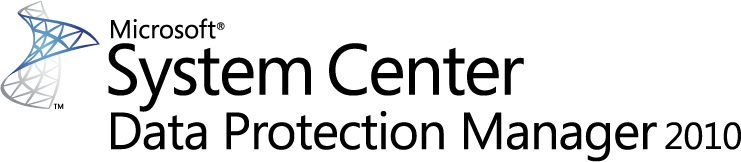


****

Protecting Exchange Server with System Center Data Protection Manager 2010

Published: June 2010

For the latest information, please see [www.microsoft.com/DPM/exchange](http://www.microsoft.com/DPM/exchange)

Executive Summary:

Microsoft System Center Data Protection Manager (DPM) provides continuous data protection for Microsoft Exchange Server 2003, 2007 and 2010. DPM 2010 protects both standalone mailbox databases and those that are members of Database Availability Groups (DAG’s). DPM 2010 offers comprehensive Exchange data protection for organizations of all sizes through disk-to-disk, disk-to-tape and disk-to-disk-to-tape technologies, helping to maintain the business value of an Exchange infrastructure by ensuring that it is better protected and always available.

Contents

[Protecting Critical Business Data 1](#_Toc263432089)

[Business Imperatives 2](#_Toc263432090)

[Improving Protection with Data Protection Manager 5](#_Toc263432091)

[Microsoft and Windows-Specific Design 5](#_Toc263432092)

[Unified Protection for Disk, Tape, and Cloud 7](#_Toc263432093)

[Ease of Use and Management 7](#_Toc263432094)

[Using Microsoft DPM 2010 to Protect Exchange Server 2010 9](#_Toc263432095)

[Typical protection for Exchange 9](#_Toc263432096)

[DPM 2010: Going Beyond Database Availability Groups 10](#_Toc263432097)

[DPM 2010 and other Exchange Roles 11](#_Toc263432098)

[Better protection for Exchange Server with DPM 12](#_Toc263432099)

[How to Protect Exchange Server 2010 with DPM 2010 13](#_Toc263432100)

[Installing the DPM 2010 Server 13](#_Toc263432101)

[Configuring Disk/Tape Media for the DPM Server 15](#_Toc263432102)

[Installing the DPM Agent and preparing Exchange 2010 servers 16](#_Toc263432103)

[Configuring Protection Groups 17](#_Toc263432104)

[How to Recover Mailboxes with DPM 2010 21](#_Toc263432105)

[Recovering an Exchange Mailbox Database 21](#_Toc263432106)

[Recovering a specific Exchange Mailbox 23](#_Toc263432107)

[Best Practices 26](#_Toc263432108)

[Storage Calculator 27](#_Toc263432109)

[Conclusion 28](#_Toc263432110)

# Protecting Critical Business Data

It is difficult to understate how critical a reliable email service is to a business’ internal and external processes. If a user’s mailbox is unavailable, an important series of “conversations” is interrupted. Even the smallest disruption of an organization’s email system can have a profound impact on internal and external relationships. For example, during delicate negotiations with an important client a delay in responding to a critical message might be the difference between winning over the client, or losing that client forever to a competitor.

There are many reasons why an organization needs a comprehensive data protection and recovery solution. Proper data protection provides:

* Point in time recovery from:
  + Data corruption
  + Server failure
  + Site failure
* Inexpensive storage for data that is infrequently used
* Long-term data storage to meet regulatory obligations
* Reduced storage footprint of protected servers

When you are determining the best way to protect both internal and external e-mail conversations, you need to find the right balance between factors such as legal requirements, auditing capabilities, data security, and cost. Determining this balance point involves understanding the underlying business cases for data protection and addressing technical challenges that may restrict you from meeting your organization’s data protection goals.

This paper outlines benefits of using Microsoft System Center Data Protection Manager 2010 (DPM) for your Microsoft Exchange data protection needs. These include:

* DPM 2010 provides specific protection for Windows environments and products, namely SharePoint, Exchange Server, and SQL Server.
* DPM 2010 offers enhanced and improved methods of backing up to tape, disk, or hosted servers.
* DPM 2010 offers a streamlined interface administrators need in order to work through complex tasks.
* DPM 2010 provides advanced mailbox and mailbox database recoverability options beyond those provided by the implementation of Exchange 2007 continuous replication (LCR, CCR and SCR) and Exchange 2010 Database Availability Groups (DAG).

## Business Imperatives

Although understanding the need for data protection is straightforward, it is necessary to first understand the business scenarios that underlie that need. When deciding on a specific data protection solution and strategy. You must first answer questions such as:

* **How much downtime is too much?** 20 years ago, most organizations could continue to function if a portion of their IT infrastructure was unavailable. Today, organizations are far more dependent on their information systems and can be crippled without access to their systems and data. Losses are not limited to the financial impact of being unable to carry out normal business operations - they include the cost of lost productivity, missed business opportunities and damaged organizational reputation. For example, a customer who is unable to place an order because the ordering system is unavailable might look for another supplier. There is a direct relationship between the amount of time it takes for an organization to recover its failed infrastructure and the cost of that loss to the organization. There is also a relationship between the amount of recovery time a solution requires and its cost. Recovery solutions that offer zero downtime generally cost significantly more than solutions that allow for recovery in a short, but predictable, amount of time.
* **How much time is available for backing up data?** Traditional IT operations have a limited, defined window of time during which they can perform backups, yet the amount of data organizations need to protect continues to grow each year. Deciding on a data protection solution requires a thorough understanding of how long your backups take and whether backups can occur at the same time as normal IT operations. Unlike traditional backup products, DPM does not require you to schedule backups during specific backup windows. The protected servers can continue to service their applications while backup is in progress.
* **Is the backup and restore technology reliable?** Organizations perform backups because technology is not always reliable. When selecting a data protection solution, you must assess the reliability of the backup medium along with the cost of the solution relative to that reliability.
* **How will you protect branch and remote offices?** Organizations need to ensure that data hosted at branch office and remote locations is as reliably protected as data hosted at the head office.

