

# *Exchange Server 2010: Migration and Testing*

The buzz surrounding Microsoft Exchange Server 2010 isn't just noise; however, new features fall short without proper setup. Get the lowdown on how to install, test and protect your Exchange upgrade.

BY SERDAR YEGULALP

- ▶ EXCHANGE SERVER 2010 OUT OF THE BOX
- ▶ MIGRATION REQUIREMENTS AND DEPLOYMENT METHODS
- ▶ TESTING EXCHANGE SERVER 2010
- ▶ HOW TO PROTECT EXCHANGE 2010 AND ITS USERS

## Exchange Server 2010 Out of the Box

*From high-availability features to new management functions, Exchange Server 2010 sports enough changes to be considered a milestone release.*

EXCHANGE SERVER  
2010 OUT OF THE BOX

MIGRATION  
REQUIREMENTS AND  
DEPLOYMENT METHODS

TESTING EXCHANGE  
SERVER 2010

HOW TO PROTECT  
EXCHANGE 2010  
AND ITS USERS

ONE OF THE biggest areas where Exchange Server 2010 differs from its predecessors is in its high-availability functionality. When you build an Exchange Server 2010 site, you have more ways to ensure that the site goes up, stays up and can withstand problems that would have previously brought your Exchange environment to a screeching halt.

The most crucial new high-availability feature is the database availability group (DAG), a way to give Exchange servers the reliability of clusters without the headaches associated with traditional clustering. DAGs gang together groups of Exchange mailbox servers to allow their databases to be replicated automatically among the servers in the group and to allow automatic failover across the servers in the DAG. Microsoft bills DAG technology as “the base component of the high-availability and site resilience framework built into Microsoft Exchange Server 2010.”

DAGs simplify many procedures when it comes to Exchange reliability. With DAGs, you can allow for failover without first having to build clustered servers and install Exchange on them. In Exchange 2010, you can add servers to a DAG at any time and allow them to replicate between each other. And because replication is more granular in Exchange Server 2010, you don’t have to replicate every mailbox.

Additionally, with DAGs, databases are not tied to a single server; they can be replicated up to 16 times across different mailbox servers. Microsoft claims a DAG with three servers better protects Exchange and recovers from disaster faster than a single, conventionally backed up server.

## MAILBOX, TRANSPORT AND RECIPIENT FUNCTIONALITY

Exchange Server has always been, and probably always will be, primarily about mail. To that end, Microsoft added a whole slew of new mail-handling features to Exchange Server 2010. They include:

- ➔ **Moderated transport.** An administrator can require approval to send messages to certain recipients.
- ➔ **Shadow redundancy.** Messages are automatically resubmitted if they're sent to an Exchange Server 2010 hub transport server and don't return a successful delivery report.
- ➔ **End-to-end message tracking.** Admins can log and analyze the entire path of a message for troubleshooting.
- ➔ **Memory handling.** Better handling of memory used to process distribution groups, so large distribution groups don't choke the server when they are expanded.
- ➔ **New transport rules and rule handling.** They let you create rules bound by Active Directory Rights Management Services.
- ➔ **Moving mailboxes.** [Move Requests](#) make it possible to move mailboxes between databases while they're still in use. Message tracking data isn't available during the move.
- ➔ **Calendar sharing.** Users can share calendars—including free/busy data—with users residing outside the organization via Outlook 2010 and the [Federated Sharing](#) feature. Note that only admins can control this, not users.

## ADMINISTRATIVE FUNCTIONS

All of the new high-availability and mail-handling features aren't worth much if you can't control them. Exchange Server 2010 also includes some new administrative capabilities that allow you to better manage your environment.

- ➔ **Exchange Management Console (EMC) behaviors.** The EMC itself sports new [features](#) such as an Organizational Health overview and the ability to add Exchange forests to the console tree.
- ➔ **Exchange Management Shell functions.** The Exchange Management Shell Command Log saves commands that you've executed in the EMC for future use. This feature complements the [administrator audit logging functions in Exchange 2010](#) to record when cmdlets are run and who runs them.
- ➔ **Exchange Control Panel (ECP).** Administrators can use the ECP for the [Outlook Web App](#) to manage features such as text and voice message integration, distribution list moderation and the ability to search multiple mailboxes.

