Regis University
ePublications at Regis University

Regis University Student Publications (comprehensive collection)

Regis University Student Publications

Fall 2008

Enterprise Vault and Discovery Accelerator: Email Archiving and Discovery Solution Implementation and the Legal Landscape

David Beebe
Regis University

Follow this and additional works at: https://epublications.regis.edu/theses

 Part of the Computer Sciences Commons

Recommended Citation

Beebe, David, "Enterprise Vault and Discovery Accelerator: Email Archiving and Discovery Solution Implementation and the Legal Landscape" (2008). *Regis University Student Publications (comprehensive collection)*. 116.
https://epublications.regis.edu/theses/116

This Thesis - Open Access is brought to you for free and open access by the Regis University Student Publications at ePublications at Regis University. It has been accepted for inclusion in Regis University Student Publications (comprehensive collection) by an authorized administrator of ePublications at Regis University. For more information, please contact epublications@regis.edu.

Regis University
College for Professional Studies Graduate Programs
Final Project/Thesis

Disclaimer

Use of the materials available in the Regis University Thesis Collection ("Collection") is limited and restricted to those users who agree to comply with the following terms of use. Regis University reserves the right to deny access to the Collection to any person who violates these terms of use or who seeks to or does alter, avoid or supersede the functional conditions, restrictions and limitations of the Collection.

The site may be used only for lawful purposes. The user is solely responsible for knowing and adhering to any and all applicable laws, rules, and regulations relating or pertaining to use of the Collection.

All content in this Collection is owned by and subject to the exclusive control of Regis University and the authors of the materials. It is available only for research purposes and may not be used in violation of copyright laws or for unlawful purposes. The materials may not be downloaded in whole or in part without permission of the copyright holder or as otherwise authorized in the "fair use" standards of the U.S. copyright laws and regulations.

Enterprise Vault and Discovery Accelerator: Email Archiving and Discovery Solution Implementation and the Legal Landscape

by

David Beebe
DavidBeebe@gmail.com

A Thesis/Practicum Report submitted in partial fulfillment of the requirements for the degree of Master of Science in Computer Information Technology

School of Computer and Information Sciences
Regis University
Denver, Colorado

October 26th, 2008

Abstract

One of the most pressing Information Technology challenges organizations are facing today is managing the vast amount of data that exist at their company, especially with regard to email data. Over the last decade many legal regulations have been passed and amended to address these growing data concerns, especially with regard to email, as they contain critical business communications. These regulations require organizations to be able to quickly and accurately search and recover email data related to legal proceedings, which has led to an overwhelming adoption of email archiving and recovery solutions. Email archiving and recovery solutions allow organizations to manage their email data in an uncompromised format, to be able to meet complex and detailed legal search requests and to comply with all the varied legal regulations. Enterprise Vault and Discovery Accelerator is a leading product suite that provides email archiving, search and recovery functionality. This thesis uses the qualitative and design research methodologies to determine how Enterprise Vault and Discovery Accelerator are able to address the legal landscape that organizations are faced with today.

Table of Contents

Certification of Authorship of Thesis/Practicum Work ii
Advisor/MSCT 698 Faculty Approval Form v
Abstract vii
Table of Contents viii
Executive Summary 1
Chapter 1 – Introduction 4
1.1 - Overview of Current Environment 4
1.2 - Legal Landscape 5
1.3 - Enterprise Vault, Discovery Accelerator and Legal Compliance 8
1.4 - Project Goals 12
1.5 - Key Archiving Considerations 14
1.6 - Barriers to Success 16
Chapter 2 – Review of Research and Methodology 21
2.1- Literature Overview and Research 18
2.2 - What is Unknown about the Project 20
2.3 - Contribution the Project will Make to the Field 21
2.4 - Research Methodology Overview 22
2.5 - Design Research Methodology Applied 23
Chapter 3 – Enterprise Vault & Discovery Accelerator Configuration 29
3.1 - Hardware 27
3.2 - SAN Storage Allocation and RAID 28
3.3 - Solution Architecture 29
3.4 - Testing, Training and New Mailbox Activations 32
3.5 - Installation Prerequisites 32
3.5.1 - Account Creation and DNS Updates 33
3.5.2 - Enterprise Vault Application Servers 35
3.5.3 - SQL Server 35
3.5.4 - Exchange Server Extensions and Forms 35
3.5.5 - Backups 36
3.5.6 - Virus Exemptions 36
3.6 - Enterprise Vault Mailbox Configuration 32
3.6.1 - Policy Configuration 37

3.7 - Enterprise Vault Journal Configuration....39
3.7.1 - Policy Configuration....39
3.8 - Enterprise Vault Reporting and Operations Monitor....40
3.9 - Discovery Accelerator Configuration....41
3.10 - Enterprise Accelerator Searches....41
3.11 - Day to Day Administration and Troubleshooting....42
Chapter 4 – Project Analysis....45
4.1 - What Went Right....43
4.2 - What Went Wrong....44
4.3 - Summary....48
Chapter 5 – Lessons Learned and Next Evolution of the Project....52
5.1 - What was learned from the project experience....50
5.2 - What would have been done differently....52
5.3 - Did the project meet initial expectations....53
5.4 - If the project continued what would be the next stages....54
5.5 - Project Summary....56
References....62
Appendix A....66
Appendix B....75
Appendix C....78
Appendix D....98
Appendix E....155
Appendix F....178
Appendix G....184
Appendix H....193
Appendix I....202

List of Figures

Figure 1: Design Research Cycle and Reasoning 23
Figure 2: Flow of Archive and Journal Data 29
Figure 3: Exchange Environment for Both Companies 30

List of Tables

Table 1: Server Name, Role and Hardware 27
Table 2: Server and Storage Allocation and RAID Level 28
Table 3: Account Creations 33
Table 4: Employee Provisioning 38
Table 5: Journal Provisioning 40

Executive Summary

The corporate scandals of Enron and WorldCom forever changed the landscape of publicly owned companies and one of the most wide reaching results from these company collapses was the rapid attitude shift by the public and government towards the swift implementation of regulations regarding corporate compliance, legislation and legal electronic discovery. Today public organizations are required by law to meet very strict legal requirements regarding the management of their data, especially as it relates to key communication mediums like email, and the inability for companies to comply with these guidelines can lead to severe consequences. Email presents one of the most significant data management challenges for any organization as it is often one of the first items that legal discovery teams will want to have searched when lawsuits are pending due to the fact that a significant amount of communication is handled over email, including the distribution of key documents relating to business operations. A study in 2003 found that email is an accepted form of written confirmation for the process of transactions in 79% of organizations (Osterman Research, 2003).

One example that clarifies the complexities of managing email data at an organization can be illustrated by doing a simple calculation. If you have a midsized company of two thousand employees and each of those employees sends and receives an average of fifty emails a day then over the course of a year an overwhelming thirty six million emails will have been sent over the company network, which means that the organization could be liable for being able to search and recover data from all of those emails to respond to legal discovery requests for pending lawsuits. Because of these challenges around search and retrieval of email data the market for email archiving

products has grown dramatically in the last five years. SearchCIO.com defines email archiving as "a systematic approach to saving and protecting the data contained in e-mail messages so it can be accessed quickly at a later date" (2007) and it has become a key area of attention for CIO's of companies of all sizes, whether public or private.

One of the pioneers in developing a product to meet this demand was KVS, which was founded in 1999 and eventually bought out by Symantec. Their flagship email archiving product, Enterprise Vault, has been deployed at thousands of organizations of all sizes around the world to meet the email retention and recovery requirements driven primarily by legal compliancy concerns. Their email search and recovery product, Discovery Accelerator, complements Enterprise Vault by allowing organizations to quickly search and export email archived by Enterprise Vault that meet the criterion established by the legal team, thereby ensuring that they are able to provide an end to end solution to managing email data and turning that data over to legal counsel for review.

This thesis used the qualitative and design research methodologies to demonstrate how this product suite is able to address the legal landscape that organizations are faced with today. Through in depth research, testing and deployment of Enterprise Vault and Discovery Accelerator at a large public organization and their parent company this thesis validates that the product suite is able to effectively meet the complex legal requirements that these organizations were faced with. Although, as with any large enterprise wide solution like this, there are many business requirements that must be addressed by key business units and many pitfalls that must be circumvented to ensure that the solution is able to not only meet all the requirements the organization has today, but able to easily and affordably adapt to the ones that are expected to be presented in the near future.

This thesis covers many of those common pitfalls and deployment oversights that frequently occur, as well as identifying key areas that need to be addressed for the effective day to day management of the solution.

Chapter 1 – Introduction

One of the challenges organizations are facing on an increasing basis is how to manage all of the email data that flows through an organization on a daily basis so that this data can still be quickly searched and recovered to meet legal obligations as they arise. The consequences for not having a solution in place to handle this requirement can be costly and potentially much more expensive than the implementation and management expenses of deploying and maintaining an email archiving and recovery solution.

One case that illustrates this is Zubulake v. UBS Warburg LLC, an employee discrimination case heard in the U.S. District Court in New York, which verified that organizations are responsible for retaining and producing electronically stored information (ESI) in a timely manner (Litigation Holds, 2008). UBS legal counsel produced 100 emails with regard to this case and stated that the results were complete, but the plaintiff's counsel was able to uncover that UBS never searched any of its backup tapes that also contained numerous relevant emails and that certain emails on the backup tapes were missing from UBS's files. The end result was a 29.2 million dollar verdict against UBS, which brings to light many relevant questions.

Was UBS really trying to hide data or was the recovery of old emails so complex and time consuming that it either wasn't completed at all, or wasn't completed properly? Once UBS responded to the legal counsel inquiry that it completed the search they exposed themselves to considerable risk if it was not complete. For example, suppose a relevant email was sent by a UBS employee to an individual at another company, and suppose that that other company provided proof to the plaintiff of that received email. Once the plaintiff's counsel was able to demonstrate that the same email was not

provided by UBS they gave credibility to the fact that UBS might be trying to hide data. This type of example is all too common with regard to many legal proceedings today, which is why companies are quickly embracing email archiving and recovery solutions like Enterprise Vault and Discovery Accelerator. This is precisely one of the driving forces that the public company and its parent company, that this thesis is based on, choose to deploy this product suite.

1.1 – Overview of Current Environment

A study done by Osterman Research in 2004 showed that only 15% of organizations surveyed had deployed an email archiving solution, but 62% of those surveyed believed that an archiving solution was either "desirable" or "very desirable". The company and parent company fall under that 62% and had decided that employing an email archive solution was not only very desirable, but essential to their long-term livelihood. Currently both are under legal hold, which is defined by Expert Business Source as a "suspension of a company's document retention/destruction policies for those documents that may be relevant to a lawsuit that has been actually filed, or even one that is reasonably anticipated" (Neuburger, 2007). These legal holds presented the companies with many challenges that they were unable to meet without considerable resources in time and money and no guarantee that even with the allocation of all of these resources that the data they provided to legal counsel was complete, which is one of their key driving forces behind the desire to implement an email archiving solution.

The company and their parent company are currently on Exchange 2003 for their email platform and both companies are in the same email organization and managed by the child company. All email data is backed up by completing full database backups

nightly as well as brick level backups for single mailbox recovery and/or single email recovery. Brick level backups, unlike full backups, backup the data differently to allow for granular recovery of individual email items, such as one specific email or a folder in an inbox. Although both of these backup methodologies allow the companies to meet many of the needs that are required, such as recovering all email after a small or large disaster and recovering individual email items when users accidentally delete them, it does not offer an effective or time efficient way to search across all email data stores and recover specific email items that refer to a specific legal discovery. For example, one Fortune 500 company was ordered to turn over all email relating to a wrongful termination suit and was presented with the possibility of having to search 20,000 email backup tapes, which was estimated to cost 1,000 a tape, for an approximate total of twenty million dollars (Morrison & Foerster, 2001). One reason this is such an excessive cost is because the general backup methodology prior to the legal landscape changing was to take a backup every night, put the data on tape and send offsite, rather than keeping and maintaining a complete record of every email sent and received onsite for quick search and recovery. Given the company and parent company's current situation the present challenges would all be met by the implementation of an email archive and discovery solution like Enterprise Vault and Discovery Accelerator.