**Technical Challenges**

Determining the best data protection solution for your organization is not just a matter of working within organizational constraints. There are also technical constraints that influence how well the solution meets organization’s needs. Traditional data protection solutions are heavily dependent on tape-based technologies. These technologies, however, are becoming less and less effective for short term protection of today’s environments for the following reasons:

* **Tape write speeds are unable to keep pace with the growth of data that requires regular backup.** Organizations have more and more data to back up, and the speed at which the backup happens must keep pace with business realities. Data can be backed up to disk significantly faster than it can be backed up to tape.
* **Tape-based data recovery can require a bigger restore window.** Organizations cannot afford to have critical infrastructure offline any longer than is necessary. Disk-based backup and restore solutions maximize the amount of data that can be restored in a limited amount of time. The faster you can restore data, the faster you can return your infrastructure to full operational status.
* **Tape-based restores may not be as reliable as other technologies.** Microsoft’s experience shows a 17% annual failure rate for its backup tapes and tape devices. Additionally, an administrator performing a tape-based restore often needs access to multiple tapes. If just one of these tapes is unreadable, the whole restore operation may come to a halt. Each tape in a backup set must be readable, and the software catalogs used to manage those tapes must also be free of corruption. Using traditional hard disks as a backup medium provides a greater degree of success when it comes to performing restore operations.
* **Tapes can be difficult to manage at remote sites.** Ensuring that tapes are rotated and that the correct tapes are made available for backup and restore is challenging when organizations may not have appropriately trained IT staff at each remote site.

Over time, applications have become more diverse in the way that they store data. For example, some applications create and process “flat” files such as Microsoft Office documents, that are opened, changed, and then closed. Protecting the data these applications generate is as simple as making a static copy of the closed “flat” file. On the other hand, other critical business applications, such as Exchange Server, SQL Server, and SharePoint products and technologies use files that remain in an exclusively open and locked state when the application or service is active.

Many real-time replication or continuous data protection products provide file or volume-level replication which replicates all changes to the underlying volume. This can lead to problems when attempting to restore data to its original state because there is a significant relationship between the application’s state in memory and what is stored on media and this relationship must be tightly managed to ensure that backups are both consistent and that they allow for recovery to a functional state.

Microsoft and many other software vendors provide supported interfaces in their applications for capturing data in a consistent state when the file hosting the data is in an exclusively open and locked state. One such interface is Volume Shadow Copy Service (VSS). VSS only provides a method through which it is possible to create a point-in-time copy. The protection software is then responsible for requesting a copy of the file and managing the copy once it exists. The technical challenge is ensuring that a chosen backup solution is able to restore data in a consistent state.

# Improving Protection with Data Protection Manager

DPM is a Microsoft product specifically developed to provide a cost-effective and reliable data protection solution to servers running Microsoft workloads. DPM addresses two specific data protection challenges: The need for more effective backup and restore functionality with disk rather than tape, and the need to better centralize remote and branch office backup.

DPM 2006 was the first version of DPM. It focused specifically on the protection of file servers and servers running file-based applications and wasn’t intended to protect Exchange workloads.

DPM 2007 was built with a high degree of awareness for specific Microsoft applications, such as Exchange Server, SQL Server, and Microsoft Office SharePoint Server read, write and store data on volumes. Hence, DPM 2007 provides tailored, application-aware protection and recovery for these key workloads.

DPM 2010 provides even more depth and flexibility in Microsoft application protection and recovery, as well as new capabilities in protecting virtualization platforms and the ability to protect Windows client data.. These features allow systems administrators and IT generalists to develop their own recovery infrastructure, perform their own Exchange Server backups, and perform mailbox database and mailbox recovery operations without relying on backup or storage specialists.

## Microsoft and Windows-Specific Design

As one of the largest IT companies in the world, Microsoft has significant internal data protection requirements. Given that the company uses its own products for its IT infrastructure, it also has one of the biggest deployments of Microsoft products in the world. Several years ago, Microsoft performed an internal investigation to analyze how the third-party data protection tools met the organization’s backup and recovery needs. The investigation found that there were gaps between the protection that Microsoft needed and the protection those products could provide.

In parallel with that, Microsoft customers and partners provided feedback on what they needed in data protection and recovery, but weren’t getting in their legacy solutions. The needs across organizations were the same, showing not only the capabilities that were missing but also the requirement that the solution fit equally well for not only large enterprise but all midsized organziations. With this disparity in mind, Microsoft began development of System Center Data Protection Manager.

DPM 2010 is part of the System Center family of IT management technologies from Microsoft. This integration means that organizations can realize synergies by combining DPM 2010 with other System Center components. For example:

* System Center Operations Manager (OpsMgr) 2007 can be configured to monitor the DPM 2010 servers, as well as all components in an Exchange Server deployment environment. This allows administrators to view, at a glance, the health and status of all protected servers, in addition to the DPM 2010 server that is providing the protection.
* System Center Configuration Manager (ConfigMgr) 2007 R2 can be used to automatically deploy DPM agents to production servers. ConfigMgr can also manage and deploy updates to DPM servers, and protected Exchange Server servers.
* System Center Data Protection Manager 2010 provides a consistent and reliable backup of Exchange Server. Because the Data Protection Manager team has consulted closely with the Exchange team, DPM 2010 provides a reliable backup and recovery solution.

Using a Microsoft solution to protect a Microsoft product can reduce confusion and frustration when trying to integrate Windows environments and third-party data protection products. When an administrator needs useful assistance with restoring critical organizational data, she wants to make contact with a single organization to get the help she needs as quickly as possible. Administrators do not want to have to go back and forth between two different organizations to determine which one will be able to assist in returning the data assets to full availability.

Some third-party backup solutions leverage unsupported and undocumented APIs, and reverse-engineered processes to back up Microsoft Exchange. Because these operations are unsupported, using them can lead to unexpected outcomes in the restoration and recovery of data and complications when resolving situations with Microsoft product support. However, when an administrator uses DPM to protect Exchange, she only needs to contact Microsoft in the event that support is required.

For more information on Microsoft’s policy towards third-party products that modify or extract Exchange database contents, consult the following article on Microsoft’s website: <http://support.microsoft.com/kb/904845>

## Unified Protection for Disk, Tape, and Cloud

DPM 2010 allows organizations to find a comfortable balance between disk-based, tape-based, and cloud-based backup systems. Administrators can use disk-based and tape-based backup to perform rapid recovery of recent data from disk media on a regular basis, and to retrieve and restore much older protected data from archival tape media when required.