## ARCHITECTURAL CHANGES

Exchange Server 2010 is a 64-bit-only product. The prevalence of 64-bit server hardware and 64-bit editions of Windows Server was one factor for moving solely to x64. Another major impetus was the fact that many Exchange installations will benefit from more memory since 32-bit operating systems are infamous for having memory constraints.

While Exchange Server 2007 shipped in both 32- and 64-bit editions, the 32-bit edition was not intended for production use—it was intended solely for lab use, virtual machines (VMs) and evaluation. Unfortunately, this hasn't stopped administrators from asking for a 32-bit version; however, that request is driven by the desire for the familiar management tools—not necessarily the need to run Exchange Server on 32-bit hardware.

There are a few workarounds for this, notes Exchange Server expert Paul Robichaux. A few options include using Remote Desktop to connect to the Exchange Server and performing management tasks using the Web-based Exchange Control Panel or using Windows PowerShell on any client that supports it.

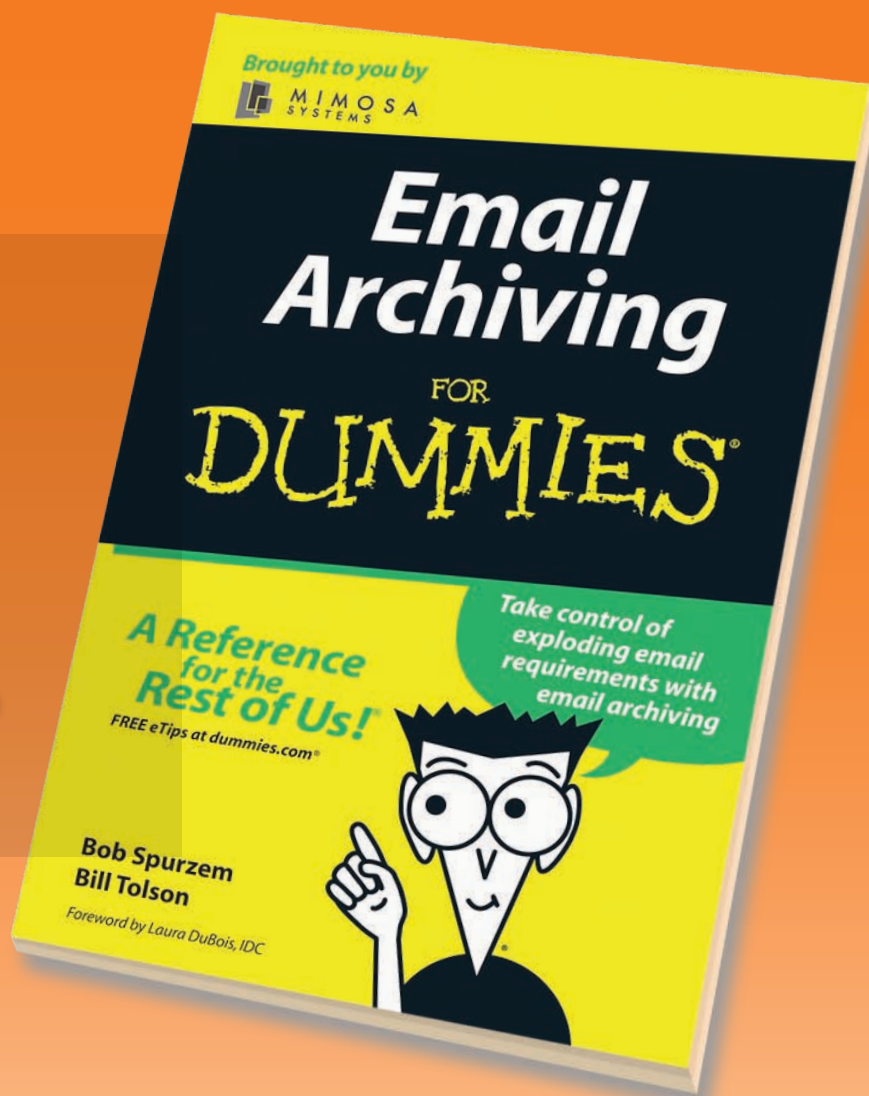
### EXCHANGE 2010 FEATURES: OUT WITH THE OLD

Many features from previous versions of Exchange are no longer supported in Exchange Server 2010—but only because they have been replaced with new or improved features. Some examples include:

- ➔ Exchange Server 2010's high-availability and site resilience features replaced clustering and continuous replication in all its incarnations.
- ➔ Mailbox database copies are another way in which DAGs replace a range of features such as storage groups.
- ➔ [Exchange Web Services](#) take the place of Web-based Distributed Authoring and Versioning extensions. If you have a lot of WebDAV-related functionality in your organization, you'll need to learn how [to migrate from WebDAV](#) before you use Exchange Server 2010.

