replication Manager, you will be prompted to configure it. If this is not the first time and you are not prompted, on the **Tools** menu, click **Configure Microsoft Replication Manager**.
4. Read the text on this screen of the wizard, as shown in Figure 4, and then click **Next**.

Figure 4. Configuring Microsoft Replication Manager Wizard

5. If this Synchronizer will participate in Indirect Synchronization, click to select **Support indirect synchronization**, and then click **Next**.

   If this Synchronizer will not be used for Indirect Synchronization, do not select it, click **Next**, and go to step 8.

6. Read the text on this screen of the wizard, and then click **Next**.
7. Select a shared network folder on this or another computer, and then click **Next**. The folder you are selecting will be used as a drop box folder for indirect synchronization of replicas over your local area network.

   Note You may use the same FTP/HTTP folder that you created as your drop box for Internet synchronization in step 1 of the previous section as the indirect drop box; but it will be possible for outside users to read and write files to your FTP folder.

8. When prompted, if your computer is an Internet server, click **Yes**, and then click **Next**.
9. When prompted, if you want to synchronize a replicated database over the Internet, click **Yes**, and then click **Next**.
10. Enter the name of the Internet or intranet server, and then click **Next**. If the computer is an Internet server that is accessible from the World Wide Web, do not include "http://" or "www" with the server name. For instance, if your Internet server is accessible over the World Wide Web as "http://www.ABC.com," you should only enter "ABC.com" as the Internet server name. If the computer is an intranet server, you should enter the name of computer, as the following illustration in Figure 5 shows.

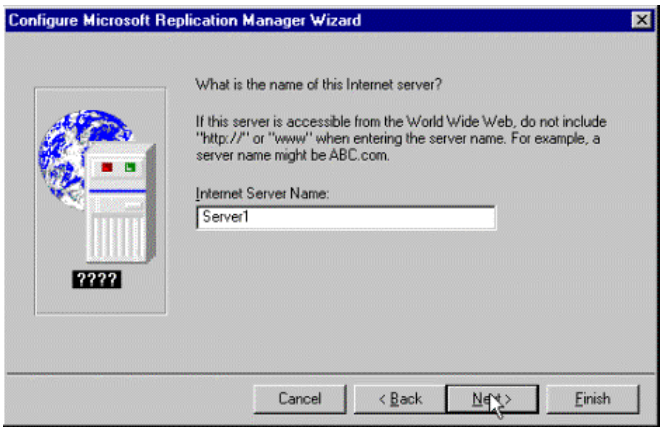
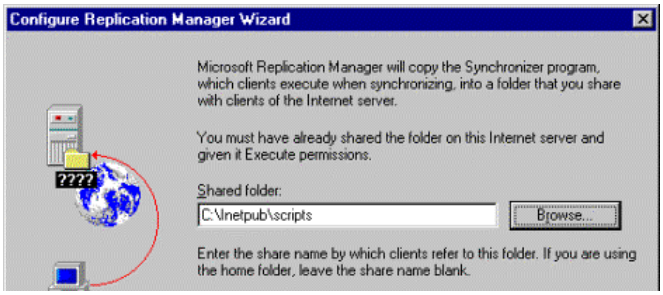


Figure 5. Enter name of Internet server

11. Click **Browse**, and select the Scripts folder discussed in step 4 of the procedure in "Configuring your Internet/Intranet Server" section earlier in this paper.
12. The alias name `Scripts` should automatically appear in the share name text box. If it does not, type it in, and then click **Next**. See Figure 6.

    Note If you are using a directory other than the Scripts directory as your shared directory, you should provide the path and share name for that directory instead.