**Disk-Based Backup.** With DPM 2010, disk-based backup is used as the storage location for short-term data protection operations. Disk-based protection allows for rapid backup and restore of protected data. This speed is critical in that the vast majority of restore operations occur within a relatively short period after a data backup.

**Tape-Based Backup**. Although protected data is not initially written to tape, tape-based backup does have a place in a DPM data protection ecosystem. DPM allows backed-up data to be copied to tape for the purposes of meeting long-term data retention and archiving requirements.

**Cloud-Based Backup**. DPM can be configured to back up data across the Internet to a disaster recovery facility at a separate data center. Microsoft has partnered with Iron Mountain to provide a service called CloudRecovery™ that sends the data from an on-site DPM server to an Iron Mountain data center ([www.microsoft.com/DPM/cloud](http://www.microsoft.com/DPM/cloud)).

## Ease of Use and Management

The DPM interface is engineered to help administrators perform complex tasks with a few simple steps. In a high-stress data recovery scenario the design of the DPM interface ensures that it is not necessary for administrators to waste time searching through a labyrinth of menus to find a way to launch a specific task or configure a specific option.

  
**Figure 1. DPM Administrator Console**

The DPM 2010 interface simplifies the process of configuring protection and recovery. The interface provides structured workflows and wizards to guide administrators through the following series of logical steps:

* Browsing the available host servers and Exchange mailbox database content
* Specifying recovery goals and retention objectives
* Protecting data

After you identify the data to be protected and establish the appropriate schedules, DPM handles locating the files or data objects to protect, managing the disk-based images and logs, and developing a tape rotation policy. DPM manages the intricacies and complexities involved with recovering data to a live system by reducing complex recovery operations to the following simple steps:

* Browse or search protected data and select a data source
* Select desired point in time from calendar control or list
* Select options as appropriate for situation at hand
* Execute recovery

# Using Microsoft DPM 2010 to Protect Exchange Server

Non-Microsoft backup solutions tend to take a generic backup functionality and adapt it to support-specific applications. In contrast, Microsoft created DPM 2010 to leverage fully supported Microsoft technologies in order to provide continuous data protection including Windows Server hosts running Exchange Server 2003, 2007 or 2010. This support includes:

* Backing up active and passive databases in a Database Availability Group (DAG), in Exchange 2010, as well as continuous replication (LCR, CCR and SCR) in Exchange 2007)
* Facilitating recovery of data from individual mailboxes.
* Facilitating recovery of Hub Transport, Client Access Server and Unified Messaging Exchange Server 2010 roles.
* Supporting Exchange High Availability and Exchange Disaster Recovery configurations.

## Typical protection for Exchange

Backing up and restoring Exchange Server mailbox databases in a consistent fashion is significantly more challenging than backing up closed, static files. Although Microsoft recommends that the Exchange VSS writer be a part of any backup solution used to protect Exchange Server mailbox and public folder databases, not all data protection products leverage this technology. If data is not captured in a consistent and supported manner, it may be difficult, if not impossible, to ensure a complete and consistent recovery of mailbox database content.

To ensure that a complete and consistent backup of Exchange occurs, some products require that Exchange databases be put in a state in which they are temporarily not available to clients while backup operations occur. This means that Exchange administrators must structure their backup routine to accommodate times when the mailbox server could be offline, even if those times are brief.

## DPM 2010: Going Beyond Database Availability Groups

A common question administrators ask is why they should use a DPM 2010 protection solution for mailbox database servers when Exchange Server 2010 offers Database Availability Group (DAG) functionality. DAG functionality allows the contents of an active mailbox database on one server to automatically replicate to passive mailbox databases on up to 15 other servers, including (under specific conditions) servers in other sites. DAG replication can be configured so that the contents of a passive mailbox database copy can be mirrored in two ways:

* **Directly** – The primary mailbox database is configured with no log replay delay.
* **Lagged** - The log replay delay is configured to a period of no more than 14 days.

Lagged copies are one way that administrators can safeguard against store/logical corruption events and accidental mailbox deletion. Without log delay replay changes caused by these events may automatically be replicated to mailbox database copies. There are several good reasons why administrators should choose to implement DPM 2010 in conjunction with DAGs, rather than relying upon an exclusive DAG solution for the protection and recovery of mailbox data. Some of these reasons are:

* **Less complicated point-in-time restoration** – Point-in-time (PIT) restoration from a lagged database copy requires an administrator to perform a complex operation that involves locating and replaying specific log files as part of the recovery process. DPM allows administrators to perform PIT recovery with several quick selections from an intuitive GUI interface. The interface minimizes the complexity and time required for a PIT restoration, ensuring that the appropriate data is reliably restored.
* **Fewer Exchange servers are needed** - Leveraging DAGs to provide a comprehensive data protection solution requires that you deploy a large number of Exchange Servers. For example, to provide a mailbox database copy that allows for automatic failover and another that allows for a point-in-time (PIT) restore, you will need to deploy a minimum of three Exchange mailbox servers: One to host the active mailbox database, one to host the up-to-date copy, and one to host the lagged copy.

If you are attempting to also provide offsite backup and recovery, even more Exchange mailbox servers are required. A robust data protection solution that relies solely on DAGs will require a significant investment in Exchange Server 2010 licenses. With a DPM solution in place, offsite backup and PIT restores can be handled through DPM with DAGs implemented primarily as a high availability solution. A DPM solution minimizes the complexity of the Exchange infrastructure, and licensing a DPM server is more cost- effective than licensing the necessary extra instances of Exchange.

* **Longer retention range** - DAG lagged copies offer administrators limited PIT recovery options. By design, PIT recovery from a lagged recovery is limited to a maximum of 14 days. PIT recovery of data protected by DPM 2010 enhances the data protection available to administrators by providing PIT restore from outside the DAG14-day limitation.
* **More consistent backup and recovery process** - DPM 2010 allows an organization to use a consistent backup and recovery process across multiple workloads such as File servers, SQL, Hyper-V, and SharePoint.

## DPM 2010 and other Exchange Roles

When protecting Exchange Server 2010, administrators must consider how other Exchange Server roles such as the Hub Transport and Client Access Server should be recovered in the event of failure. The configuration data for these roles is stored within Active Directory – this can mean that in the event of complete server failure a typical recovery of a server hosting these roles will involve rebuilding the server with the same name, joining it to the domain and then using SETUP.EXE /m:RecoverServer. It may be necessary to then reconfigure any custom settings that were present on the server.