Microsoft has a full rundown of what it removed or replaced in Exchange Server 2010 and earlier versions on its website. The older your existing Exchange architecture, the more you'll benefit from a complete understanding of what you're gaining and what you're losing. ■

# Get Your FREE Copy of *Email Archiving For Dummies*®



[www.mimosasystems.com/ttjuly](http://www.mimosasystems.com/ttjuly)

It's not just financial companies that are subject to government records retention requirements. **Most entities are subject** to one or more federal, state, or local records retention requirements. If you employ people, if you sell goods or services to the federal government, or if you are subject to federal civil litigation, **you have retention requirements.** Email Archiving For Dummies will help you recognize those retention requirements you are subject to and suggest ways to **meet your obligations.** Request a **free copy today.**



3200 Coronado Drive,  
Santa Clara, CA 95054  
408-970-9070  
[info@mimosasystems.com](mailto:info@mimosasystems.com)

Mimosa Systems and Mimosa NearPoint are trademarks of Iron Mountain. All other product and company names herein may be trademarks of their registered owners.

# Migration Requirements and Deployment Methods

*There are a few prerequisites you must meet as well as tricks to keep in mind when deploying Exchange 2010 in your environment.*

EXCHANGE SERVER  
2010 OUT OF THE BOX

MIGRATION  
REQUIREMENTS AND  
DEPLOYMENT METHODS

TESTING EXCHANGE  
SERVER 2010

HOW TO PROTECT  
EXCHANGE 2010  
AND ITS USERS

YOU SHOULD NEVER begin an Exchange Server 2010 deployment until you've confirmed that you can meet Microsoft's [prerequisites](#). You'll need [sufficient hardware](#) to run Exchange Server 2010 (at least 4 GB to 8 GB of RAM is recommended), Windows Server 2008 or Windows Server 2008 R2 and machines configured to handle the required directory server roles.

A useful tool to download and run while you're still preparing to deploy Exchange Server 2010 is the [Exchange Pre-Deployment Analyzer](#), which examines the environment in which you're planning to install the server and alerts you to any existing problems with the network topology.

Microsoft's [Exchange Server Deployment Assistant](#) is another useful tool. You enter information about your existing Exchange Server setup and the tool generates a checklist of things to do and watch for in the new environment. This is especially helpful if you're running a mixed architecture of Exchange Server 2003 and Exchange 2007, for example.

Running the latest Microsoft [Baseline Security Analyzer](#) prior to rolling out a migration project to determine if there are any outstanding security issues in your organization is also beneficial.

## ACTIVE DIRECTORY

One major prerequisite for adding Exchange Server 2010 to an organization is to [prepare the Active Directory schema to accommodate Exchange](#). If you're upgrading from Exchange 2003 to Exchange Server 2010, part of the process

includes configuring [legacy permissions](#) to ensure that Exchange 2003's Recipient Update Service (RUS) will still work properly. With the release of Exchange Server 2010, changes across all three of the most recent versions of Exchange are being tracked in a single document called [Active Directory Schema Changes Reference](#).

And you can't mention Active Directory without discussing the Microsoft [Active Directory Topology Diagrammer](#), which can read your current AD topology and produce a Visio diagram from it. The only drawback of this tool is that you need Visio 2003 or higher.

### TRICKS TO AN EXCHANGE 2010 UPGRADE

Upgrading an existing Exchange infrastructure is one of the most common scenarios—and also one of the trickiest. For example, the process of upgrading to Exchange Server 2010 might defy common sense about how systems are upgraded.

➔ **In-place upgrades.** You can't perform an "in-place upgrade" of Exchange Server 2007 to Exchange Server 2010. Instead, you must install Exchange Server 2010 in parallel, on a different system and then migrate the data to the new servers. Upgrades to Exchange Server 2007 had that same restriction, so experienced Exchange administrators will already be familiar with it.

In the long run, this restriction actually helps. You can leave your existing Exchange installation untouched and the new setup coexists with it until you choose to decommission it.