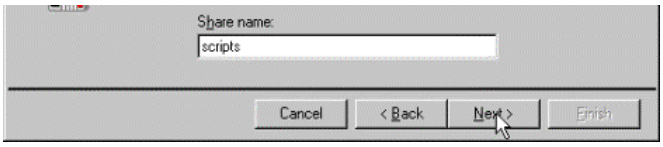


Figure 6. Share name text box

13. Type `Drop box` in the FTP/HTTP alias name text box, and then click **Next**. See Figure 7.

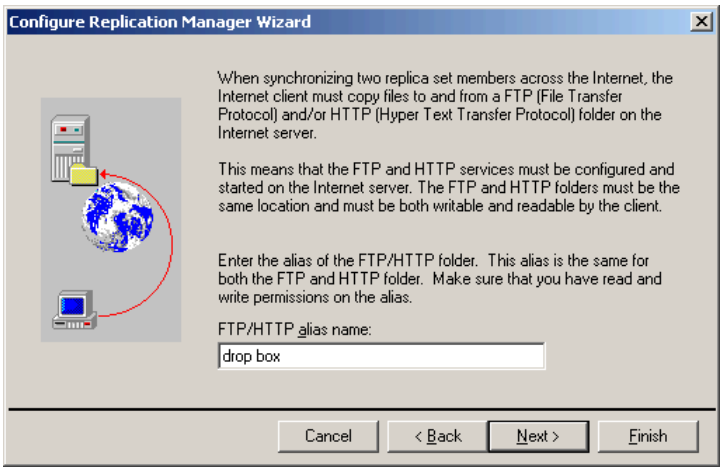


Figure 7. FTP/HTTP alias name text box

14. You can select the priority of the types of synchronization that will be tried when you attempt to synchronize two replicas. The default order is Indirect, Internet, and then Direct. To change this order, use the arrow keys. Once you have set the priority of synchronization types, click **Next**. See Figure 8.

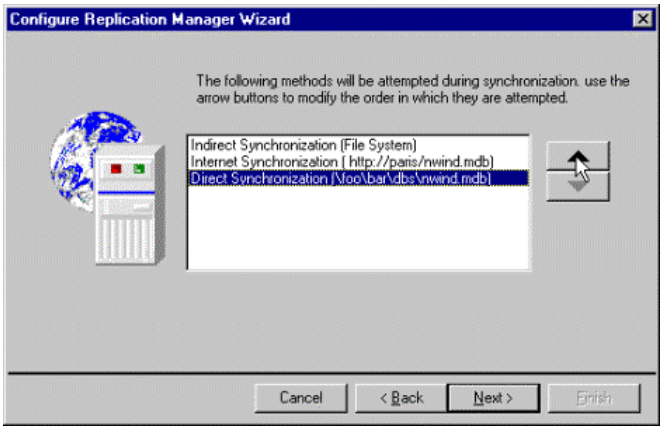


Figure 8. Using arrow buttons to set priority of synchronization types

> **Note** If you don't select **Support Indirect Synchronization** in step 5, you will not see the **Indirect Synchronization (File System)** item in the method list.

15. Select a path for the log file, and then click **Next**.
16. Select a name for the Synchronizer, choose whether you want the synchronizer to be run automatically when the computer starts, and then click **Finish**.

Distributing a Replica Set on the Internet/Intranet

After configuring Microsoft Replication Manager on your Internet or intranet server, you must manage at least one member of the replica set on the server. This stamps the replica with the Internet address of the Synchronizer managing it. After managing the replica in Microsoft Replication Manager, you should synchronize with other members of the replica set. This propagates the Internet address of the Synchronizer that is managing the hub replica to other members of the replica set, and enables them to synchronize to it over the Internet.

After a replica set has been enabled for Internet synchronization, you must determine the best way to distribute the set to your users. There are several ways to accomplish this:

Place a replica on a shared folder on the network and allow users to copy the file to their local hard disks. (Because this replica

need only be copied by users, the share can be read-only.)
Send users a copy of the replica on disk (Floppy, CD, or removable media) that they can copy to their local hard disks.
Put a copy of the replica in an FTP directory where users can connect and download it.

In all cases, you must make sure that the replicas made available for distribution were created with knowledge of the Internet server that is managing the hub replica. You can ensure this by using Replication Manager to create a new replica from the managed hub, and then distribute that replica. Another thing to consider is the use of anonymous replicas at the Internet client computer. Anonymous replicas can only be created through the Microsoft Access user interface or through Jet and Replication Objects (JRO) code. An example of creating an anonymous replica is included later in this paper.

If you are distributing your replicas using FTP, you do not have to manage the replicas in the shared folders. The following diagram in Figure 9 illustrates how you might distribute a replica set for Internet synchronization using FTP. In this diagram, the Managed Replica would be in an unshared folder, and a copy of that replica is placed in an FTP folder. The FTP folder used to distribute the replica can be different than the Drop box folder (discussed earlier) and need only have Read permissions.