1.2 – Legal Landscape

The legal landscape for messaging has changed dramatically over the years as email has become the accepted medium of communication for key business operations. Historically government regulations lag behind newer technologies such as messaging, but over the last decade the government has amended and passed many regulations to

catch up on the exponential acceptance and widespread use of email, requiring organizations to handle their messaging infrastructure in different ways. Some of the key regulations include, but are certainly not limited to, Sarbanes-Oxley (SOX), Gramm-Leach-Bliley (GLB), Health Insurance Portability and Accountability Act (HIPAA), and the Federal Rules of Civil Procedure (FRCP).

HIPAA is related to the healthcare industry and most of the privacy rules became officially enforced on April 21st, 2005 (HIPAA, 2006). This regulation requires organizations that send email messages which contain protected health information be secured and that both the sender and the recipient of the message are properly verified and authenticated, as well as ensuring the messages are protected whether they are in transfer or in rest. As with most regulations referenced here there are not specific technologies that should or should not be used to meet them, even though in general email archiving solutions are considered to be one of the ways of complying to these regulations. Although email archiving can be used to meet some of the requirements with regard to HIPAA, clearly this does not address all of the Information Security requirements of this regulation, as well as the fact that HIPAA applies to a small subset of organizations that do business in the health care industry and send health care information via email, which does not impact either the company or parent company.

GLB was passed in 1999 and is also referred to as the Financial Modernization Act and its primary goal is to protect consumers' financial data (GLB, 2006). The act refers primarily to Nonpublic Personal Information (NPI) and the collection, use and disclosure of NPI and what is called the Safeguards Rule, which is related to the processes that must be taken to protect NPI. The Safeguards Rule is related to the

messaging infrastructure and it has to do with the inclusion of security relative to the size and complexity of the infrastructure and the implementation of technologies that assist in the detection and prevention of intervention as well as the overall security of email. Also it requires logging and reporting that is able to demonstrate compliance.

SOX only applies to public companies and is probably the most familiar of all the regulations, as anyone that has worked in an IT organization for a larger public company has probably been involved in some sort of audit regarding the compliance to SOX (SOX, 2006). This regulation goes as far as including criminal penalties for those who fail to comply to its' provisions and the overall intent is to ensure accountability and transparency to corporate financial operations. Sections 302 and 404 are the most relevant to the messaging infrastructure and include many of the same regulations as GLB and HIPAA with regard to Information Security and the confidential transmission and storage of email data and tracking and logging of messaging traffic. Also it includes requirements for message indexing, archiving and retention. This regulation has the most direct impact on the companies and is one of the primary drivers of implementing an email archiving and discovery solution.

FRCP applies to all organizations that have the potential of being involved in litigation in the U.S. Federal Court system and there are various amendments that went into effect on December 1st, 2006 that specifically mandate electronic discovery of data requirements, specifically where their data is and what data should be searched and how to retrieve it (FRCP, 2007). It requires companies to be able to discuss how and where they store their Electronic Stored Information (ESI) in the pretrial proceedings, to preserve their ESI compliancy and be able to produce it while ensuring that metadata is

intact and produce it within discovery timelines. Failure to comply with this can include sanctions, fines and executive liability. This regulation, along with SOX, are critical for both companies as currently both are involved in lawsuits, which are a common occurrence, and given the amount of business done via email it is critical that they are able to meet the e-discovery requirements stipulated in FRCP. Take, for example, the case Zubulake v. UBS Warburg LLC mentioned earlier, not only did they lose 29.2 million to the plaintiff in this case; the government could have come after them as well for violating this law.

Depending on the industry the business operates in, the size of the business, whether it is publicly or privately owned and whether it can be involved in litigation in the U.S. Federal Court System, one or many of these regulations might affect the way they have to manage their messaging infrastructure with regard to email archiving, discovery and retrieval. Although these are the most well known and far reaching regulations related to this topic there are some others that are worth noting. California l386 requires disclosure of computer related security breaches and California AB 1350 requires businesses that manage personal information about California residents to implement "reasonable security procedures" to protect that data (Overly, 2006). And the Family Educational Rights and Privacy Act (FERPA) govern the privacy of student records, which includes email (Overly, 2006). Along with these regulations it is worth noting that there are IT frameworks that help organizations research, implement and maintain sound practices and policies around the messaging infrastructure that would also assist them in complying with these regulations. The next section provides a more

detailed evaluation of these regulations and how email archiving solutions like EV and DA address them.

1.3 – Enterprise Vault, Discovery Accelerator and Legal Compliance

With regulatory requirements and the risk of penalties including civil damages and, in some cases, even criminal prosecution organizations have had to embrace new messaging solutions that help them manage the incredible amount of email that flows through an organization. Many of these regulations previously covered are addressed by email archive and retrieval solutions, such as Enterprise Vault (EV) and Discovery Accelerator (DA). There are primarily three areas to look at when reviewing how regulations apply to the messaging infrastructure and how they are met by Enterprise Vault and Discovery Accelerator, which are the origination of the email, the delivery of email and the storage and management of the email and messaging data.

The origination or creation of the email has to do with ensuring that each message is being sent from a specific person, that there is proper security in place to protect the data in the email, especially if it is health related or contains NPI data, and that the appropriate disclaimers are in place marking the data as proprietary or as containing health information, etc. The main regulations that apply to this are HIPPA, GLB and SOX, and EV and DA offer certain compliancy benefits with regard to this, but only would supplement the security solutions that would be required to meet this. EV and DA allow every email sent to and from the organization to be archived for quick review and recovery, so we would be able to see the email, ensure it contained the proper disclosures, review the content to see what information was contained in the email and see who sent the email and when exactly they sent it. This information would also be available in

exchange logs and from backups, but could end up being a very time intensive process to recover, especially if the request was in the past by a week or more. Also backups are usually only run every night, so if journaling was not used to capture this data, like with Enterprise Vault, the data could be compromised before it is backed up.

The delivery of email must ensure that there are controls in place to prevent NPI or private health information from being improperly accessed, ensuring there are audit trails that can be reviewed and that the organization is preventing unauthorized access to corporate trade secrets and confidential information, as well as preventing the forwarding of any of this information. The main regulations that apply to this are HIPAA, GLB and SOX and EV and DA can help organizations comply in this area quite a bit. Enterprise Vault can be set to do a full index of every message sent to or from the organization and the integration with Discovery Accelerator allows for this data to be quickly searched for relevant terms, as well as scheduled searches to be completed on a set regular basis. This allows for an organization to quickly become aware if specific content that meets certain criteria is emailed outside of the company or sent where it should not be. Also EV and DA offer detailed logging and reporting capabilities that can be reviewed to see exactly where an email was sent to or forwarded to, if it was blind copied to someone else and what data was contained in that email. For example, several months after deploying the solution for the parent company there was a concern that confidential information sent in an email was forwarded to another email account that was not authorized to see this information. This concern was raised to the Director of IT which subsequently requested an immediate search for all email that was sent or received containing that

specific text in the body of the email. Within one hour all email had been searched and all results were accurately turned over to the necessary managers for review.

Arguably one of the most important areas that an organization must meet regulations has to do with the management, storage and eventual deletion of email data. The email must not be accessible by unauthorized individuals, must not be altered or compromised and must be able to be retrieved as necessary. Most importantly they should be retained for the amount of time stated in the email data retention policy, which ideally should exist, and should not be retained past that specified amount of time, unless they are in middle of litigation in which case IT should be working with legal counsel to determine the new temporary retention requirements of the email data. This applies to all of the regulations discussed, including HIPAA, GLB, SOX and FRCP and is where EV and DA can offer the greatest benefits in meeting these requirements. EV stores all of the archived emails in tiny files and even if they were accessed could not be used to review email data. It also can be set to do full indexing of all emails, provides detailed logging and reporting and can handle all the organizations archiving and email deletion requirements automatically.

A significant challenge for IT organizations is being able to adapt to the changing retention needs of email data based on pending litigation and other requirements, and EV can be changed in a matter of seconds to purge old email data or to keep all email ongoing until the end of a lawsuit. The best way to elucidate this is to give an example. Many organizations that I have been involved with send full email backups on tape to their offsite storage vendor every night and when they meet their retention requirement those backup tapes are able to be called back for re-use for other backups, since the tape

is still in fine condition to be used again. Often those tapes are not re-used in a timely fashion, sometimes resulting in months of email data existing on tape beyond their documented retention policy. If that company was to enter into litigation all of this data would be subject for search, even though it officially should no longer exist. That could add substantial risk and costs to the company since e-discovery would have to potentially occur against that data as well.

With EV the retention dates are put into the policy and they are automatically maintained, so once the retention date has passed that data is no longer retrievable. The other key area that this solution affects is the retrieval of relevant email data. With the amendments to FRCP organizations are required to be able to quickly search and recover relevant data to litigation, and DA not only meets these needs, but exceeds them as it is able to search millions of records in minutes. It also optimizes the complete process of reviewing the items returned in the search, allowing for the reviewers to quickly mark the relevant emails and discard the irrelevant messages. It even lets the company get more granular by allowing them to complete detailed searches, retain the relevant emails, and then continue following their existing retention policy for all email that was not returned as relevant to the lawsuit. The power and granularity of DA integrated with EV ensures that organizations are not penalized for the inability to quickly return relevant results to litigation or other important requests.

1.4 - Project Goals

The overall goal of this project is to address legal liabilities and search and recovery challenges by implementing Enterprise Vault and Discovery Accelerator for the

company and parent company. To accomplish this there are many incremental steps that need to be successfully completed to ensure that this end goal is reached.

First the solution must be compatible with the email solution in place at the organization. Microsoft Exchange has a 65 percent market share across all organizations therefore a majority of solutions are designed to be compatible with Exchange (Ferris Research, 2008). In this thesis the company and parent company are on Exchange 2003 so the first criteria addressed were confirming the solution was compatible with this version of Exchange. Then all of the prerequisites and configuration changes must be identified and completed prior to the installation and configuration of Enterprise Vault and Discovery Accelerator. There are two types of archiving that will be implemented with Enterprise Vault, Individual Email Archiving and Journal Archiving. Email journaling, or journal archiving, allows you to archive all incoming and outgoing email in the organization, so all email that is sent or received is logged and kept for the time period the company determines. This is the key component for meeting legal regulations as this archive maintains a copy of every email message sent and received without the user being able to modify the contents, so legal teams are able to maintain confidence that this is a pristine data set that is not compromised. Enterprise Vault is also going to be deployed on every user's individual mailbox, or individual email archiving, so they can archive their own email in their own mailbox. When they archive their email it takes up less storage space on the mailbox server while still allowing them the ability to search and retrieve their own email, that way they can keep more email without hitting their mailbox quota as quickly.

The deployment of the solution will be completed in a phased approach, with each phase requiring manager signoff before moving on to the next stage. A pilot group for each company will be deployed with a test plan to ensure that Enterprise Vault does not have any adverse impact before being deployed corporate wide. Enterprise Vault Reporting and Operations Manager will be deployed after the applications are installed and configured to ensure the stability and functionality of the solution. Installation and configuration of Discovery Accelerator will be completed in the initial phases, including the testing and training to key individuals at both companies that will be processing the search requests, to ensure that no configuration changes will need to be made to EV due to search and recovery issues with DA.