➔ **No backward migration.** Exchange Server 2010 does not support adding an earlier version of Exchange into an existing Exchange Server 2010 organization. According to Microsoft, if you create a new forest in which to install Exchange Server 2010, you can't add earlier versions of Exchange at a later time. If you plan to keep an earlier version of Exchange around for backward com-



patibility, building your new Exchange infrastructure in parallel allows you to do that. But it also means you must think ahead and not pull the plug on your legacy Exchange setup until you're sure that it's no longer needed.

Remember that you cannot set up Exchange Server 2010 to coexist with any version of Exchange prior to Exchange Server 2003. And any earlier versions of Exchange Server must be running in native mode, not mixed mode, before deploying Exchange 2010.

- ➔ **Third-party products.** Another major area to consider before attempting a migration is what third-party products you will use in conjunction with Exchange 2010. This decision isn't just about whether or not the product will work with Exchange 2010, but also whether the product's functionality is native to the new server version. For example, a third-party backup product may not be necessary since Exchange Server 2010 includes database availability groups.
- ➔ **Deprecated APIs.** Exchange Web-based Distributed Authoring and Versioning is being replaced in Exchange Server 2010 with Exchange Web Services or the EWS Managed API. This change mostly affects third-party applications that use WebDAV or custom-written, in-house programs. If you can't replace affected applications immediately, one workaround is to maintain an Exchange Server 2007 server for mailboxes that are managed by Web-DAV-based applications.
- ➔ **The Store Events APIs, CDOEX and ExOLEDB.** APIs have been removed from Exchange 2010 and were replaced by Exchange Web Services. In the future, a few other APIs, such as the Exchange Server MAPI Client and Collaboration Data Objects, will be moved to "extended support" status. ■

## Testing Exchange Server 2010

*Testing your Exchange Server setup lets you explore exactly how well your configuration will hold up under real-world conditions.*

EXCHANGE SERVER  
2010 OUT OF THE BOX

MIGRATION  
REQUIREMENTS AND  
DEPLOYMENT METHODS

TESTING EXCHANGE  
SERVER 2010

HOW TO PROTECT  
EXCHANGE 2010  
AND ITS USERS

EXCHANGE SERVER 2010 comes with a fair amount of self-testing functionality baked directly into the product. As with Exchange Server 2007, you can access them through cmdlets that have the prefix **Test-**. Here's a look at a few basic test-centric cmdlets that you'll want to run right after deploying Exchange Server 2010.

- ➔ **Test-ServiceHealth:** Determines if all the services that Exchange Server requires are up and running. This cmdlet also prints a report of the results.
- ➔ **Test-SystemHealth:** Performs several whole-system tests to determine if your server is configured according to best-practices guidelines.
- ➔ **Test-ReplicationHealth:** Determines if the mailbox servers in a given database availability group are replicating correctly with each other. You can also use **Test-MRSHealth** to check the health of the Mailbox Replication service.
- ➔ **Test-WebServicesConnectivity:** Checks that Exchange Web Services are functioning properly. **Test-OwaConnectivity** and **Test-ActiveSyncConnectivity** do the same thing for Outlook Web App and ActiveSync connectivity.
- ➔ **Test-Mailflow:** Checks whether or not mail can be sent to and from the system mailbox.

### KEEP A WELL-STOCKED TOOLBOX

So, what's available to test your Exchange Server 2010 deployment outside of the box? Microsoft has published a variety of testing components for Exchange, and these tools are a good place to start.

One of the most widely used tools for testing Exchange Server deployments is the Exchange Load Generator (ELG), which is available in both 32- and 64-bit versions. This program simulates user activity on a given Exchange server. Since different users might generate different loads—because of the size of their mailboxes or other user-specific configurations—this is a good way to determine if a given user's activity or a user group is causing a performance bottleneck.

However, the [ELG has two major caveats](#). First, you need to have client management tools installed on the machine generating the load, not on the server itself, and you shouldn't use it in a production network environment. The other caveat is that you should not run the ELG using your normal admin credentials for Exchange; use a reduced-privileges account as an additional security measure.

Microsoft recently revised the Exchange Load Generator tool and reissued it as Exchange Load Generator 2010. As the name implies, the company specifically designed this version to test Exchange Server 2010 installations, so you can't use it on older Exchange versions. If you have a heterogeneous environment (Exchange 2010 and earlier versions), you'll need to obtain both versions of ELG and use the appropriate one where needed. ELG 2010 is currently labeled as a beta version, but the final version is not expected to change much.