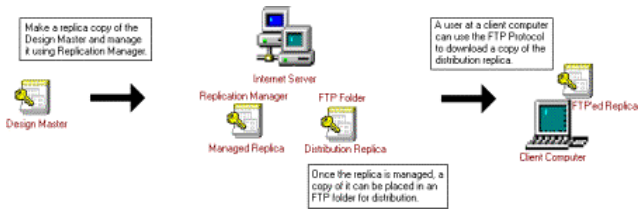


Figure 9. Distributing a replica set for Internet synchronization using FTP

To properly distribute a replica set on the Internet or intranet, you will have to convert a database to a Design Master, make a hub replica that is managed by the Replication Manager, and create a distribution replica.

Creating a Design Master

1. Open Microsoft Replication Manager.
2. On the **Tools** menu, click **Convert Database to Design Master**.
3. After you select a source database, the Convert Database to Design Master wizard appears. Read the information on the first page, and then click **Next**.
4. Click to select **Yes, I want to make a backup**, note the directory location of the backup file, and then click **Next**. It is important to make a backup file to maintain a copy of your original database in a non-replicated form. See Figure 10.

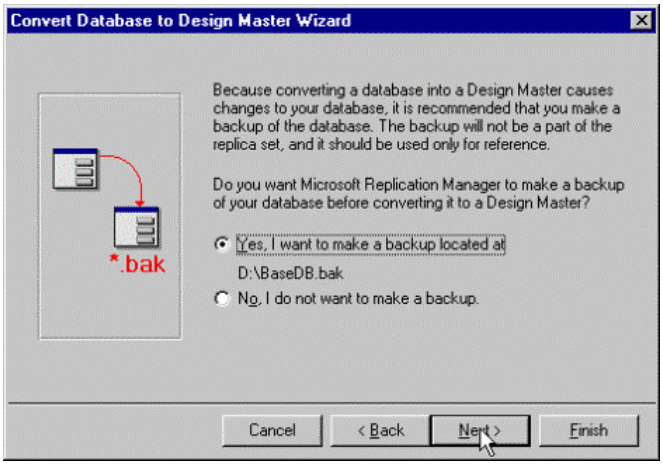


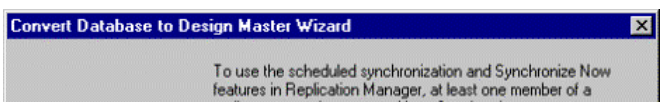
Figure 10. Making backup of database before converting to Design Master

5. Enter a descriptive name for the replica set, and then click **Next**.
6. Click to select **Make all objects available to the entire replica set** to make a full replica, and then click **Next**.
7. Click to select **I want to be able to create read/write replicas**, and then click **Next**.

   Note If you select the option to make read-only replicas, you will not be allowed to enter data into any of the replicas made from this Design Master.

8. Click to select **No, don't manage it with this synchronizer**, and then click **Next**.

   Note It is recommended that you do not manage the Design Master, but instead use a replica as the hub for synchronization. See Figure 11.



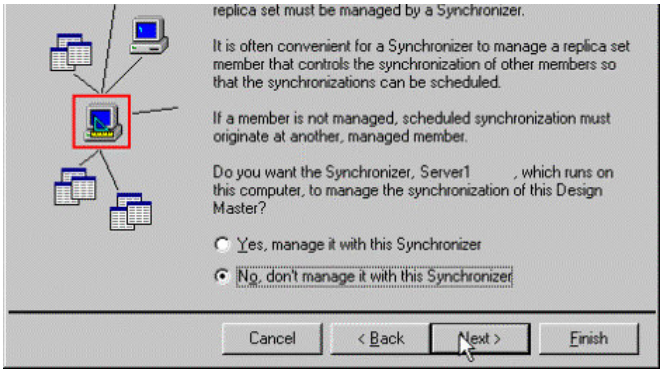


Figure 11. Managing or not managing the synchronization of the Design Master

9. Click **Finish** to complete the creation of the Design Master.

Creating a Hub Master

1. From the Microsoft **Replication Manager**, on the **File** menu, click **New Replica**.
2. The **Create New Replica** wizard appears. Read the information on the first page, and then click **Next**.
3. Type the path to the Design Master that you created earlier into the **Source replica set member** box, or click **Browse** and select the Design Master.
4. Type the path and name for a new replica. This replica can be located in any directory on the Internet server. See an example of the **Create New Replica Wizard** screen in Figure 12.