If DPM 2010 is used for the protection of servers hosting the Hub Transport and Client Access server roles it is possible to perform a complete bare-metal recovery of the servers hosting these roles. This recovery can be performed either to physical hardware or a virtualized infrastructure. It will also take significantly less time than reinstalling and configuring the host operating system on a replacement server in preparation for running the SETUP.EXE /m:RecoverServer Installation recovery routine.

## Better protection for Exchange Server with DPM

DPM 2010 is engineered to provide the best possible protection for Exchange Server. In fact, the team that built DPM 2010 worked in consultation with the team that built Exchange Server to ensure that Exchange workloads are reliably protected.

DPM 2010 seamlessly interacts in the following ways with the Exchange Server VSS writer to capture consistent versions of an Exchange deployment without interrupting client access to mailboxes and public folders:

* A baseline copy of the Exchange Server data can be made using either the DPM block-level synchronization engine or can be done manually.
* Express full backups are captured. These backups use the Exchange Server VSS writer and DPM agent to identify only those blocks that have changed in the mailbox database(s) and then forward those changed blocks to the DPM server.
* Exchange mailbox database transaction logs are continuously synchronized with the DPM server as frequently as once every 15 minutes (between express full backups). DPM synchronizes the log files using a VSS incremental operation to again ensure only supported protection and restore operations.
* Best practice is to configure nightly express full backups and transaction log synchronization every 60 minutes.

# How to Protect Exchange Server with DPM 2010

In this section you will learn how to perform specific Exchange protection tasks using DPM 2010. These tasks are:

* Install DPM 2010 server
* Configuring disk/tape media for the DPM server
* Installing the DPM agent and preparing Exchange
* Configuring protection groups

### Installing the DPM 2010 Server

Microsoft requiresthat you run DPM 2010 on a server running an x64 version of Windows Server 2008 or Windows Server 2008 R2 with 4 GB of RAM, 1 GB free on the system volume, 1.3 GB available on the volume that hosts the DPM files and 900 MB on the volume hosting the database. In a simple deployment, you should devote one disk to hosting the operating system, DPM software and SQL server database and use other disks for hosting protected data. Prior to installing DPM 2010 you should ensure that your computer is running Windows Server 2008 with the following components installed:

* .NET 3.5 Service Pack 1
* Windows Installer 4.5
* Windows Single Instance Store (SIS)
* PowerShell 2.0

These components are already available on servers that use the Windows Server 2008 or 2008 R2 operating system. DPM 2010 should not be installed on a server under the following circumstances:

* The server functions as a Management Server for OpsMgr 2007.
* The server is part of a Windows Server 2008 or 2008 R2 failover cluster.
* The server hosts significant server workloads relative to server and storage capacity.

DPM 2010 also requires access to a private instance of SQL Server 2008 or SQL Server 2008 R2. This instance can be installed locally on the computer that will host DPM 2010 as a part of the DPM installation process, or can be configured separately on a remote server. It is strongly recommended to use the local instance that is installed by default. Both DPM 2010 and SQL Server 2008/2008 R2 can be hosted on an x64 virtual machine running Windows Server 2008 or Windows Server 2008 R2.

To install DPM 2010, perform the following steps:

1. On the Microsoft System Center Data Protection Manager 2010 screen, click the **Install Data Protection Manager** item.
2. Review and then accept the license agreement, then click **OK**. On the Welcome page, click **Next**. The DPM 2010 installer will now perform a prerequisite check. Once the check completes successfully, click **Next**.
3. On the Product Registration page enter registration details.
4. On the Installation Settings page select the folder that will host the DPM program files. Specify whether you want to have an SQL Server instance installed locally or if you are going to use an instance of SQL Server that you created earlier.
5. On the Security Settings page configure passwords for the MICROSOFT$DPM$Acct and DPMR$<computer name> local user accounts and then click **Next**.   
   ***Note -*** If you are using a remote SQL server, which is not recommended, specify the appropriate domain account credentials.
6. On the Microsoft Update Opt-In page, specify if you want to sign up for Microsoft Update and then click **Next**. On the Summary of Settings page review the installation choices that you have made and then click **Install.** After installation completes, restart the DPM 2010 host computer.

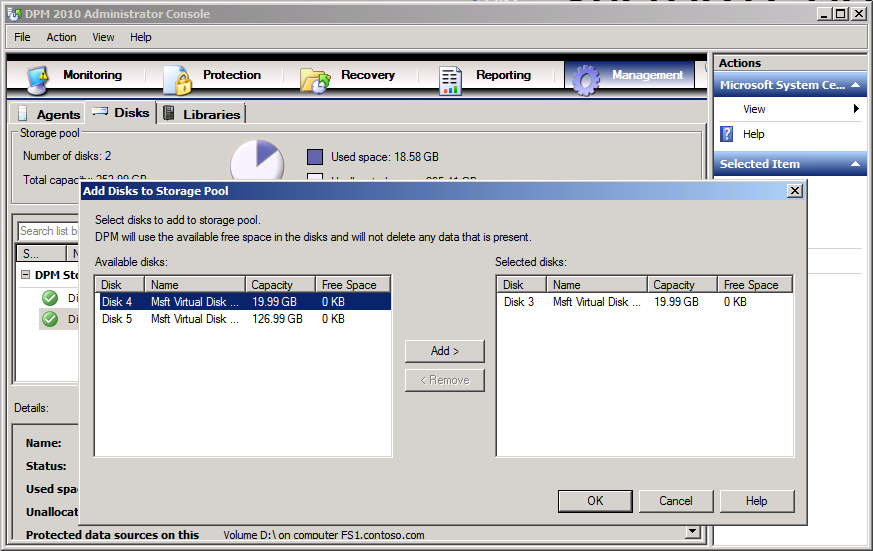
To get the most up-to-date information about installing DPM 2010, consult the DPM TechCenter on Microsoft TechNet: <http://technet.microsoft.com/DPM>

### Configuring Disk/Tape Media for the DPM Server

Windows Server must recognize a storage device as locally attached before DPM can use it for storage. DPM can use direct-attached storage (DAS) or SAN devices attached through iSCSI or Fibre Channel to store protected data. DPM cannot store protected data on removable disk media like USB or IEEE 1394 hard disk drives because these devices are not always attached and do not support VSS unless these devices are part of a VTL solution that appears as a tape device to DPM. Any volumes that are used must be dedicated to DPM. Microsoft recommends the use of RAID5 for DPM as this provides the necessary data integrity and storage reliability. When performing this task, design the RAID5 configuration, take the IOPS requirement into consideration and then balance the number of overall LUNs used to meet the IOPS. You must also pay attention to the number of LUNs allocated for the RAID parity bits as this affects the IOPS as well.