The Exchange Server Stress and Performance (ESP) tool is also very useful. Although it sounds like a clone of the ELG, it has slightly different functions.

*One of the most widely used tools for testing Exchange Server deployments is the Exchange Load Generator. However, the ELG has two major caveats.*

The ESP tool simulates large numbers of client sessions and includes support for a wide variety of protocols that Exchange uses. You can run ESP from a single client, but it's best to run it from multiple clients in different network segments for the most realistic testing results. The ELG is also available in both 32-bit and 64-bit versions. With this tool, however, you use the version that's most suited to the client machine that you're running on—not the server.

If you're unsure about the I/O capacity of the disk hardware for the system on which you're installing Exchange Server 2010, the Microsoft Exchange Server Jetstress tool can help. Jetstress simulates the type of I/O load that the Exchange database produces when multiple users access it.

Currently, there are three versions—two for Exchange Server 2007 (32-bit and 64-bit) and a 64-bit beta version for Exchange Server 2010. The final version for Exchange 2010 will support earlier versions of Exchange as well.

A common test for Exchange Server is to determine if the system is accessible from the outside. Instead of running this assessment yourself, Microsoft can do some of the work using the [Web-based Exchange Remote Connectivity Analyzer](#). This tool performs a variety of Exchange service tests from Microsoft servers to yours that include ActiveSync connectivity, Exchange Web Services, Office Outlook connectivity and inbound/outbound Internet email verification.

*If you're unsure about the I/O capacity of the disk hardware for the system on which you're installing Exchange Server 2010, the Microsoft Exchange Server Jetstress tool can help.*

### LOAD-TESTING EXCHANGE SERVER

In addition to testing Exchange Server's functionality, you have to know whether a given Exchange server setup can withstand its intended operational

load. Each third-party vendor has different views on how best to do this. Reading vendor white papers can help you parse out the tool that works best for your needs in varying situations.

Storage vendor EMC's paper on [Exchange Server 2010 performance validation and test results](#) examines how its CLARiiON storage product can help server performance. It also contains some helpful advice and capacity-planning strategies, such as how to compute the amount of server resources you need to support a specific number of users as well as which is more important in your organization—I/O throughput or capacity. The dichotomy between those two variables isn't always well-understood, but it's a crucial part of putting together an Exchange Server installation. The more redundancy and disks you add to a system, the more throughput, but the cost is that much more disk space.

*In addition to testing Exchange functionality, you have to know whether a given server setup can withstand its operational load. Each third-party vendor has different views on how to do this.*

VMware's paper on [scaling Exchange Server 2007 with VMware virtualization](#) focuses on how Exchange Server runs under VMware, instead of on bare metal. Although this is about Exchange 2007 and not Exchange 2010, it does emphasize the building-block approach to Exchange resources. It also looks at how this approach is easier to implement in a virtualized environment. ■

EXCHANGE SERVER  
2010 OUT OF THE BOX

MIGRATION  
REQUIREMENTS AND  
DEPLOYMENT METHODS

TESTING EXCHANGE  
SERVER 2010

HOW TO PROTECT  
EXCHANGE 2010  
AND ITS USERS

## How to Protect Exchange 2010 and Its Users

*Protecting Exchange Server 2010 is largely a matter of following best practices before and during every step of the product's lifecycle.*

EXCHANGE SERVER  
2010 OUT OF THE BOX

MIGRATION  
REQUIREMENTS AND  
DEPLOYMENT METHODS

TESTING EXCHANGE  
SERVER 2010

HOW TO PROTECT  
EXCHANGE 2010  
AND ITS USERS

MANY EXCHANGE SERVER experts have outlined some major steps you can take to protect an Exchange installation. Microsoft MVP Brien Posey recommends implementing relay restrictions to prevent the system from being used to send email without your authorization. This encompasses using **Sender ID**, **SPF** or **DKIM** to describe who can use your mail relays.

Other methods to safeguard your system include the following:

- ➔ Set up some type of mailbox protection.
- ➔ Use RPC over HTTP to limit the scope of what resources can be accessed remotely.
- ➔ Protect front-end servers with some type of edge protection independent of Windows Server itself when possible.
- ➔ Keep everything up to date.

The last point is easier to uphold when you use Exchange 2010's database availability groups for redundancy; you can apply rolling patches without worrying about much downtime. You do, however, need to be mindful of [suspending mailbox services on the server](#) before rolling out updates.