> **Note** Internet synchronization will not work properly if your managed hub replica is located on a different computer and managed using a UNC path. If you must save your managed hub replica to a different computer, you will need to map a drive from the Internet server to the computer where the hub replica is stored. You can then manage the replica using the drive letter.

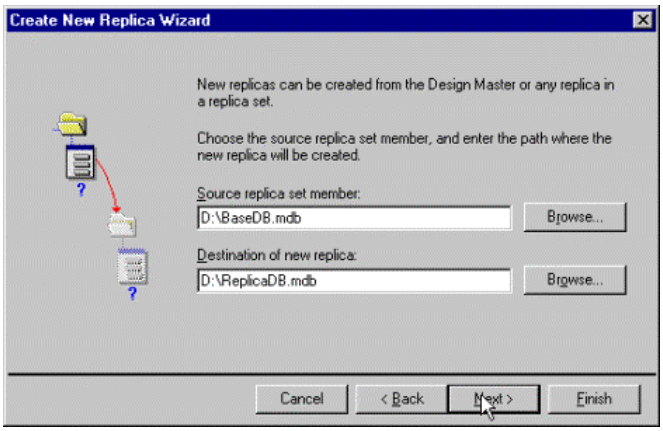


Figure 12. Create New Replica Wizard screen

5. Click **Next**.
6. Click to select **I want to be able to make data changes in the replica**, and then click **Next**.
7. Click to select **Yes, manage this replica with this Synchronizer**, and then click **Next**. See Figure 13.

> **Note** Although it is possible to manage a partial replica as the hub replica on your server, it is not a good idea. The Microsoft Jet Synchronizer will only use a partial replica for synchronization if it is the only member of the replica set that is managed. Also, it is important to remember that you can never synchronize a partial replica to another partial replica. So if you are distributing partial replicas, you must manage a full replica.

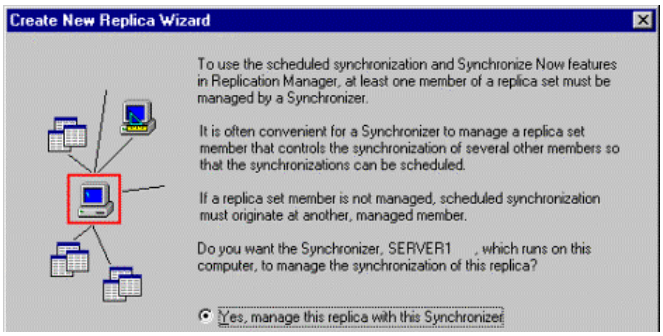


Figure 13. Managing the replica with the Synchronizer

8. Click **Finish** to create the new replica.
9. On the **File** menu, click **Managed Replicas**.
10. In the **Managed Replicas** dialog box, select the replica that you created in the steps above, and then click **Open**.
11. The **Replication Manager** window will now show you a topology including a Synchronizer and your unmanaged Design Master.

Creating an Anonymous Replica for Distribution

(Optional)

While it is not required to use anonymous replicas as the client databases, several design changes in Jet database engine 4.0 make anonymous replicas ideal for Internet replication:

An anonymous replica can only synchronize to its parent replica, so topology of synchronization can be controlled. (For successful synchronization to occur, all anonymous replicas must be created from the Managed hub replica on the server.) The information about anonymous replicas that is stored in the MSysReplicas table of its parent is periodically purged to reduce the size of the parent database. This will also reduce the amount of clutter in the **Synchronize**r window of the **Replication Manager**.

To create an anonymous replica for distribution, you will have to open the managed replica in Microsoft Access 2000 or later. You can either open the managed replica directly from Access, or use **Replication Manager** to start Access with the managed database selected. See Figure 14.