In the later phases there will be many things that will need to be finalized to ensure the appropriate IT staff all has knowledge and experience to support the solution. A detailed FAQ and training session will be completed with the help desk to ensure they are able to effectively respond to any questions and concerns brought up by the end users. Documentation and testing will be completed of all daily, weekly, monthly and quarterly operational responsibilities and implementation of a process to ensure that these checks are completed in the necessary time windows. Documentation will also be completed for common troubleshooting procedures and application support information.

The end goal will be to complete the deployment to the rest of the employees at both companies, including the installation of the Enterprise Vault Outlook Snap-In on all of the client desktops and laptops, and ensure that all new employees hired are also deployed on this solution. The completion of all of these tasks will mark the successful completion of the deployment of Enterprise Vault and Discovery Accelerator. The true

mark of success will be when the first legal request is received by the Information Technology organization and they are able to respond quickly and accurately to the request.

1.5 – Key Archiving Considerations

Email archiving and discovery adds an added layer of complexity to the messaging infrastructure and therefore there are some key configuration considerations that need to be made prior to the installation of any solution that addresses these requirements. Many of these decisions will need to be made at the management level and therefore should be addressed far enough in advance of the planned deployment so that it doesn't impact the project timeline. Many of these decisions should be documented in a corporate data retention policy as they will contain critical information with regard to legal proceedings and discovery of email data.

The most important consideration will most likely be based on email retention requirements. This needs to be considered with regard to the Individual Email Archiving and Journal Archiving, explained in the previous section. Many organizations prior to introducing a product like EV have defined a single email retention requirement for the whole organization, but EV offers granularity that allows organizations to approach this much differently. For example it might be required that Executives and Legal staff have different email retention requirements then standard users. All of this can be configured, but requires up front determination; otherwise it will take extensive work to change this configuration at a later time. For example the company and parent company decided to organize the users into Executive, Legal, HR and Standard to allow for different retention requirements for these groups.

Once the grouping is defined by the business they will need to decide how long to retain the email for each group. These may or may not be all the same when the solution is first deployed, but this is a setting that can easily be adjusted at any time based on the business requirements, legal obligations, etc., as long as the proper grouping has already been established. It is important to note that most likely the Individual Email Archives and the Journal Archives will have the same retention settings, but regardless the Individual Email Archives should never have a retention setting longer than the Journal Archives. This is based on the fact that the Journal Archives is the only repository that should be used to meet legal requests and if email is maintained longer in the Individual Archives the organization might be liable for searching that data, even though most likely it is not a pristine data set. Recall that the Individual Email Archives is managed by the user and items can be deleted prior to being archived, which is why it should not be used for legal requests, whereas the Journal Archive contains every single email sent to and from the organization and this data cannot easily be compromised.

With regard to the Individual Email Archives there are many specific settings that need to be configured as well. The most important one is when email is automatically archived for the employee. For example the company automatically archives all email older than three months and the parent company older than six months. One consideration to make here is with regard to mobile email devices and how long they retain email on them by default, so if that is configured to one month you probably never want to archive an email automatically unless it is older than one month. When an email is archived a shortcut is left for that email in the inbox, which will contain a specific number of characters, and this represents another configuration option. Both companies

chose 500 characters as this is the recommended configuration. You can also get more detailed with archiving, for example you can set it to archive any email with an attachment over a certain size after a certain amount of time. The company decided to automatically archive all email over two months old that was over two MB in size, but the parent company has no space issues for mailbox size or restrictions so they decided this setting would not offer any benefits.

These represent the key settings that will impact the end users and the business, so once these have been addressed the installation and configuration will be able to be completed with little delay. There are many other configuration options that will be reviewed in the detailed installation and configuration documentation part of this paper.

1.6 – Barriers to Success

There are many barriers to success that need to be identified up front to ensure the successful implementation of Enterprise Vault and Discovery Accelerator. In a survey of over 1,000 executives and project managers, research firms VitalSmarts and The Concours Group identified five key areas to project success, which include unrealistic project deadlines and budgets, project sponsors that are not vested enough, team members who do not point out project concerns and problems and those that do are not willing or able to support the project (Wall Street & Technology, 2008). Each of these was potential barriers that were addressed in this project to ensure the success.

Fortunately one of the most common barriers sited by this survey was overcome very early in the project, which was management's approval of the overall budget of this project, including the hardware, SAN storage space, professional services, software and maintenance costs.

To address potential barriers to success related to project members and concerns with identifying project challenges and issues a phased deployment approach was used that required management approval to move forward with each phase of researching, testing and deploying the solution. Without that it is common that projects will be deployed to production without implementing a detailed test plan to ensure that there are no adverse and unwanted side effects of the new solution. This is especially critical given the fact that Enterprise Vault interfaces directly with arguably one of the most important infrastructure applications at an organization, email. EV also adds a snap-in to the Outlook client which will be installed on virtually every desktop and laptop in the company, so even if only 1% of the individuals have adverse affects from the installation of it that still can be a significant number of users impacted depending on the size of the organization. Given the reach of this solution it is critical that the proper time and resources are allocated to ensure that there is not a negative impact to the day to day business operations and flow of email internally and externally.

Another barrier to success listed by Wall Street and Technology is the ability to address and overcome various project challenges, which will most likely require time, resources and management approval often driven by the project sponsor. Projects this complex have a tendency to require last minute configuration requirements that may impact other business critical applications, such as email in this case, and if they are not addressed they may stop the project from moving forward. Therefore it is key when these do arise that the proper time, resources and management approvals can be addressed quickly so the project doesn't stall, for when a project stalls too long many things can happen, ranging from lack of confidence from management that the project is

being handled properly to other projects coming up that have a higher priority which may require a reallocation of resources. Overall the barriers to success for this project are very controllable as long as the engineer, project manager and project sponsor meet regularly to discuss the project status and existing challenges and use the proper phased approach to deploy the solution.

Chapter 2 – Review of Research and Methodology

The research for this project covers two main areas, an in depth analysis of the email archive and recovery solution Enterprise Vault and Discovery Accelerator, and a review of the legal landscape and how it has reacted and shifted over the years to the widespread acceptance of email use by businesses. These two topics are brought together by the fact that email archiving and recovery solutions like EV and DA facilitate organizations to meet and even exceed many email related components of the federal regulations and offer flexibility and scalability to new regulations that might be introduced in the future.

2.1 – Literature Overview and Research

There were several methods of research used to gather relevant information for the core data required to complete this project, although obtaining research online was instrumental throughout the process as most key references required were available electronically from a wide variety of sources. Once again this research varied quite a bit based on the type of data required, as research around EV and DA, including key benefits of the product suite, best practices for settings and the overall configuration of the product to meet business requirements was primarily qualitative. The research completed regarding the legal regulations related to the retention, search and recovery of email data was completed using online research, professional book publications, professional journal publications, technical white papers, electronic copies of the Federal regulations and specific legal case references.

Author Steiner Kvale writes that the interview approach to qualitative research is "a careful questioning and listening approach with the purpose of obtaining thoroughly

tested knowledge" and follows up by saying "The topic of the interview is introduced by the researcher, who also critically follows up on the subject's answers to his or her questions." (1996). This captures how much of the research was obtained for EV and DA, through the proper interviewing, or simply conversations and meetings as Kvale also explains as part of this interviewing qualitative process, with various executives, project stakeholders, records management staff, technical experts and professional consulting services with Symantec. These meetings were a critical component to the research process as it was the only way we were able to clearly evaluate all of the features and options within the product suite and come to a consensus on the key settings that each company wanted to implement to address the various business requirements and legal regulations. Also throughout the deployment of the product suite while the consultant was onsite there were literally hundreds of inquiries and follow up questions that were asked and then evaluated accordingly to determine the relevancy and direction that the companies would want to take from those answers. A critical part of the process, as Kvale stated in the quote above, was following up on the answers received, which was done extensively to clarify details, question recommendations and summarize the information to assure that the direction of the conversations were coming to a clear consensus of the preceding actions to be taken.

Completing the research on the legal landscape was done through a variety of means. There were two areas I was primarily concerned with in regard to the legal research, first a brief review of the history and changes over the years with technological advances and how the government reacts by adopting laws to cover these changes. Second, and most importantly, I completed a detailed analysis of all of the legal

regulations related to electronic discovery and in particular how email archiving and recovery can help organizations meet this requirement. Once again authoritative online resources in this area were plentiful. The U.S. Government's official web portal, USA.gov, was able to direct me to a multitude of resources in obtaining electronic copies of the actual regulations as well as analysis of the regulations that assisted me in breaking down how the laws impacted and related to the companies and the email archiving and recovery solution. Other online resources included technical white papers, newspaper articles, magazine article and trade journal publication databases such as LexisNexis Academic and ACM Digital Library, and some print based resources. Search engines such as Google.com, AskJeeves.com and Cuil.com were also valuable resources in leading me to many of these valuable online resources.

2.2 – What is Unknown about the Project

There is considerable information available regarding the legal regulations and how organizations can take steps to comply with these, but there are many unknowns to how these regulations might change over time. Currently the regulations are technically unspecific with regard to what types of solutions or technologies need to be implemented to ensure compliancy and they are also extremely vague on many areas, such as specific requirements around search and recovery times for email. Rather the way these are written leaves quite a bit of room for interpretation with regard to how quickly companies need to return results with regard to legal requests. This represents a significant unknown, especially with regard to how this might change over time. Regardless the solution deployed for these companies should easily meet any changes in the regulations

with regard to the adoption of any specific timeline requirements for searching and recovering email data.

Another unknown in this project, that was specifically not covered, is related to the email archive and retrieval market as a whole. Although Enterprise Vault and Discovery Accelerator are leaders in the market place with regard to maturity, deployments and overall functionality, there are many competing solutions that offer much of the same and additional functionality. Research related to those solutions was not completed due to the decision from the start by the companies to go with Enterprise Vault. This was based on the reputation of the solution and the existing role the vendor already played at both companies. Therefore an unknown is what the tradeoffs would be if other solutions were researched and evaluated.

2.3 – Contribution the Project will Make to the Field

Based on the research that I completed throughout all phases of this project I believe this will make several noteworthy contributions to the field. First, outside of documentation from Symantec on best practices and other implementation material in deploying Enterprise Vault and Discovery Accelerator I was unable to find any other well thought out and documented unbiased real world configuration and implementation research for these products. Given the reach that this solution has in the market place there is a definite need for more information from customers that have deployed these solutions and the challenges that had to be addressed throughout the process. The Lessons Learned section of this project would be invaluable to any engineer that is going to be deploying this solution for their company as it quickly identifies some of the challenges faced that other organizations will certainly face as well.

The other main contribution this project will add to the field has to do with the legal regulations and compliancy research related to EV and DA. One undeniable benefit that this solution offers is to the Information Technology staff, which is based on the fact that this dramatically reduces time and effort required when legal search requests are inevitably received. These types of requests can be very tedious and take days to weeks to complete when a solution like this is not in place, therefore the benefit of getting management approval for this solution can be a big boon to the IT staff. The legal regulations and compliancy details discussed in this project, and in particular some of the cases outlined, help IT organizations communicate the value that this solution offers to the business as a whole. The end result is that the IT organization will look better when these requests are received and they will have more time to dedicate to other projects and tasks.