To add disks to the storage pool, perform the following tasks:

1. Open the DPM Administrator Console, click **Management** on the navigation bar and then click the **Disks** tab.
2. To add disks to the DPM storage pool, click **Add** in the Actions pane. This will open the Add Disks To Storage Pool dialog box, shown in the figure below. This dialog box will list all locally attached disks that are available for use by DPM. This list will include all appropriately configured iSCSI and Fibre Channel disks.
3. Select the disks that you wish to add to the storage pool and click **Add**. You can also use this dialog box to remove disks from the DPM 2010 storage pool.



**Figure 2. Configuring disk media for a DPM server**

### Installing the DPM Agent and preparing Exchange servers

After you have deployed DPM, it will query the Active Directory service to locate computers that can be protected. You can access this list through the Protection Agent Installation Wizard. You can then install the agent directly using the DPM 2010 console. Alternatively, you can deploy the agent by using System Center Configuration Manager (enterprises) or System Center Essentials (midsized organizations), by deploying the installer using software installation policy options of group policy, or by manually executing the agent installation package on the desired system.

To install the DPM protection agent on an Exchange server using the DPM 2010 console, perform the following steps:

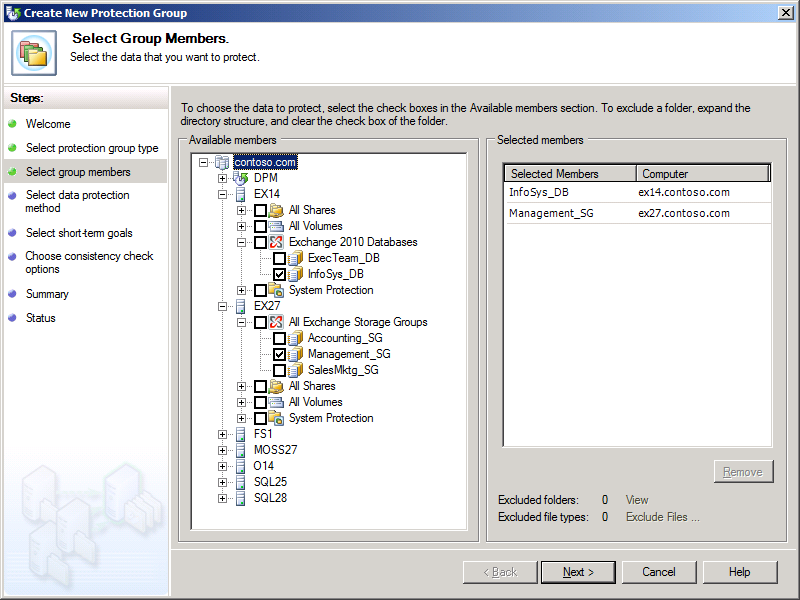
1. In the DPM 2010 console, click **Management** and then click the **Agents** tab. In the Actions pane select **Refresh**, wait for it to complete and then click **Install.** This launches the Protection Agent Installation Wizard.
2. Select the Microsoft Exchange servers on which you want to install the protection agent from the list of discovered computers, and then click **Add**. When all Exchange servers that you want to protect are added to the list, click **Next.**
3. Enter the details of the administrator account to use for the installation of the agent. The domain account must be a member of the local Administrators group on each target Microsoft Exchange server.
4. Specify how you want the target servers to restart in order to complete the installation of the DPM agent.   
   ***Note*** - Agent installation does not typically require a restart to complete.
5. Review the summary and click **Install Agents**. Once agent installation is complete, click **Close** to close the Protection Agent Installation Wizard.

### Configuring Protection Groups

Protection Groups in DPM allow you to group together similar resources so that they can be protected in a similar way. Exchange servers in the same protection group use the same short- and long-term protection policies.

When you configure a protection group, the wizard recommends allocations for the replica and recovery point volumes based on an estimate of the size of the data in the specified protection group. To configure protection groups, perform the following steps:

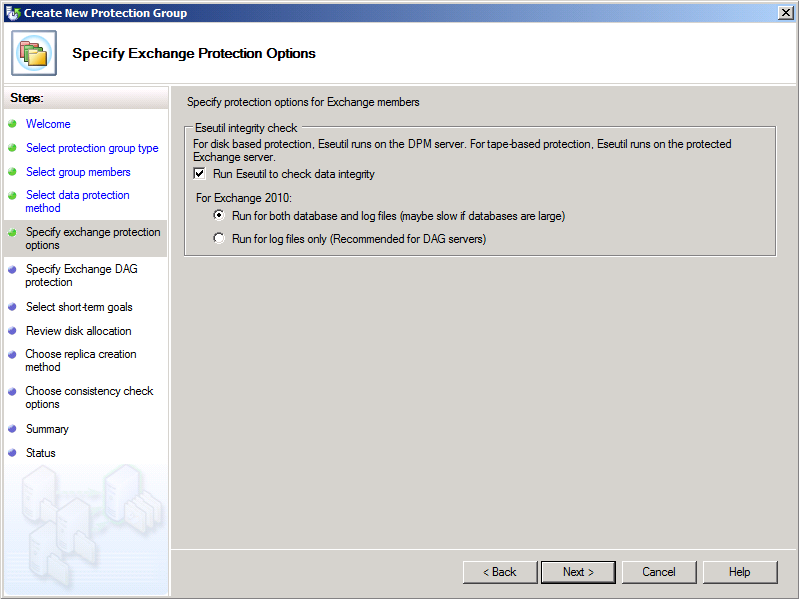
1. In the DPM Administrator Console, click **Protection** on the navigation bar.
2. In the Actions pane, click **Create Protection Group**. The Create New Protection Group wizard will start. On the Welcome page, click **Next**.
3. On the Select Protection Group Type page, click **Servers** and then click **Next.**
4. Expand the Exchange server list and select the 2010 mailbox databases or 2007/2003 storage groups that you want to add to the protection group as shown in Figure 2.