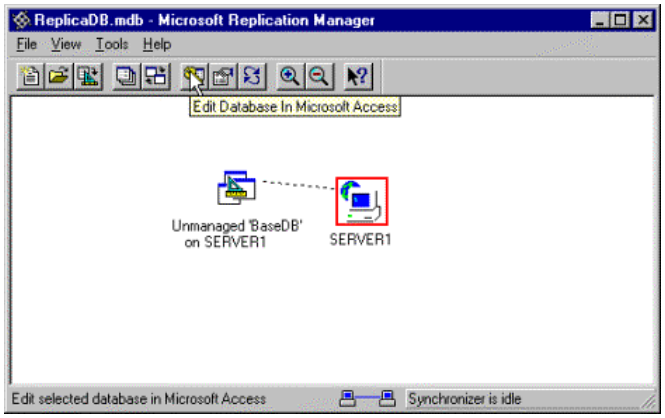


Figure 14. Starting Access using Replication Manager

Once Access is running, you can create the anonymous replica.

1. On the **Tools** menu, point to **Replication**, and then click **Create Replica**. (If the **Replication** command is not visible, you have adaptive menus turned on. Move the pointer to the bottom of the **Tools** menu, and hover over the double arrow. This will expand the **Tools** menu to show all possible commands.)
2. In the **Location of New Replica** dialog box, select a location for your replica and give it a name. In the **Save as type** box, select **Microsoft Access Databases Anonymous (*.mdb)**, and then click **OK**. See Figure 15.

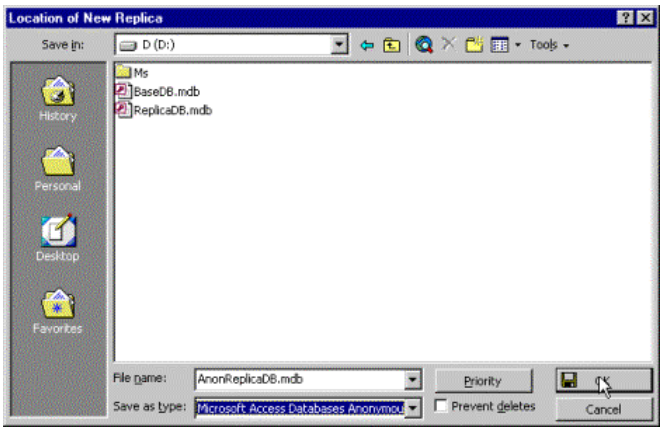


Figure 15. Location of New Replica dialog box

After the anonymous replica has been made, it can be distributed using any means appropriate for your application. Any copies of an anonymous replica will also be anonymous replicas with the same Managed hub replica as its parent.

Synchronizing the Replica

1. Use your selected method of distribution to get a copy of the managed replica or the anonymous replica to the remote client computer.
2. Open the replica in Microsoft Access.
3. On the **Tools** menu, point to **Replication**, and then click **Synchronize Now**.
4. In the **Synchronize Database** dialog box, click to select the **Directly with Replica** option, select the address to the Internet or intranet server in the combo box, and then click **OK**. See Figure 16.

   Note Even though the option says **Directly with Replica**, by selecting the Web address, you will be using Internet synchronization.

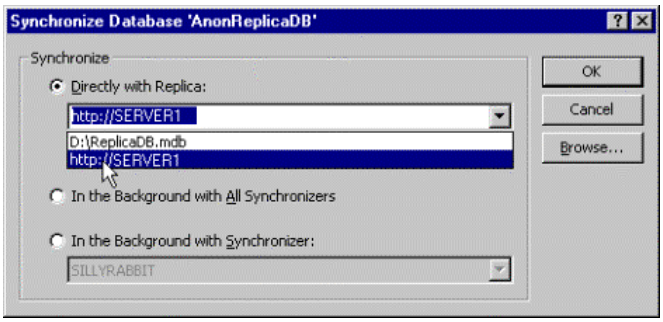


Figure 16. Synchronize Database dialog box

5. When you receive confirmation that the synchronization was complete, click **OK**. Microsoft Access will close and re-open the database. You can now either continue to use the replica normally or resolve any conflicts that occurred during synchronization.

Securing the Internet Server

Limited Directory Security is available for use with Internet Synchronization when working with IIS. When an FTP or HTTP service is configured for Anonymous login, you can limit the number of users that can access the service by individual user IP address, Network ID, and Sub-net Mask or Domain. If your Internet Server supports the use of both FTP and HTTP, then directory security must be implemented for the drop box **Virtual Directory** in both services.