2.4 – Research Methodology Overview

There were two research methodologies used for the process of obtaining, integrating and creating value in the research for this project. These methodologies ere very different based on the fact that there were two distinctively different research objectives that were required for this project, but in the end both come together for a complete understanding of the solution and how it meets legal regulations. The first research methodology used was discussed in more detail earlier in this section and was the interview method of qualitative research (Kvale, 1996). This method was highly effective and appropriate based on the goals required to successfully deploying EV and DA. It required many individuals in different disciplines to agree upon key global

application settings that had to be properly communicated to all employees in both companies and in line with various business requirements and legal regulations.

The second research methodology used in this project was the Design Research Method (DRM). Figure 1 outlines the general design cycle of the DRM and on the left the reasoning that occurs during this process and on the right the outputs (Takeda, 1990). This cycle can be used as a valid research technique (Vaishnavi, 2004) and serves as the outline that was followed to obtain the legal research required to complete this project.

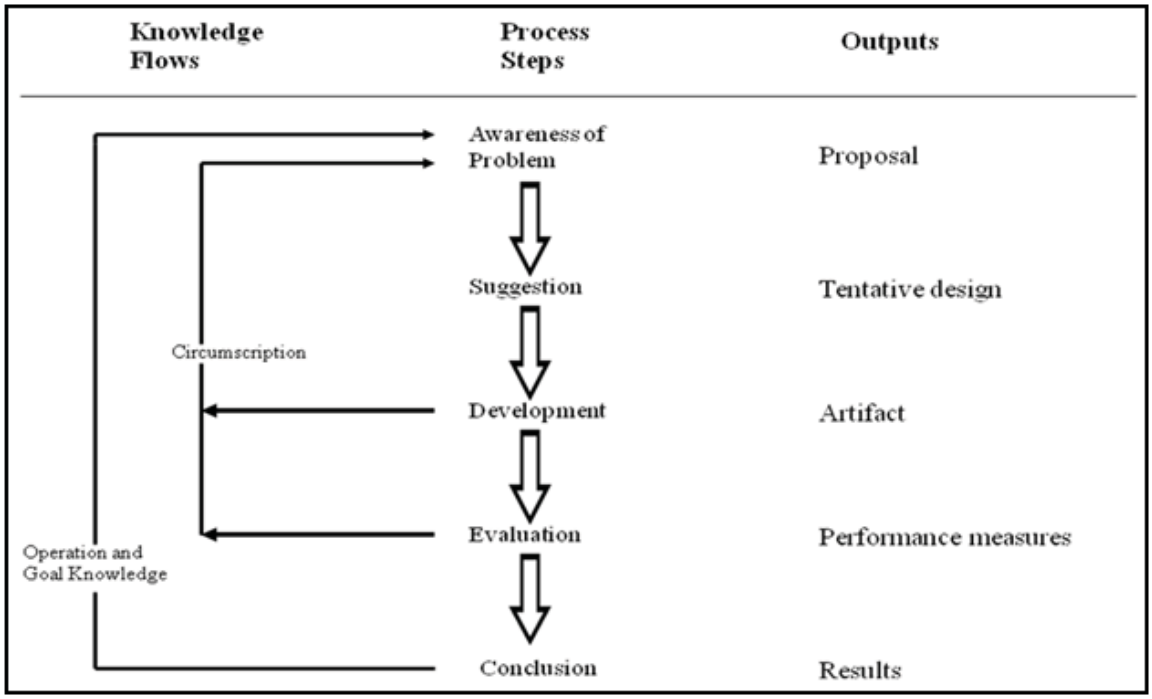


Figure 1: Design Research Cycle and Reasoning

2.5 – Design Research Methodology Applied

The first phase of this methodology is Awareness of Problem, and this was clearly identified early on in the process. With regulations such as FRCP being amended in 2006 to include email discovery, SOX auditing being an ongoing process at both companies and legal holds and discovery requests occurring on a regular basis the problem of searching and recovering the vast quantities of email data quickly and accurately was

visibly recognized. The output of this phase is a proposal, which in this case was a research proposal to better understand the legal landscape and responsibilities of the company, which was covered in the Legal Landscape section earlier in this project.

The second phase of this methodology is the Suggestion, and this works closely with the proposal and eventually the tentative design of the research. In this case the Suggestion is to do an in depth analysis of all of the regulations that are related to legal discovery and compliance for the companies, how and if they apply to the company and to what extent they apply. Although these first two stages are closely integrated it isn't until the Suggestion phase that the email archive and recovery solution, Enterprise Vault and Discovery Accelerator, is introduced into the methodology to be researched. This Suggestion was covered in the Legal Compliance section addressed earlier in this project.

The third phase of this methodology is Development, where the tentative design is implemented in this phase to result in an artifact. The artifact in this case is a research artifact, which in this case is specifically the integration of EV and DA as it relates to the legal landscape. The joining of the suggestion with the problem results in the development, in which case is specifically how Enterprise Vault and Discovery Accelerator meet the legal regulations, and more specifically, what settings specifically need to be configured in the solution to comply. This is specifically covered under the Legal Compliance and Key Archiving Consideration sections in this project.

The fourth phase of this methodology is Evaluation, which has the intended output of performance measures. In a research methodology like this one the key to this phase is to evaluate the research to ensure that it is comprehensive and then to come up with various performance measures to evaluate this research against. In this case

detailed research methods mentioned in the Literature Overview and Research section were used to make certain that the data obtained was thorough and addressed all of the legal regulations that applied to the companies. There is no absolute way to assure that all regulations were covered, but by researching this from many different resources increased the confidence that all of the primary regulations were addressed in this research. Also through the evaluation of this data against the Problem, Suggestion and Development phases of this methodology there can be a level of confidence that the research was complete.

The last phase of this methodology is the Conclusion, with the intended output of the results. With regard to the legal research this has to do with completeness and accuracy of the legal research related to Enterprise Vault and Discovery Accelerator. The Project Analysis section of this project covers many of the conclusions of how all of the research came together to capture the legal landscape, problem and solution. The end goal of this research methodology was to uncover all of the legal obligations and regulations that apply to the companies that can then be applied to the email archiving and recovery solution to determine the bigger legal compliancy question. The end result is that with regard to the legal research the Design Research Methodology is a very effective phased approach to follow to complete the research, although from the Suggestion phase through the Conclusion phase it was necessary to integrate knowledge obtained from the interview qualitative methodology regarding EV and DA product knowledge to properly complete the design research phases.

Chapter 3 – Enterprise Vault & Discovery Accelerator Configuration

The audience for this section will be the engineer or administrator responsible for doing the technical work required to deploy the product suite although many of the specific configuration parameters will be based on the business requirements previously collected. The company has purchased Enterprise Vault 2007 (Version 7.5) for Exchange and Discovery Accelerator, which will be deployed corporate wide for the company and the parent company. Enterprise Vault for Exchange will be deployed to all employees of both companies, which are approximately 1800 users. All of these users will have a desktop Outlook Client Add-In installed to access their archived email. Macintosh users will not have a desktop client; rather they will access their archived email via the links in the shortcuts created after the email is archived or by using Outlook Web Access.

There are many key settings that will be configured within Enterprise Vault and will apply to all users. This first group of settings has to do with Individual Mailbox archives and will be based on the business preferences and will not have an impact on meeting legal compliancy concerns, but is still important configuration considerations with this product suite. These settings were discussed with Symantec professional services and key management at both companies to come to a consensus on configuration options. All of the employees email for the company older than three months will be automatically archived, assuming they have been modified in the previous three months. All of the email for the parent company will be archived after six months. Calendar items and tasks are not archived for either company. Archived emails will leave shortcuts in the mailbox which will contain the first 500 characters of the body of the

email and then links to view the remaining text and any attachments. All email for the company that is over 1 month old and 2 MBs in size will be automatically archived, but this will not be done for the parent company. Retention categories, how long archived email is retained for before it is automatically deleted, will be set to 99 years for all email and journal archives until a later date, at which these will change depending on the decision made by the management team.

Employees will be provisioned based on group membership, including the use of Standard, IT, HR, Legal and Executive user groups which are defined for both companies. Each company's employees will be provisioned in separate groups due to the potential need for different retention categories; therefore there will be a total of eight groups which a user can be a member of with regard to retention settings.

Clients will be able to delete email shortcuts from their inbox after they have been archived, but the actual emails will still remain in their archive. Any email deleted by the client's mailbox, including from the deleted items folder, will not be archived, but will still remain in the journal archive. Indexing of all archives is set to "Full" to ensure successful legal discovery of all emails when required.

3.1 – Hardware

The hardware listed in Table 1 has been chosen for the production Enteprise Vault server roles of Mailbox Archive and Journal Archive. Once again Symantec professional services were consulted on these settings and specific consideration was given to meeting the long term growth of this solution, which was primarily addressed by implementing on servers that offered easy upgradeability and backend SAN storage for

data growth requirements. They will be named following the company's server naming convention.

Table 1: Server Name, Role and Hardware

Server	**Role**	**Model**	**CPU**	**RAM (GB)**
STEVAULT01	Mailbox Archive	PowerEdge 1950 Blade	2xQuad-2.3GHz	4
STEVAULT02	Journal Archive	PowerEdge 1950 Blade	2xQuad-2.3GHz	4
STEVAULTSQL01	SQL Server	PowerEdge 2950	2xQuad-2.3GHz	8

3.2 – SAN Storage Allocation and RAID

Storage allocation and raid levels are listed in Table 2. EV1 refers to STEVAULT01 and SQL1 refers to STEVAULTSQL01, etc. Note that the Indexes are stored on HP EVA 8000 Series SAN's to ensure that the expected growth of the archives will be easily addressable.

Table 2: Server and Storage Allocation and Raid Level

Partition Name	**Server Attached To:**	**Disk Configuration**	**Available Disk**
C:\ (OS)	EV1, EV2, SQ1	RAID 1	68 GB
D:\ (Application)	SQ1	RAID 1	68 GB
L:\MSSQL_LOGS (SQL DB)	SQL1	SAN	30 GB
Z:\MSSQL_DATA (SQL DB)	SQL1	SAN	30 GB
I:\EV1\Indexing (EV Index)	EV1	SAN	200 GB
V:\Enterprise Vault Stores (EV Mailbox Archives)	EV1	SAN	1200 GB
I:\Indexing (EV Index)	EV2	SAN	200 GB
V:\Enterprise Vault Stores (EV Journaling)	EV2	SAN	1750 GB

3.3 – Solution Architecture

Figure 2 outlines the two Enterprise Vault application servers, the SQL server and the flow of archive and journaling data between all of the components. Note that the failover servers and the EV FSA SharePoint Servers will be deployed at a later date.