**Figure 3 – Selecting configuration protection groups.**

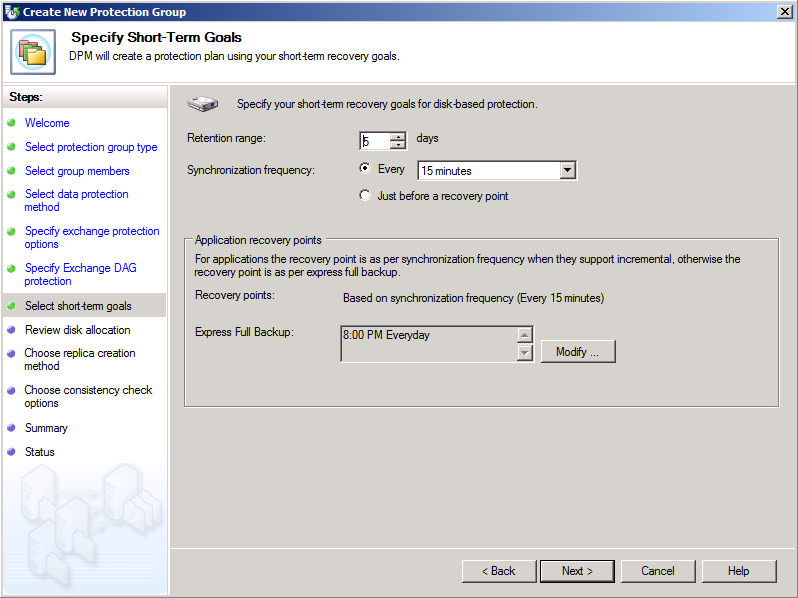
1. Specify a unique name for the protection group or accept the default name.
2. Define protection policies:
   * For short-term protection for this protection group, select the **I Want Short-Term Protection Using** checkbox and then select the media where protected data will be stored.
   * For a long-term protection policy for the protection group, select the **I Want Long-Term Protection Using Tape** checkbox.
3. To perform a mailbox database integrity check on the DPM server, choose **Run Eseutil to check data integrity**.

***Note*** - Microsoft recommends that you run an integrity check using eseutil for both the database and log files if the protected server is not part of a DAG. (You can check only the log files if the protected server or servers are members of the same DAG.) If you choose to perform the check you must ensure that the version of eseutil on the DPM server is the highest version amongst protected Exchange servers.



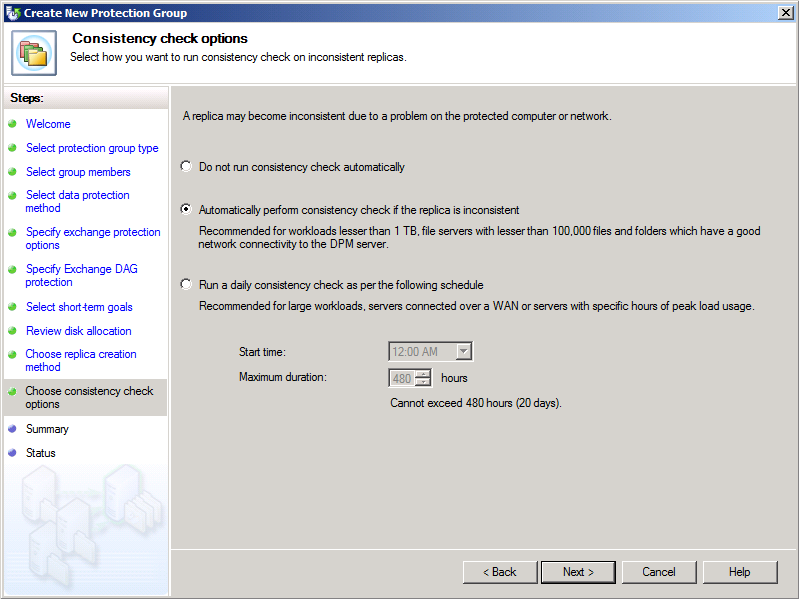
**Figure 4 – Configure mailbox database integrity check.**

1. On the Specify Exchange DAG protection page, select which database copies will be selected for full backup and which database copies will be selected for copy backup. When protecting mailbox servers that are members of DAGs, it is only possible to perform a full backup on one copy of the database due to federated log truncation. DPM must back up other copies of the database up using a copy backup.
2. If you choose short-term protection, choose retention duration for data recovery in the **Retention range** box. To specify the synchronization frequency modify the recovery point schedule for a data source, click **Modify**. Select the desired day and time and then click **OK**.



**Figure 5 – Configure synchronization frequency.**

1. DPM will display recommended disk allocations for the replica volume and the recovery point volume. You can either accept the recommended allocations or adjust the allocations by clicking **Modify**.   
   ***Note -*** You cannot modify allocations to lower than 1.01GB for the replica and 1.56GB for the recovery point volume.
2. On the Choose a Replica Creation Method page, specify whether you want the replica created automatically now, at a specific later point in time, or whether you want to create a replica manually.
3. Choose whether DPM will perform a consistency check on the replica. You can select between not running a consistency check, running one automatically, or running one on a scheduled daily basis. Automatic checks are recommended for workloads smaller than 1 TB where there is good connectivity between the protected data and the DPM server.