FTP Directory Security

Directory security settings are configured from the Internet Information Services (IIS) Manager by opening the **Properties** dialog box for the virtual directory on which you want to set up security. Once the **Properties** dialog box is open, click the **Directory Security** tab. You have two options for security configuration. By default, all users are granted anonymous access to the folder, and you can add specific users, groups, or domains that will be denied access. These instructions focus on the second option, in which you deny all users access to the directory, and then add specific users, groups or domains that will be granted access.

Note If you plan to secure your Internet server, you must specifically grant access permission to the IP Address being used by your Internet Server, together with any other users.

1. Click to select **Denied Access**.
2. Click **Add** to grant anonymous access to a user, group, or domain.
3. In the **Grant Access** dialog box, you can choose to grant access to a **Single computer**, **Group of computers**, or **Domain name**. Select the type of access you want to grant.

   Note The access type "Domain name" is available only for HTTP service in IIS 6.0.

   Single computer. You can specify either the IP Address for a single user's computer or, if your system supports Domain Name Services, you can click the DNS Lookup button, and then specify the DNS computer name of the user's computer. Click **OK** to save the entry.

   Group of computers. You can specify a group of computers to grant access to by specifying the Network ID and Subnet Mask for the group of computers. Every computer in the specified group will have access to the directory. Click **OK** to save the entry.

   Domain name. You can specify a domain name to grant access to every computer in the domain. Granting permissions by domain name is by far the slowest of these methods.

HTTP Directory Security

Directory security for the HTTP service is configured similarly to the FTP service.

1. Open the **Properties** dialog box for the drop box **Virtual Directory**, and click the **Directory Security** tab.
2. Under the IP Address and Domain Name Restrictions section, click **Edit**.
3. In the **IP address and domain name restrictions** dialog box, configure directory security as described earlier in the previous section, "FTP Directory Security."

Directory Security Limitations

Incorrect configuration of the directory security settings can prevent users from accessing the FTP and HTTP services. If this happens, synchronization attempts by your users will fail. You should fully understand TCP/IP Networking, IP Addressing, and the use of subnet masks before using these options.

You should be aware of the following limitations when you use directory security with replication:

If access is being granted to a single computer, the users need to have static IP addresses.
Granting access by domain name is very slow.
If the users accessing your Internet Server are behind a Proxy Server, you should grant access to the Proxy Server's IP address. Be aware that this will grant access to all users of that Proxy Server.
Placement of an Internet Synchronizer behind a Proxy Server has not been tested and is not supported by Microsoft.

Common Jet 4.0 Internet Replication Deployment Errors

The following synchronization errors and their causes are associated with incorrect IIS and NTFS settings:

Failure to write to an Internet handle

NTFS permissions on the drop box do not allow Write permissions for the anonymous user.
IIS permissions on the drop box virtual directory do not allow Write permissions for the anonymous user.
The .tmp extension is not a recognized MIME Type.
The WebDAV extension is prohibited under Web Service Extensions.
The URLScan utility has been installed with a configuration that does not permit certain processes that are required for HTTP or FTP synchronization.

Internet Synchronizer exited unexpectedly on the server. Look at the partner replica exchange history on the Internet server to figure out the problem.

Unknown CGI Extensions are prohibited.
Scripts folder is not set to **Scripts and Executables**.
The Internet Synchronizer program (Mstrai40.exe) is not in the Scripts folder.

Internal Internet Failure

The .msg extension is not a recognized MIME Type.

Invalid HTTP Address

This problem may occur when you try to use Jet 4.0 Service Pack 7, Jet 4.0 Service Pack 8, or the 837001 hotfix. See "Jet Database Tips" in the following section of this paper for information about correcting this problem.

For more information about replication errors, see the following articles:

Microsoft Knowledge Base Article – 304026: ACC2000: Troubleshooting Common Replication Errors
Microsoft Knowledge Base Article – 262833: MOD2000: Errors When You Use Partial Replicas with Indirect or Internet Replication
Microsoft Knowledge Base Article – 311068: ACC2002: "Failure to Write to an Internet Handle" Error Message After You Install the URLScan Utility

Tips and Tricks

Internet/intranet synchronization works well when the replica set remains small (fewer than 10 individual replicas) and the number of data inserts and updates are limited. When determining if Internet/intranet replication will suit your needs, also consider the hardware and network requirements for your application. To implement Internet/intranet replication properly requires a network connection capable of handling the appropriate traffic, an Internet server that can handle enough user connections, and the hardware resources to manage running the different programs involved in synchronization, including the Internet Server, the Internet Synchronizer, and the Jet database engine. Frequently, replicated applications that work well in a small test environment will become slow or fail altogether in a much larger production environment. Make sure that when you test a replicated application, the test environment adequately duplicates the production environment not only in design, but also in resource usage.