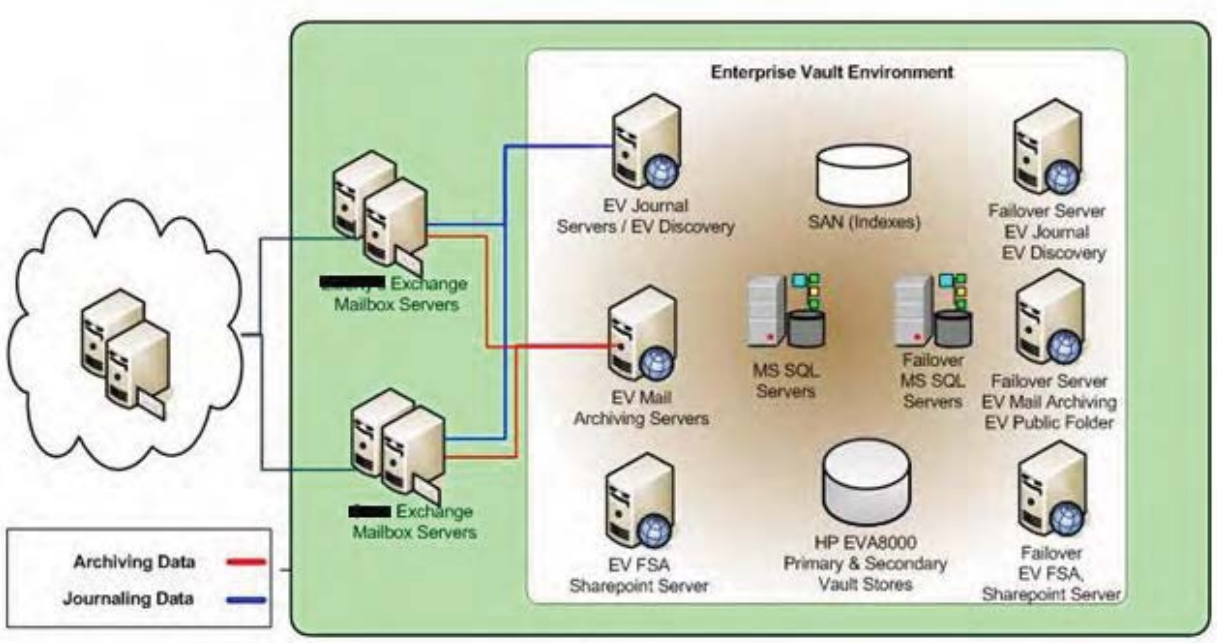


Figure 2: Flow of Archive and Journal Data

Figure 3 details the existing Exchange environment that will be archived and journaled by the Enterprise Vault solution.

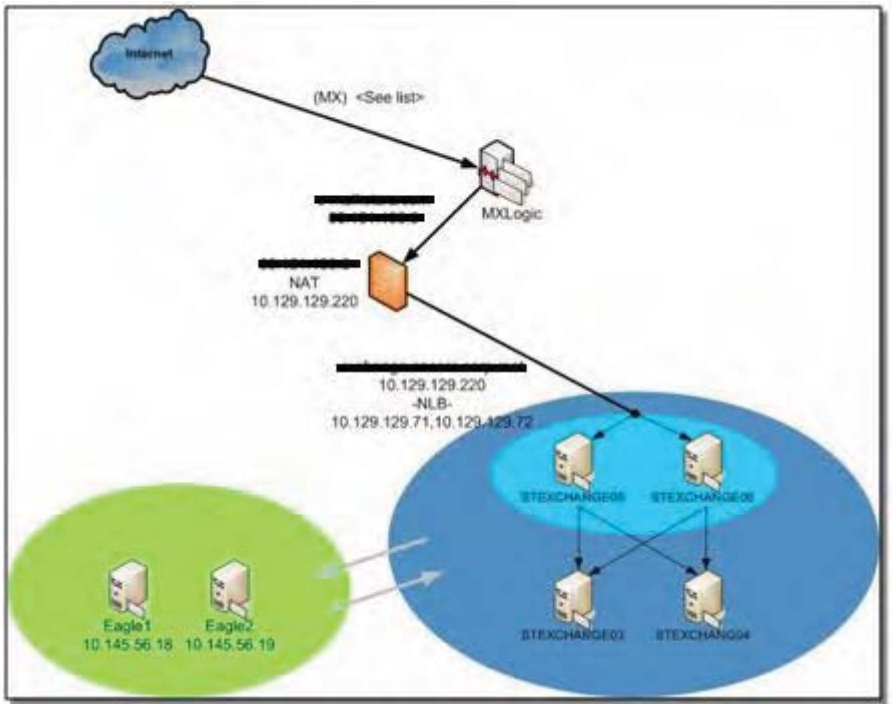


Figure 3: Exchange Environment for Both Companies

3.4 – Testing, Training and New Mailbox Activations

As with the deployment of any enterprise wide solution of this size it should be deployed in a staged process to ensure that any issues are uncovered and resolved quickly before they impact all users. Therefore the deployment of Enterprise Vault for both companies will happen in a staged process, with several pilot groups being the first deployed on the new solution and then over the course of a few weeks approximately 500 users will be enabled each week. Key to this is ensuring that everything is working as expected, so testing will be paramount to the success of the project. Also end user training is critical as some users will want to know how to make use of this new solution, but the training should not be mandatory as many users will prefer to continue to work without any interruption or responsibility to learn a new application, in particular one like Enterprise Vault which is intuitive and basically can be ignored by the end user. With each EV activation two things are going to be sent, first a detailed document walkthrough of how to use Enterprise Vault, one that must be completed by users in the pilot phase, and a new user activation email, automatically generated when their mailbox is enabled. This just explains what the new product is and what it can and will do for them. Refer to Appendix A for the test plan and to Appendix B for the new user activation email.

3.5 – Installation Prerequisites

Because of the overall reach of Enterprise Vault and Discovery Accelerator into the Exchange organization and clients on every desktop and laptop in the companies there are many prerequisites that need to be addressed prior to installing and configuring Enterprise Vault. These prerequisites include account creations, DNS updates,

preparation work on the Enterprise Vault servers, SQL Server work, virus exemptions, Exchange server extensions and forms and backups.

3.5.1 – Account Creation & DNS Updates

These steps need to be completed on all Enterprise Vault servers, which are STEVAULT01 and STEVAULT02. Create the domain accounts listed in Table 3 below with the permissions listed and all accounts should have the password set to never expire. To grant the necessary permissions to the Vault Admin account you may need to add the following registry entry on the computer you are administering exchange from: Current User > Software > Microsoft > Exchange. Add the dword value "ShowSecurityPage" with a value of "1".

Table 3: Account Creations

Domain Account	**Account Details and Permissions**
VaultAdmin	This account is used for the overall management of all of Enterprise Vault. Create a mailbox on any mail server, Full Exchange Administrator, Override the deny access on mailboxes, Local Administrator on all Exchange servers and all Enterprise Vault servers. Dbcreator role on the Enterprise Vault instance (default) on STEVAULTSQL01.
SEG_EVJournal	This mailbox has all journaling emails sent to it for the company and parent company. Create a mailbox on STEXCHANGE03 in Storage Group 1, Mailbox

	Store 1.
svc_evom	This account is used for the Enterprise Vault Operations Monitoring (EVOM) application and has specific permissions on the Enterprise Vault website. This account does not require a mailbox.
EVSystemMailbox03	This account is used for sending messages to enabled Enterprise Vault users and only needs to be on mail servers that have user mailboxes. Needs a mailbox created on STEXCHANGE03.
EVSystemMailbox04	This account is used for sending messages to enabled Enterprise Vault users and only needs to be on mail servers that have user mailboxes. Needs a mailbox created on STEXCHANGE04.
EVSysMailEag01	This account is used for sending messages to enabled Enterprise Vault users and only needs to be on mail servers that have user mailboxes. Needs a mailbox created on Eagle1.
EVSysMailEag02	This account is used for sending messages to enabled Enterprise Vault users and only needs to be on mail servers that have user mailboxes. Needs a mailbox created on Eagle2.
svc_evowa	This is the account used for Enterprise Vault to work with Outlook Web Access. It does not require a

	mailbox.

Create new Alias (CNAME) records in the domain the exchange servers reside in for “ev” pointing to STEVAULT01 (use fully qualified domain name), “evserver01” pointing to STEVAULT02 (use fully qualified domain name) and “evserver01” pointing to STEVAULT02 (use fully qualified domain name).

3.5.2 – Enterprise Vault Application Servers

There are a variety of steps to ensure that the Enterprise Vault Application servers are configured properly before deploying the application. These include installing the deployment scanner to ensure that all the prerequisites are met, configuring MSMQ services, installing Outlook 2003 and .NET Framework 2.0, completing several registry updates and ensuring the server is up to date with all patches and hotfixes. Refer to Appendix C for detailed information on this.

3.5.3 – SQL Server

The SQL server configuration has some of the same prerequisites that the Enterprise Vault servers do that need to be completed prior to the installation of the application. These steps include ensuring the proper accounts have the proper rights, installation of the SQL Server 2005 and IIS 6.0 and configuring the maintenance plan. Refer to Appendix C for detailed steps on this prerequisite.

3.5.4 – Exchange Server Extensions and Forms

A significant benefit of Enterprise Vault is that archiving individual mailboxes and journals does not require any installations on the mailbox exchange servers, which significantly reduces risks on the exchange servers, but if Outlook Web Access (OWA) is

used, which is web based access to email, and users need to be able to access and archive email with Enterprise Vault through OWA, there needs to be certain extensions and forms on the front end exchange servers and a reboot will be required. Refer to Appendix C for detailed installation instructions.

3.5.5 – Backups

As with any critical enterprise system backups must be configured, but there are specific requirements that need to be configured with regard to Enterprise Vault that is not the same with other applications. The main concern is the archive bit has to be reset because when emails are archived for an individual they turn the email into a shortcut in the specific mailbox, but it only completes this after it has verification that it has been successfully backed up, which is done after the archive bit is reset. This is a safety measure to ensure the company can roll back if necessary. Also the timing of backups are critical as there are various processes that run that you don't want run before exchange backups and system backups have completed. Refer to Appendix C for detailed information on this configuration.

3.5.6 – Virus Exemptions

As with many application servers there needs to be exemptions setup to specific directories for virus scanning otherwise it can negatively impact the performance of the application. SQL database and transaction log files by default in most virus applications are excluded, but if not be sure to exclude the mdb and log files from scanning. Also the MSMQ directories need to be excluded, which can be found by going to Computer Management > Expand Services and Applications > right click Message Queuing > Properties > Storage tab, the EV index directories, which you can find from the properties

of the Index Service > Index Locations tab, the Vault stores. This can be seen from the properties of each partition (***.dvs** files), the Windows temp folder and the temp folder under Documents and Settings for the Vault Service Account (VSA).

3.6 – Enterprise Vault Mailbox Configuration

There are two core components that need to be considered when deploying Enterprise Vault for Exchange, the Individual Mailbox Archives for each individual mailbox and the Journal Archives. Journaling is the retention of all email sent to and from all mailboxes and is not seen or managed by the end user; rather it is managed by the IT team. This data is used by Discovery Accelerator for search and retrieval functions and is essential to meeting legal compliancy requirements. The other component is the Individual Mailbox Archives, which is the storage of emails that is managed by the end user as well as controlled by the settings determined by the company. These help manage the mailbox size for the user and offer them search and retrieval capabilities that are often not used to meet key compliancy requirements by the organization. Refer to Appendix D for detailed installation and configuration information.

3.6.1 – Policy Configuration

One of the more important considerations is how the individual users are provisioned for Enterprise Vault. There are several ways to do this, but most companies do it by Active Directory groups, Organizational Units or Distribution Lists. The companies choose distribution lists as these are managed with the employee hire and termination policy and were deemed the best way to manage them by the company. Table 4 is a critical table to create for your company as it maps out all the key settings in

Enterprise Vault, including the Policies, Retention Categories and Provisioning Groups. Each of these groups will be applied to the distribution list listed to manage the users Enterprise Vault Archive settings. Each policy is linked to a retention setting to determine how long to retain the email and then linked to a provisioning group, which contains many detailed settings for archiving, and then this is linked to a group of users that will get these settings. In the table "Parent" refers to the parent company and "Company" refers to the main company. The reason it is necessary to have different groupings is it allows for different settings, most importantly email retention settings, which is a critical consideration for any company archiving email. Through the business requirement discovery process completed by each company and mentioned earlier in this thesis the companies have determined they need the ability to have different email retention settings for different classes of users, such as Legal, HR, Executive and Standard. There is also some different policies setup for employees that leave the company and laptop users, as these both have certain different settings than the other policies. Refer to Appendix D for specific details on these settings.