**Figure 6 - Setting up consistency check on inconsistent replicas.**

1. Review the summary and then click **Create Group**. Close the confirmation page.

# How to Recover Mailboxes with DPM 2010

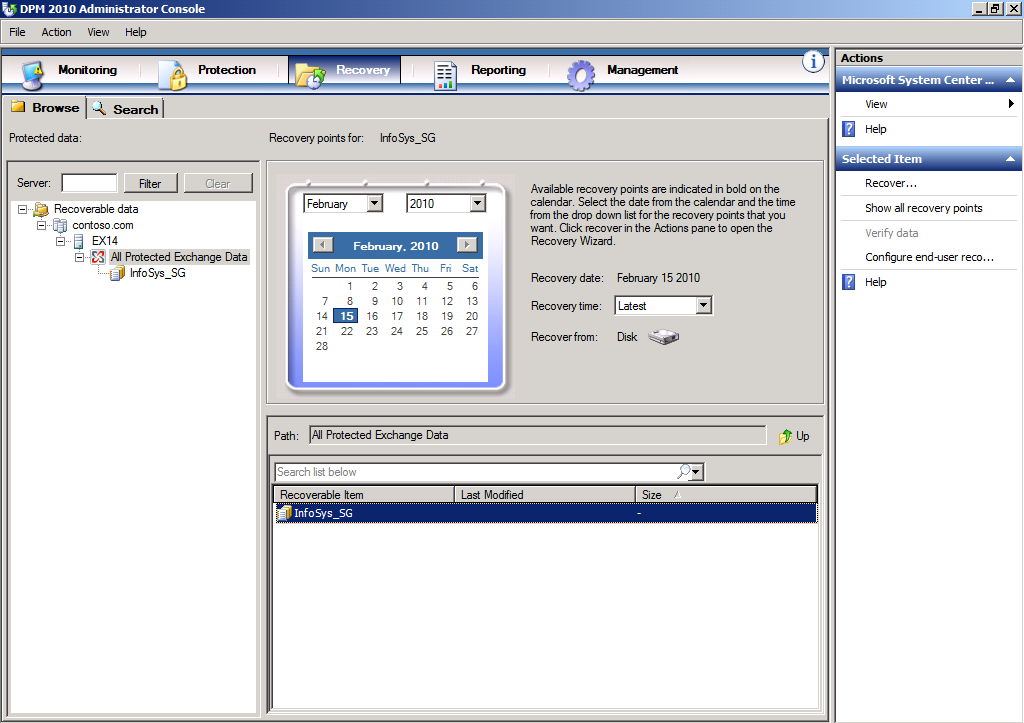
DPM 2010 supports the following mailbox database and mailbox recovery scenarios:

* Recovering all protected Exchange Data
* Recovering a mailbox database
* Recovering a specific mailbox

## Recovering an Exchange Mailbox Database

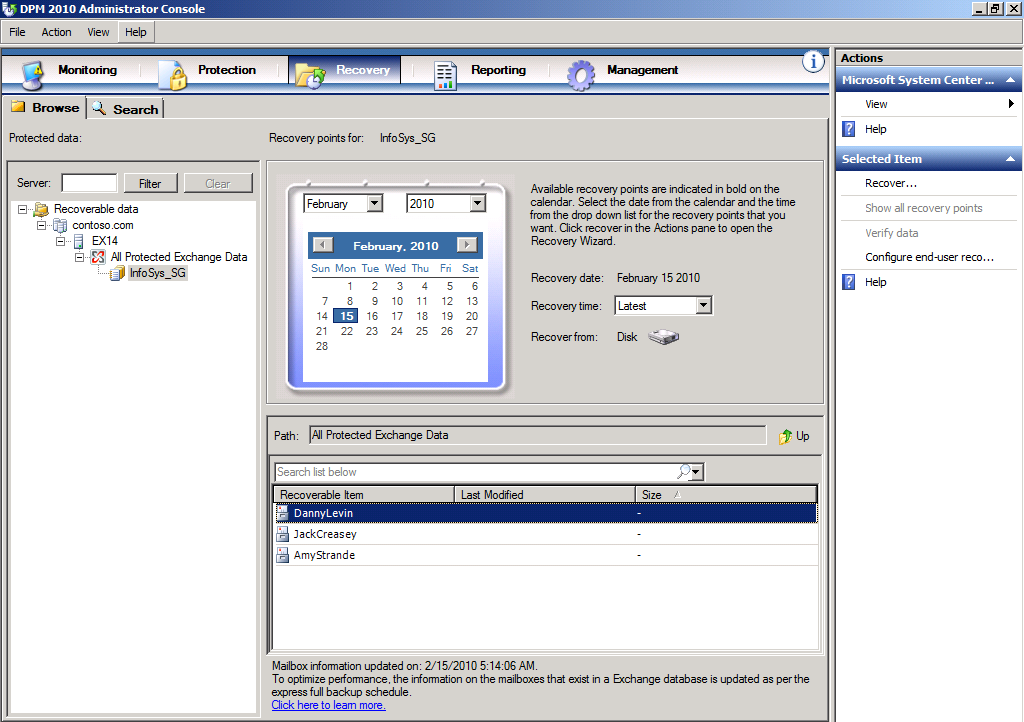
You can use DPM 2010 to recover an Exchange Mailbox database to the mailbox server that originally hosted it or to another Exchange Server mailbox server that has the DPM agent installed. To recover an Exchange mailbox database to its original location, perform the following steps:

1. Open the DPM Administrator Console and then click **Recovery** on the navigation bar. In the Protected Data area, browse to the Exchange server that hosts the mailbox database that you want to recover.
2. Click any bold data in the calendar to see available recovery points. Select the recovery point, click the **All Protected** **Exchange Data** node and select the mailbox database name. To recover specific databases or items, you can drill down from this point. Click **Recover** in the Actions pane to launch the Recovery Wizard.
3. Review the recovery selection and then click **Next**. Select **Recover To Original Exchange Server Location** and then click **Next**.
4. On the Specify Recovery Options page, specify whether you want to have the mailbox database mounted after recovery, whether or not you want to utilize bandwidth throttling, and the option of SAN based recovery using hardware snapshots if the preparatory steps have been performed. If you want DPM to send an e-mail message once the recovery process completes, select **Send A Notification When This Recovery Completes** checkbox and enter one or more e-mail addresses. Use a semi-colon to separate multiple e-mail addresses. Click **Next.**
5. Review your settings and then click **Recover**. When the recovery completes, click **Close**.