While not considered part of the standard configuration required for successful Internet/intranet synchronization, you can tweak some settings to improve synchronization success when working with large replica sets or applications requiring frequent or numerous data inserts or updates. Most of these settings involve modification of the Windows Registry or changes to IIS. Before making changes to the Windows Registry, you should back up the registry.

IIS Tips

The amount of time required for the Internet Synchronizer to run is proportional to the amount of data being exchanged. When you attempt to exchange a large number of data changes or fewer data changes involving more data, it is possible that the Internet Server may close the connection to the client before the exchange is completed. A timeout setting in IIS controls the amount of time before the server will close a connection.

CGI Script Timeout: The CGI Script Timeout determines the amount of time a CGI script is given to execute and return a value before the operation is stopped. If you are experiencing synchronization failures during long exchanges, you may benefit from increasing this timeout in the Internet Service Manager.

Jet Database Tips

Make sure you have the latest updates for the Jet database engine and the replication files. For more information, see the following articles:

Microsoft Knowledge Base Article – 239114: How To Obtain the Latest Service Pack for the Microsoft Jet 4.0 Database Engine
Microsoft Knowledge Base Article – 870753: Description of the Jet 4.0 Database Engine Post-837001 Hotfix Package: July 21, 2004
Microsoft Knowledge Base Article – 321076: Updated Version of the Microsoft Jet 4.0 Service Pack 8 Replication Files is Available in the Download Center

Because Access replication works in Jet databases, modifying some settings that affect the Jet database engine may improve the efficiency and success rate of synchronization.

Increasing Maximum Locks Available: When inserts and updates are being exchanged, the synchronization needs to obtain a Jet lock on the database that is being modified. If you are exchanging many rows in a single synchronization and experience frequent failures due to locking problems, you might benefit from increasing the number of available locks. The *MaxLocksPerFile* value in the Windows Registry controls the number of locks that can be obtained for any single file and has a default value of 9500. The *MaxLocksPerFile* value is in the registry at the following location:

HKLM\Software\Microsoft\Jet\4.0\Engines\Jet 4.0

Note Novell allows a maximum of 10,000 locks. If you are experiencing locking issues while synchronizing and one of the databases involved is on a Novell server, you may have to move the replica to successfully synchronize.

For more information about automating replication, see the following article: Microsoft Knowledge Base Article – 258539: MOD2000: The Syntax for Synchronization Using Microsoft Jet and Replication Objects

References

For more information about configuring an Internet server for Internet replication, search the Microsoft Replication Manager 4.0 Help Index for "Replication Manager, Internet or intranet servers."

For more information about Microsoft Replication Manager, see the Microsoft Jet Replication white paper, included with Microsoft Office 2000 Developer. You may also obtain this white paper from the Microsoft Software Library on the World Wide Web. For more information on how to obtain the Microsoft Jet Replication white paper, see the following article: Microsoft Knowledge Base Article – 190766: ACC2000: Jet 4.0 Replication White Papers Available in MSDN Online Library.

For more information about configuring IIS, see the following articles:

Microsoft Knowledge Base Article – 172138: How To Create a Virtual Directory in Internet Information Services (IIS)
Microsoft Knowledge Base Article – 323384: How To Set Up an FTP Server in Windows Server 2003

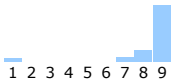
Print E-Mail

How would you rate the quality of this content?

1 2 3 4 5 6 7 8 9
Poor Outstanding

Tell us why you rated the content this way. (optional)

Average rating:
8 out of 9



88 people have rated this page

Manage Your Profile | Legal | Contact Us | MSDN Flash Newsletter

© 2006 Microsoft Corporation. All rights reserved. Terms of Use | Trademarks | Privacy Statement

Microsoft