Table 4: Employee Provisioning

Policy	**Retention Category**	**Provisioning Group**	**Distribution List**
Parent Executive	Parent Executive	Parent Executive	DL - LMC - EVault - Executive
Parent Legal	Parent Legal	Parent Legal	DL - LMC - EVault - Legal
Parent HR	Parent HR	Parent HR	DL - LMC - EVault - HR
Parent Standard	Parent Standard	Parent Standard	DL - LMC - EVault - Standard

Company Executive	Company Executive	Company Executive	DL-SEG-EVault-Executive
Company Legal	Company Legal	Company Legal	DL-SEG-EVault-Legal
Company HR	Company HR	Company HR	DL-SEG-EVault-HR
Company Standard	Company Standard	Company Standard	DL-SEG-EVault-Company DL-SEG-EVault-Generic
Company Standard Laptop	Company Standard	Company Standard Laptop	DL-SEG-EVault-Company-Lap
Company IT	Company IT	Company IT	DL-SEG-EVault-IT
Company IT Laptop	Company IT	Company IT Laptop	DL-SEG-EVault-IT-Lap
Company ITIS	Company IT	Company ITIS	DL-SEG-EVault-IT IS
Company Zero Day	Zero Day	Company Zero Day	DL-SEG-EVault-ZeroDay

3.7 – Enterprise Vault Journal Configuration

Journaling is the retention of all email sent to and from the organization and is used to meet legal compliancy requirements for search and recovery of key email communications. Refer to Appendix E for detailed configuration of Enterprise Vault journaling.

3.7.1 – Policy Configuration

As with the configuration of Enterprise Vault Individual Archives it is vital to also have a table outlining the configuration of journaling. Table 5 below details the mailboxes, distribution lists, journal name and mailbox locations for the company and parent company. There are 4 journals for both companies to account for 4 potentially

different retention categories, once again determined during the business requirement process completed by the companies – Standard, HR, Legal and Executive. Note that users must be placed in the appropriate mailbox stores based on their position in the company since journaling is only as granular as the store level and this can present a challenge for many organizations if their mailboxes were not setup like this originally. Refer to Appendix E for detailed installation and configuration information.

Table 5: Journal Provisioning

Distribution List	**Mailbox**	**Location**	**Journal – Vault Store**
DL – LMC – Journal – Standard	EV-LMC-STD-Journal	EAGLE1 > Second Storage Group > Journal Store	PARstandardJournal
DL – LMC – Journal – Executive	EV-LMC-EXEC-Journal	EAGLE1 > Second Storage Group > Journal Store	PARexecutiveJournal
DL – LMC – Journal – Legal	EV-LMC-LEG-Journal	EAGLE1 > Second Storage Group > Journal Store	PARlegalJournal
DL – LMC – Journal – HR	EV-LMC-HR-Journal	EAGLE1 > Second Storage Group > Journal Store	PARhrJournal
DL-SEG-Journal-Standard	EV-SEG-STD-Journal	STEXCHANGE03 > Storage Group 1 > Mailbox Store 1	SEGstandardJournal
DL-SEG-Journal-Executive	EV-SEG-EXEC-Journal	STEXCHANGE03 > Storage Group 1 > Mailbox Store 1	SEGexecutiveJournal
DL-SEG-Journal-Legal	EV-SEG-LEG-Journal	STEXCHANGE03 > Storage Group 1 > Mailbox Store 1	SEGlegalJournal
DL-SEG-Journal-HR	EV-SEG-HR-Journal	STEXCHANGE03 > Storage Group 1 > Mailbox Store 1	SEGhrJournal

3.8 – Enterprise Vault Reporting and Operations Monitor

Enterprise Vault plays a vital role in the organization and therefore it is critical that you are able to run various reports and actively monitor the solution. This functionality is built into the application. Refer to appendix F for detailed instructions on how to install and configure this.

3.9 – Discovery Accelerator Configuration

Discovery Accelerator is the discovery and review component that integrates tightly with Enterprise Vault to enable the quick discovery and review of email data archived by Enterprise Vault to meet various needs at the company, most of which are related to legal and HR. It is also the key component that allows the company to quickly discover search terms from millions of email records to meet many of the existing federal regulations for electronic discovery. Refer to Appendix G for detailed installation and configuration steps on how to do this.

3.10 – Discovery Accelerator Searches

Without the ability to search the archived data quickly, accurately and effectively the solution is virtually worthless, especially from a legal compliancy perspective. Therefore it is critical to have a well documented search and recovery process for recovering archived email. One of the most important, and most easily confused, is making sure the right journal archives are selected when processing a search, since if the data is in different archives like it is for these companies the right archives have to be selected or the search will not be accurate. Also it is important to note that the individual email archives can be searched as well, but remember that this data is most likely not complete as it is only archiving email older than a certain age in a users mailbox, and email deleted prior to that age is not archived unless the user manually did that. Also if

the email was deleted before it reached the archive age limit the email would not exist in the individual email archive. Therefore if it is being searched to meet legal obligations the data will be incomplete and very likely the search would not meet legal requirements. Refer to Appendix H for a detailed test plan on how to search and review archived email.

3.11 – Day to Day Administration and Troubleshooting

Enterprise Vault requires specific day to day administration and troubleshooting to ensure the stability and functionality of all archiving, as well there are many requirements that end users request on a regular basis. These include things like generating a report of all Enterprise Vault settings, enabling mailboxes for Enterprise Vault, granting access to other archives, restoring archives back to mailboxes, importing or exporting PST's, troubleshooting common client issues and mailbox activations, rebuilding indexes for archives, daily, weekly and monthly tasks and a detailed FAQ for the help desk. All of these detailed guides can be found in Appendix I.

Chapter 4 – Project Analysis

This project touched on two specific areas, both of which can be broadened quite a bit to reach into many other related areas. Email archiving, search and retrieval, and specifically Enterprise Vault and Discovery Accelerator, is one of many solutions that can be implemented to address these needs, each with their own strengths and weaknesses. The more recent impact of legal regulations on email and discovery are a significant driving force for companies implementing email archiving and recovery solutions, but the regulations reach far beyond what email archiving and recovery can address. This project is specific to the Enterprise Vault email archiving and recovery solution and how it specifically addresses many of the legal regulations organizations are faced with today.

4.1 – What Went Right

Overall the project was very successful based on a variety of criteria. The main goal of implementing Enterprise Vault and Discovery Accelerator while addressing legal regulations for both companies was completed successfully and the deployment was virtually transparent to the end users. One interesting observation was that even though new functionality was introduced on the Outlook client for all users, including new icons on the toolbar, a far majority of them didn't even notice that Enterprise Vault archiving had been deployed on their mailboxes. They received notification of their mailbox activation and optional training on how to use it, but most choose to not do the training and were pleased that they could use the solution if they wanted to, but also could continue to work normally without any impact. Many users stated that the deployment was seamless and even email that was archived automatically after three months was able

to be retrieved so easily that they didn't even notice they were accessing it from Enterprise Vault instead of their mailbox. Therefore the perception from the user population was very positive, as some users found it very beneficial to have the extra mailbox space and search capabilities, while others were happy they could continue to do their job without impact.

The most important criteria of being able to quickly and accurately search all email data and turnover results to legal counsel was the most successful portion of this project. Since the deployment numerous tests have been completed to validate the functionality and several incidents have occurred where searching all email was required, some of which required a very short turnaround time for results. Each time the team was able to search email across the respective company for the required time frame and accurately return results that could be reviewed by legal counsel. The staff hours saved by optimizing this functionality is in the hundreds, and as more searches are required the return on this investment will be realized quickly.

The other thing that was done right with this project was the deployment approach, especially with regard to the detailed testing and training that was completed and the phased approach to the project. Testing and training uncovered many issues and questions that the project team was able to address and answer before deploying to the rest of the employees not in the pilot phase, so when the same questions were presented the team was able to quickly address them. The project team was also able to make relevant changes to the configuration when necessary, which avoided issues in production.

4.2 – What Went Wrong

There were various things that went wrong with this project, but as with any project of this magnitude certain last minute challenges are expected and it is how the IT staff is able to effectively respond to and resolve them that differentiates how successful the deployment is in the end. One of the main issues was related to the project timeline, and unfortunately this deployment, like most Information Technology projects, was not completed within the original timeline defined. Although it is relevant to mention that management was not concerned with this and in fact decided to slow down the implementation to ensure we properly uncovered any issues. In the end the delay was about three weeks, so the impact was negligible as there were no pending search and recovery requests and there were no projects that were pushed back due to the project timeline extending.

There were several things that were uncovered in this project that accounted for the delay in the project completion, with the biggest one being related to the organization of mailboxes in the Exchange mailbox stores. This was a configuration requirement that was not clearly identified by Symantec professional services when we gave them our business requirements and ended up requiring the business to take a delay in the deployment to re-architect the layout of all the mailboxes for both companies. The issue was the businesses required that all journaled email have separate retention settings for different user groups, being Executives, Legal, HR, and Standard, and a limitation in Enterprise Vault is that it can only have different retention settings as granular as Exchange 2003 journaling can get, so if a separate retention setting was needed for two separate groups than those mailboxes had to be in two separate mailbox stores in exchange. The original configuration of mailboxes at these companies did not account

for this and even though the requirements were established before the deployment it wasn't until halfway through the rollout that this was uncovered, which meant we had to postpone some work to schedule an outage to move over one hundred mailboxes to different mailbox stores. The end configuration resulted in all Executive, Legal, HR and Standard users being identified and put in separate mailbox stores in Exchange and a process being put in place to ensure all new and/or promoted employees are placed or moved into the correct information store.

The most visible and concerning thing that went wrong occurred several weeks after Enterprise Vault and Discovery Accelerator was deployed for both companies. There was a substantial failure in journaling which resulted in a significant loss of data for some of the journaled data for the company, although the parent company was not affected by this failure. When the journal mailboxes were setup they automatically inherited the default mailbox size of 250 MB and this configuration was never changed, or recommended to be changed by professional services that assisted in the deployment of this solution. About two weeks after Enterprise Vault was deployed for journaling two of the five journals for the company stopped journaling email and ceased to journal for three weeks until a ticket by an employee was opened for a recovery request which prompted us to review one of the archives that was no longer journaling. What occurred is journaling will let email queue up in the journal mailbox based on the number, size and frequency of email received over a given time period and at one point two weeks after implementation two of the journal mailboxes reached their limit and the mailboxes both stopped receiving email. There were no checks in place recommended by professional services to catch this and their reporting tool did not display this data as well, so it was

roughly three weeks later until this ticket was opened in which questionable results prompted us to look closely at what was occurring, at which time we identified the issue. We later found out that professional services were supposed to ensure that all mailbox quotas were turned off during setup. The end result was we had to document that we had missing data for those two journals for that time period, communicate this data with management, and deploy a new daily check to ensure that the journals were being updated on a daily basis to prevent this from happening again.

There was another lesson learned with Outlook Web Access (OWA) configuration and integration with Enterprise Vault, which was once again completed through guidance by professional services from Symantec. OWA integrates with Enterprise Vault so all archived email in personal inboxes can be recovered through web based access to email, but the testing was not completed thoroughly and several pieces of functionality were missing from the web based client. A ticket was opened with Symantec and we discovered several missing configuration parameters which resolved our issues. Because email isn't archived automatically for three months most users did not even need this functionality yet, so it ended up being a minor issue that was resolved quickly, but once again should not have occurred in the first place had the test plan been completed properly.