 **Figure 7 - Choosing a date and time to recover back to.**

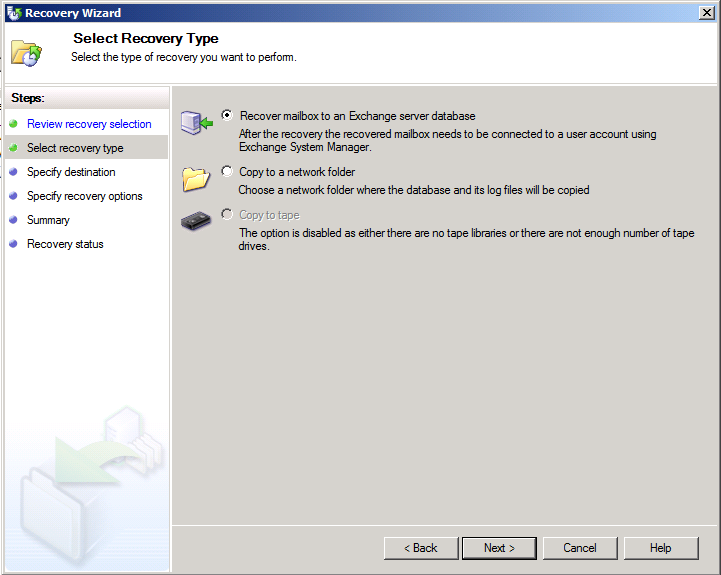
## Recovering a specific Exchange Mailbox

To use DPM 2010 to recover an individual mailbox either to another Exchange Server server or to a network folder, perform the following steps:

1. From the DPM Administrator console, click **Recovery** and then navigate to the Exchange mailbox database that hosts the mailbox that you want to recover in the Protected Data pane.
2. Select the mailbox that you want to recover as shown below and then click **Recover** in the actions pane. This will launch the Recovery Wizard. 

**Figure 8 - Finding mailboxes for RSG/RDB restoration.**

1. On the Review Recovery Selection page, click **Next**. On the Select Recovery Type page, choose the recovery location.   
   ***Note*** - You have the option of recovering to the original instance, to any other Exchange Mailbox server with a DPM agent installed, to a network folder available from the DPM server, or to tape if the appropriate hardware is available. When recovering to an Exchange Mailbox server, you recover to a recovery database rather than directly to the database that hosted the original mailbox. The recovery database must exist prior to attempting this recovery.

 **Figure 9 - Setting up recovery type.**

Click **Next**. On the specify recovery options, choose whether you want to use network bandwidth usage throttling and SAN based recovery using hardware snapshots if available and applicable.

1. If you want DPM to send an e-mail message once the recovery process completes, select **Send A Notification When This Recovery Completes** checkbox and enter one or more e-mail addresses. Use a semi-colon to separate multiple e-mail addresses. Click **Next**.
2. Review your settings and then click **Recover**. When the recovery completes, click **Close**.

# Best Practices

The list shown here provides advice on additional aspects of DPM 2010 deployment.

* When protecting mailbox databases that are members of a DAG, it is not necessary to select the active mailbox databases in a DAG for protection by DPM. DPM is database role agnostic and can be configured to protect a server that hosts a collection of active or passive mailbox databases.
* With DPM 2010 you need to configure at least one Full Backup per day. The Full Backup backs up the mailbox database and log files and then truncates the log files. When protecting more than one copy of an Exchange mailbox database (such as when you are protecting multiple members of a database availability group) you should configure one node for full backups and the rest as copy backups. Copy backups do not truncate log files.
* Microsoft recommends that you protect at least two copies of a mailbox database if Exchange is implemented with inexpensive SATA/JBOD (Just a Bunch Of Disks) disks. As mentioned previously, one and only one backup should be a full backup and additional backups of different copies of the same mailbox database should be copy backups.
* The DPM 2010 default setting has Exchange 2010 running ESEUTIL on Exchange mailbox databases as a background task to verify their integrity. DPM 2010 allows you to skip running ESEUTIL on the mailbox database and only use the utility to verify the integrity of the log files
* If the Exchange DAG node hosting the copy of the mailbox database on which the Full Backup is taken goes down temporarily, it is not necessary to perform any steps on the nodes on which copy backups are taken. If it becomes necessary to switch to another node because the failed node will no longer be available, you need to reconfigure DPM to take a full backup of the new target node. As mentioned earlier, DPM 2010 is not sensitive to as to whether the full backup is taken of an active or passive mailbox database copy - the node on which the backup is taken just needs to be available to DPM.

## Storage Calculator

Storage calculator allows you to estimate how much storage you must allocate in DPM 2010 to protect specific resources. DPM 2010 Exchange storage calculator is provided to help you plan the protection of your Exchange 2010 deployment. The storage calculator also provides guidance on three aspects of a DPM 2010 protection strategy:

* Estimates how much storage is required to protect a specific Exchange Server 2010 deployment.
* Outlines the type and class of server, memory requirement, storage requirement and guidance for critical system parameters such as the page file size that are required to create a DPM server.
* Estimates backup window SLAs by providing the time needed for both Initial Replication and Incremental Synchronization.

Additional tools are available to help you estimate some of the input parameters for your specific implementation such as the amount of change in data from day to day, called “data churn.” Data churn plays a crucial role in estimating the requirement to protect your Exchange installation. Another factor that influences the amount of storage you will need for the recovery volume is the Retention Range, or the number of days you expect to keep a recovery point. The Backup Frequency determines how many recovery points you will have.

The storage calculator can be used in the initial phase of your Exchange 2010 protection strategy to not only estimate the amount of storage you will require but to model your backup policies. You can conduct a what-if analysis to see the impact on backup SLAs by changing the storage IOPS and also by varying the network bandwidth available for backup and recovery. You can vary the storage consumption parameters - churn and the Retention Range - to see the effect on the storage requirement over time.

Using the storage calculator to estimate your deployment requirements can result in a deployment configuration that is robust and can function optimally over a period of time. You can access more detailed documentation related to the DPM 2010 Storage Calculator, as well as the Storage Calculator spreadsheet for Exchange, at the following address: <http://www.microsoft.com/downloads/details.aspx?FamilyID=c136c66c-bd4a-4fb1-8088-f610cd02dc51&displaylang=en>

# Conclusion

Data Protection Manager 2010 provides fully integrated data protection for Microsoft Exchange 2003, 2007 and 2010. DPM was designed in consultation with the Exchange team at Microsoft; therefore, you can have confidence that:

* DPM can be used to reliably and quickly back up Microsoft Exchange data from production servers at frequent intervals throughout the day without a negative impact on performance.
* DPM replicas and recovery points allow organizations to reliably restore Exchange data not only in its most recently backed up state, but in any state that was captured in recovery points.
* Flexible recovery options allow Exchange mailbox data to be restored not just to the original Exchange server, but to other protected servers and arbitrary file locations.

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This white paper is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS   
DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in, or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

© 2010 Microsoft Corporation. All rights reserved.

The example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious. No association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred.

Microsoft, Active Directory, Microsoft Exchange, SharePoint, SQL Server, Windows, Windows Server are trademarks of the Microsoft group of companies.

All other trademarks are property of their respective owners.