Properly planning and designing your network topology also helps protect your environment. Devin Ganger, an Exchange MVP, has listed a few [security best practices for Exchange Server 2007](#), many of which also apply to Exchange Server 2010, including the following:

- ➔ Use the Client Submission port for incoming email from trusted clients.
- ➔ Disable insecure (non-SSL) HTTP connections.
- ➔ Use commercial X.509 certificates—not default certificates—for Internet-facing servers.
- ➔ Use the Security Configuration Wizard to make sure that the operating system and Exchange are set up securely.
- ➔ Be sure to properly place Exchange servers. For example, you should place an Edge Transport Server role on your perimeter or Internet-facing machines and place other server roles—client access, hub transport, mailbox or unified messaging—behind that.

EXCHANGE SERVER  
2010 OUT OF THE BOX

MIGRATION  
REQUIREMENTS AND  
DEPLOYMENT METHODS

TESTING EXCHANGE  
SERVER 2010

HOW TO PROTECT  
EXCHANGE 2010  
AND ITS USERS

### SECURITY PRODUCTS FOR EXCHANGE

The most logical place to look for add-on security products for Exchange Server would be Microsoft, which pushes its own Forefront Protection 2010 for Exchange Server as a one-stop solution for security from outside threats. The Unified Access Gateway product for Forefront also allows remote users to plug securely into your Exchange environment; however, it requires that clients use Windows 7. Therefore, it won't be useful if the majority of your clients are on Windows XP or Vista.

There is a range of third-party Exchange security products: [Symantec Mail Security for Microsoft Exchange](#) supports not only Exchange Server 2010 but also Hyper-V virtualized installations. A downside of this product is that it comes with a high price per mailbox, but it does offer a great deal of protection for organizations without other methods in place.

GFI MailDefense Suite uses multiple virus scanning engines as part of its detection system. Individual products within the suite, such as GFI MailSecurity, are available separately, so you can tailor the product to your organization's specific needs. ■

ABOUT THE  
AUTHOR



**ABOUT THE AUTHOR:**

*Serdar Yegulalp has been writing about computers and IT for more than 15 years for a variety of publications, including SearchWinIT.com, SearchExchange.com, InformationWeek and Windows magazine. For questions about Exchange Server 2010 or previous versions of Exchange, contact Serdar at [thegline@optimum.net](mailto:thegline@optimum.net).*

EXCHANGE SERVER  
2010 OUT OF THE BOX

MIGRATION  
REQUIREMENTS AND  
DEPLOYMENT METHODS

TESTING EXCHANGE  
SERVER 2010

HOW TO PROTECT  
EXCHANGE 2010  
AND ITS USERS



**SearchExchange.com**

**Cathy Gagne**

Editorial Director

[cgagne@techtarget.com](mailto:cgagne@techtarget.com)

**Matt Gervais**

Site Editor

[mgervais@techtarget.com](mailto:mgervais@techtarget.com)

**Michelle Boisvert**

Managing Editor

[mboisvert@techtarget.com](mailto:mboisvert@techtarget.com)

**Martha Moore**

Copy Editor

[mmoore@techtarget.com](mailto:mmoore@techtarget.com)

**Linda Koury**

Art Director of Digital Content

[lkoury@techtarget.com](mailto:lkoury@techtarget.com)

**Marc Laplante**

Publisher

[mlaplante@techtarget.com](mailto:mlaplante@techtarget.com)

**Peter Larkin**

Senior Director of Sales

[plarkin@techtarget.com](mailto:plarkin@techtarget.com)

©2010 TECHTARGET. ALL RIGHTS RESERVED.



## ABOUT OUR SPONSOR



- ▶ [Migrating to Exchange 2010: Using EM Archiving to Resolve Issues and Simplify the Migration Process](#)
- ▶ [Osterman Research: The Concise Guide to eDiscovery](#)
- ▶ [Strategies for PST File Elimination](#)

**About Iron Mountain:** Iron Mountain Digital is the world's leading provider of information management services for email (MSFT Exchange Server), file and SharePoint archiving, eDiscovery, data protection and recovery, and intellectual property management. The technology arm of Iron Mountain Inc. delivers a comprehensive suite of on-premise and hosted solutions to thousands of companies around the world, directly and through a worldwide network of channel partners.