Another challenge that was identified during the pilot testing and caused intermittent issues throughout the deployment and early phases of production release had to do with conflicts between the Enterprise Vault Snap-In, Exchange System Manager tools and Outlook 2007. There is an issue when the three of these applications are installed on the same computer which renders the Enterprise Vault Snap-In unable to

function. Unfortunately Symantec had very little documentation on this issue and it wasn't until three months after the solution was deployed that there was a consistent work around to resolve the issue, but there was a more tedious work around that we deployed that resolved it. Given the applications installed to cause the conflict it only affected IT staff, since no one outside of IT had the Exchange System Manager tools installed, so we were able to work directly with those impacted to resolve the conflict.

Another project oversight had to do with Macintosh clients. It was not clear at the start of this project that there were over fifty Macintosh clients at a remote office that would also be on Enterprise Vault. Enterprise Vault is limited with its integration to Macintosh clients, and their email client, Entourage, does not have a Snap-In to allow it work the same way as the Outlook client, but all of the shortcuts for archived email have a link to pull up the email in a browser. The issue with this is Enterprise Vault is not compatible with Firefox or Safari, so if they didn't have Internet Explorer installed they could not access their archived email. In the end these users were not very happy with the solution, but several workarounds were made available to them.

The last issue was minor and had to do with the sizing of the LUNs for the journal volumes. We gave Symantec professional services complete data on the amount of email sent and received by the companies on a daily basis and they took that data and advised us on the space to allocate to meet our storage requirements for two years, but after three months it became clear we would run out of space within only six months. This was easily resolved by allocating more storage on the SAN to the journal server and extending the volume.

4.3 Summary

Overall the project was considered a success, but there were definitely some issues that could have been avoided. The main issues that came up were in fact the result of not getting proper guidance from professional services and these issues were communicated back to the vendor as recommendations for future implementations. Clearly the most unacceptable problem was the missing journal data, but from a conversation with another peer that recently deployed Enterprise Vault he was clearly told to turn off mailbox limits for journal mailboxes so it appears that consulting does usually address this issue.

Chapter 5 – Lessons Learned and Next Evolution of the Project

The overall process of writing this research paper and the integration of addressing legal compliancy concerns with an email archiving and retrieval solution has served as the establishment of a solid foundation on which to build upon. The solution covered addresses some key compliancy concerns for the companies, but alone does not meet all the regulations and business requirements that they must abide by. Through this process there were many valuable lessons learned that can be applied to the future evolution of this project and other related projects that will address the vastly growing and changing legal landscape for electronic discovery.

5.1 What was learned from the project experience?

There were many things that I learned from the deployment of Enterprise Vault and Discovery Accelerator to address many Federal regulations. On the top of this list was the fact that this project offered a fantastic opportunity to learn how to properly deploy and document an Enterprise Information Technology solution and the added value gained by deploying a solution with such attention to all of the details throughout all of the stages of the project. An example that exemplifies this is when the missing journal archive issue was uncovered almost two months after the deployment and a call was opened with Symantec support the cause was not readily identified and they started to advise me that I had to make what appeared to be some significant configuration changes stating they should of already been set when we originally configured the application. I assured them that was not the case but they persisted, at which time I was able to send them the detailed configuration documentation and screenshots illustrating to them otherwise. I stated I would be willing to make the changes, but that I would be

communicating this back to their consultant asking why this was not setup right. At that point they decided not to have those changes made and we explored the issue further, which is when we found out that the root cause was not related to that configuration. On other projects that documentation would most likely not have been available and changes might have been made that would have negatively impacted the solution, so the value of having this documentation was clearly demonstrated in this example. Also since the deployment there have been several times where I was out of the office and the documentation was concise enough that peers were able to refer to it instead of contacting me while I was out.

Another key lesson learned from this project was some of the benefits and tradeoffs of working with professional services to assist in the deployment of a new solution, especially one that interfaces with the exchange organization and installs a client on every desktop and laptop. The benefits are significant as you bring in knowledge from dozens to hundreds of installations and are able to tap into that knowledge base to make sure everything is deployed properly. The trade off is that often the engineer in charge at the company isn't given substantial time for research, preparation and testing of the solution, yet still is expected to ensure the successful deployment of the solution. The challenge is trying to have enough product knowledge to ensure that things are done properly while still trusting the consultants' knowledge and capability of ensuring this is successfully deployed. My experience included several issues that came up from days to months later and as much as I can say that we were not properly consulted on certain configurations I am still in the end responsible and accountable for the solution deployed. This reinforces the need to approach Enterprise

projects of this magnitude with the same attention to detail regardless of the involvement of professional services so you can limit the number of issues that may come up later on.

Another lesson learned from this project experience was the importance of the documentation that was covered in the introduction of this paper. If you are able to succinctly identify the problem, the existing situation, the legal landscape and implications, the key goals and the barriers to success for an upcoming project you will clearly lay out a foundation for success in the deployment of it. Too often IT organizations are reactive rather that proactive and approaching new projects like this are often disregarded due to time constraints, poor leadership and/or inexperienced engineers. Whereas if a proactive approach was taken to new deployments many questions would be asked and answered before they resulted in a high visibility issue.

The last lesson learned to me is obvious, but can't go without stating. The information contained in the lessons learned section is critical to this process and is a necessity for the engineer and organization to learn from their experiences. Without evaluating what was done right and wrong, what lessons were learned and what would have been done differently it is not only difficult to grow and learn from your mistakes, but hard to clearly see and appreciate everything that was done right.

5.2 What would have been done differently?

There are several things that would have been done differently with regard to this project, many of which have been touched upon in the earlier sections. The most obvious one would have been to ensure there were checks in place to make sure I could quickly identify if there were issues with emails being properly journaled. Given the significance of journaling and the ability to search these archives it seems logical that

there should have been some check put in place to ensure that the journals are functioning properly on a daily basis, but there was none recommended. After the issue occurred we developed our own check against the SQL database to ensure this, but in retrospect clearly this would have been done in advance so at most we would have lost a day or two of journal archives rather than three weeks.

The other thing that should have been handled differently is the issue with the Macintosh clients. Unfortunately this was not clearly identified as a business requirement and even though the vendor was made aware of some Macintosh clients they gave us no information as to the extent that these clients are limited from interacting with Enterprise Vault for almost all the functionality that an Outlook client on Windows XP can. The importance of accurate and complete business requirements prior to project deployment cannot be understated for any project.

Overall the project went very well and I would have not done anything else differently. Almost all the main issues that came up were all technical oversights or, in my opinion, details that were not covered with us by professional services that should have been. So I certainly would of liked to have seen that handled differently, but I also believe that it is status quo to have various things like we experienced come up in projects of this magnitude and it is how you overcome and resolve those unexpected issues that arise that separate the successful projects from the unsuccessful ones.

5.3 Did the project meet initial expectations?

The initial expectation of the project was to deploy an email archive and discovery solution that would allow both companies the ability to quickly and effectively search all email data for key criteria established by legal counsel. Although Enterprise

Vault offered many ancillary benefits, these were not of primary concern to the companies and therefore were not considered with regard to initial expectations. As a result the expectation was met as this solution not only offered this core capability, but offered everything and more that the legal team was hoping for with regard to searching archived email data and thereby addressing many legal compliancy concerns. The initial tests completed for the legal teams were met with resounding approval and a realization that significant amounts of money will be saved in not only the retrieval of the relevant email data, but also in the costs with external counsel reviewing this data. This is due to the search results containing exactly what was requested, rather than with previous searches containing duplicate and irrelevant data because of search and recovery limitations. The one issue that occurred shortly after deployment did not garner a lot of attention because it was limited to only two journals for the primary company, and did not affect the parent company which was the biggest proponent of implementing this solution.

5.4 If the project continued what would be the next stages?

The initial deployment of Enterprise Vault and Discovery Accelerator for Exchange is really just the beginning stage for this solution as there are other planned rollouts and extensions of this product suite and functionality that will be completed once the business is satisfied that this product meets all of the company's initial needs and is reliable. The first step will be to deploy this for public folders, which are shared folders, mailboxes, calendars, etc. that are stored in exchange that have customizable permissions, but as of right now the business did not want to enable this for the public folders since they are not used extensively. So there is still some indecision on whether that will be

completed. The key thing to consider with this rollout is that all public folders will be stored as a single archive, which means the retention setting has to be the same for all folders, you cannot limit searches to specific folders and if you grant access to this archive you are granting access to every public folder rather than just to specific ones.

Additional functionality of the application not implemented yet has to do with reporting and PST migration. There are some very valuable data analysis and operational reports that can be run and would be valuable to management so there has been some discussion to generating some new monthly reports. The most significant, and a bit of an overwhelming undertaking, is PST migration. A PST is a personal file folder that is often used to store email that a user moves from their Exchange mailbox to make sure they don't go over their mailbox quota or to save long-term outside of their main email inbox. Many organizations, like the two covered in this project, use PST's extensively. With Enterprise Vault you can automatically have all data from the PST's imported into the individual mailbox archives and then disallow the use of PST's. This is ideal to do, especially when considering compliancy issues and search and retrieval of old email, but it also is a very political and complex issue since they are used extensively. One issue for example is if you import all the email from the PST's it could end up putting them significantly over their mailbox quota, and if the company has a retention setting for example of 1 year, where email older than 1 year is automatically deleted, then it is possible that all of the email will be imported and then immediately deleted, depending on the age of the email being imported. The planning and end user training and communication will be extensive for the company to successfully take on this challenge.

Licenses for Enterprise Vault for SharePoint and File Server were also purchased with this solution, although the timeline for the rollout of these solutions is still not determined. Both of these solutions will take extensive planning and user training as it will also create shortcuts for all documents over the predetermined age range, which is something that users have a hard time accepting. Regardless the integration of these solutions is essential to the long-term plans for both companies as they want an end to end document retention compliancy and search and recovery solution and this will be a core part of the overall solution.

The initial rollout of Discovery Accelerator made use of the basic functionality of the solution, but it has significant more functionality that has not been utilized yet. Discovery Accelerator offers some excellent tools in allowing legal counsel to individually access and review every email returned in the search and mark it as relevant or not, which would expedite the time legal counsel currently spends reviewing the email, but currently all of that work is outsourced to external legal teams so to set this up we would need to add it to our Citrix environment and get a variety of approvals and licenses to complete this. Clearly there are many steps that the companies want to take as they move forward with integrating this solution in more of their data sets, but as with Enterprise Vault and Discovery Accelerator they need to be properly tested and deployed.

5.5 Project Summary

IDC estimates that worldwide email correspondence has increased from 9.7 billion messages a day in 2000 to roughly 35 billion a day in 2005, and Gartner Group estimates that corporate mailboxes are increasing by 40% year over year. Given these estimates it is obvious that the role email plays in business is continuing to grow

considerably, so it is no surprise that organizations are looking for ways to manage this vast amount of email data internally so they can meet all the various regulations regarding legal discovery. Enterprise Vault and Discovery Accelerator is a leader in the email archiving and discovery market and was the product suite chosen by the companies to be deployed to address their business requirements.

Although the implementation of an email archiving and recovery solution over time can easily pay for itself in the savings of time and resources to complete what otherwise would be very a complex manual search and recovery of email data, it also needs to be carefully planned and tested before it is deployed in production. The deployment discussed in this research paper was complex due to several factors, but the main reason being that it interfaced with the Exchange email organization, one of the most important business applications for the companies, and it installed a client on every laptop and desktop at both organizations. Therefore its reach was all encompassing, so an issue with the way it interfaced with exchange or an issue with the installation on users computers could result in a significant impact to the businesses. Regardless as long as it is properly tested, documented and deployed in a phased approach the solution will not only be seamless to the end users but will offer the businesses a huge advantage in responding to legal requests that are virtually inevitable given the nature of their business.

The legal regulations were a significant driving force for the companies implementing EV and DA as this solution addressed many requirements that are outlined in Sarbanes-Oxley, Gramm-Leach-Bliley and the Federal Rules of Civil Procedure. The American Management Association estimates that 24% of companies have experienced their employees' email being subpoenaed and 15% have gone to court because of

lawsuits brought on by their employees' email. The risks of not being able to quickly search and recover your email represent not only a significant threat to losing lawsuits, but puts the companies at risk of being penalized by the government for not complying to Federal regulations.

Since the deployment of Enterprise Vault and Discovery Accelerator for both companies there have been two official legal counsel requests for the primary company and three official legal counsel requests for the parent company. All of these requests were completed within several business days, and in one case a few hours, of the search terms being received and all resulted in an accurate data set that was able to be easily distributed to legal counsel for review. Prior to this implementation these requests would have been tedious and at times not even possible, resulting in responses back to legal counsel advising them on what data we could give them and what data we could not give them with full confidence that it was complete or accurate.

Clearly the benefits of deploying a solution like Enterprise Vault and Discovery Accelerator are far greater than the costs and risks of trying to manage this with standard backup and recovery software. This research paper clarifies many of the areas that engineers and project managers will need to focus on to ensure that this is successfully implemented and addresses the organizations legal liabilities. In conclusion I think it is best to summarize with an issue brought to attention by Stephen McDevitt, an official in the presidential CIO office. This is in relation to missing White House emails that received national attention over the first two quarters of 2008. He stated he "told the committee that a new email archiving system that would have addressed the problems" and it was planning to go live in 2006. He concluded by saying, "CIO Theresa Payton

canceled the new system in 2006, because it would have required modifications and additional spending.", but it is clear that this spending would have been offset by avoiding such negative press and potential legal liability (Yost, 2008). I believe I demonstrated clearly in this project the costs and modifications required to implement email archiving and recovery are not to be overlooked, but the risk of not doing so can be as vast as is the case with our own government and therefore cannot be overlooked or undervalued.

References

Osterman Research, Inc. (2003). *Enterprise Email Archiving: Market Problems, Needs and Trends.* Retrieved August 4th, 2008 from http://www.researchandmarkets.com/reportinfo.asp?report_id=220572

Cascarino, Richard. (2007). *AUDITOR'S Guide to Information Systems Auditing*. John Wiley & Sons, Inc.

Overly, Michael R. (2006). *Email Compliance Quick Reference Guide. Strategies for Regulatory Compliance and Legal Risk Management.* Retrieved August 7th from http://www.ironport.com/pdf/ironport_email_compliance_guide.pdf

Kvale, Steinar. (1996). *Interviews. An Introduction to Qualitative Research Interviewing.* Sage Publications Inc.

Athena Archiver. (2006). *Gramm-Leach Bliley Act (GLBA).* Retrieved August 12th, 2008 from http://www.athenaarchiver.com/downloads/pdfs/compliance/banking-glba/aa-compliance-banking-888.pdf

Athena Archiver. (2006). *Sarbanes-Oxley Act (SOX).* Retrieved August 12th, 2008 from http://www.athenaarchiver.com/downloads/pdfs/compliance/accounting-sarbanes-oxley/aa-compliance_sarbanes-oxley-888.pdf

Athena Archiver. (2006). *Healthcare and Medical (HIPAA).* Retrieved August 12th, 2008 from http://www.athenaarchiver.com/downloads/pdfs/compliance/healthcare-hipaa/aa-compliance-hipaa-888.pdf

The Committee on the Judiciary House of Representatives. (2005). *Federal Rules of Civil Procedure with Forms.* Washington, DC: Author

One Hundred Seventh Congress of the United States of America. (2002). *Sarbanes-Oxley Act of 2002.* (H.R. 3763). Washington, DC: Author.

Osterman Research, Inc. (2004). *Email Archiving Market Trends, 2004-2007.* Retrieved August 4th, 2008 from http://www.researchandmarkets.com/reportinfo.asp?report_id=220417

Jason Park and Litigation Solution. (2002). *PST…what's in that file?* Retrieved August 2nd, 2008 from http://www.lsilegal.com/misc/pst.htm

Vaishnavi K., Vijay K. Vaishnavi, William Kuechler, Jr. (2007). *Design Science Research Methods and Patterns: Innovating Information and Communication Technology.* CRC Press.

Senqupta, David. (2005). *What is an Exchange brick-level backup?* SearchExchange.com. Retrieved August 1st, 2008 from http://searchexchange.techtarget.com/expert/KnowledgebaseAnswer/0,289625,sid43_gci1104242,00.html

March, Hevner, A., Park, S., and Ram, J. (2004). Design Science in Information Systems Research. *MIS Quarterly*. 28(1): 75-105.

U.S. Senate Committee on Banking, Housing, and Urban Affairs. (2008). *Gramm-Leach-Bliley Summary of Provisions.* Retrieved August 13th, 2008 from http://banking.senate.gov/conf/grmleach.htm

Neuburger, Jeff. (2007). *Legal Landscape.* ExpertBusinessSource.com. Retrieved August 2nd, 2008 from http://www.expertbusinesssource.com/blog/720000272/post/1900010190.html

Lexis Nexis® (2007) Federal Rules of Civil Procedure. LexisNexis, a division of Reed Elsevier Inc. Retrieved August 12th, 2008 from http://www.lexisnexis.com/lawschool/learning/reference/pdf/2006/LA119090_FRCP.pdf

Takeda, H., Veerkamp, P., Tomiyama, T., Yoshikawafm, H. (1990). Modeling Design Processes. *AI MagazineWinter*: 37-48.

Vaishnavi, V. and Kuechler, W. (2004/5). *Design Research in Information Systems.* Association for Information Systems. Retrieved August 5th, 2008 from http://www.isworld.org/Researchdesign/drisISworld.htm

Undocumented Author. SearchExchange.com. (2008). *An IT Manager's Guide to Email and File Archiving.* Retrieved August 10th, 2008 from http://searchexchange.bitpipe.com/data/document.do;jsessionid=078FBACE6DEBB42BA086EB7308398730?res_id=1216919042_158&src=DED_sxch_07_30_08

Evans, J. Litigation gold mine: Email messages can contain explosive discovery material. LA Daily Journal (Nov. 29, 1995), 1.

Computer Business Review. (2008). *KVS Info.* Retrieved August 5th, 2008 from http://www.cbronline.com/storefronts_detail.asp?co=KVS_Info&z=\

Jaqott, Siegfried. (2008). A Few Regulations Relevant to Journaling. *WindowsITPro.* Retrieved August 12th, 2008 from http://windowsitpro.com/article/articleid/98504/a-few-regulations-relevant-to-journaling.html

Wall Street & Technology. (2006). *Warning! Failure is Imminent.* Retrieved October 31st, 2008 from http://www.wallstreetandtech.com/news/operations/showArticle.jhtml?articleID=193401728

LiveOffice LLC. (2008). *FRCP Regulations*. Retrieved August 8th, 2008 from http://www.liveoffice.com/regulations/frcp.asp

Ferris Research. (2008). *Business Email System Pentetration Varies Greatly by Customer Size, Industry and More, Says Ferris Research.* Retrieved November 1st from http://software.tekrati.com/research/10045/

Morrison & Foerster, LLP. (2001). *Electronic Discovery and Evidence: Safeguarding Against Misuse of Technology in the Workplace.* Retrieved October 26th from http://www.mofo.com/news/updates/bulletins/bulletin75.html

FaceTime. (2008). *Meeting e-Discovery Requirements*. Retrieved August 8th, 2008 from http://www.facetime.com/solutions/ediscovery.aspx

Osterman Research, Inc. (2008). *A Guide to Message Archiving.* Retrieved August 12th, 2008 from http://viewer.bitpipe.com/viewer/viewDocument.do?accessId=7996232

Grote, Mark. (2005). *Implementing Exchange 2003 Message Journaling.* MSExchange.org. Retrieved July 24th, 2008 from http://www.msexchange.org/tutorials/Implementing-Exchange-2003-Message-Journaling.html

Yost, Pete. (2008). Why Was All the E-Mail Missing From Cheney's Office on Key Dates in CIA Leak Probe? *The Associated Press.* Retrieved July 27th, 2008 from http://www.law.com/jsp/article.jsp?id=1204113031721

Undocumented Author: Bocada (2006). *How to "ACE" Your Next SOX Audit: Eight Steps to Straight A's.* Retrieved from http://www.bocada.com/download/Acing%20SOX%20Audits.pdf

Undocumented Author. SoftLanding.com (2006). *The IT Manager's Working Guide to Sustainable SOX Compliance.* Retrieved August 7th, 2008 from http://www.softlanding.com/downloads/index.htm#SOX

Undocumented Author. SearchExchange.com (2008). *Chapter 3 – Litigation Holds: How Windows Shops Can Reduce with a Successful Litigation Hold Process.* Retrieved July 26th, 2008 from http://searchexchange.bitpipe.com/data/document.do;jsessionid=4A0580819FB9989024AAF8759CB8352B?res_id=1212860325_327&src=DED_sxch_08_01_08

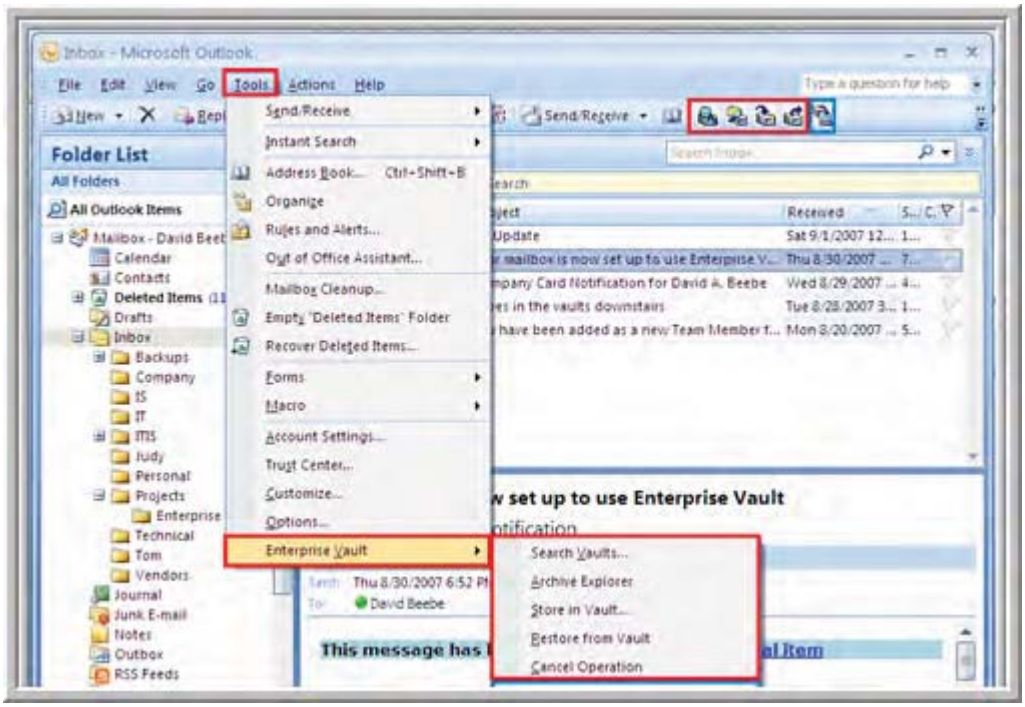
Undocumented Author. SearchCIO.com. (2007). *Email Archiving Strategies for CIOs.* Retrieved July 27th, 2008 from http://searchcio.techtarget.com/generic/0,295582,sid182_gci1238426,00.html

Appendix A

Client Side Overview/Test Plan of Enterprise Vault

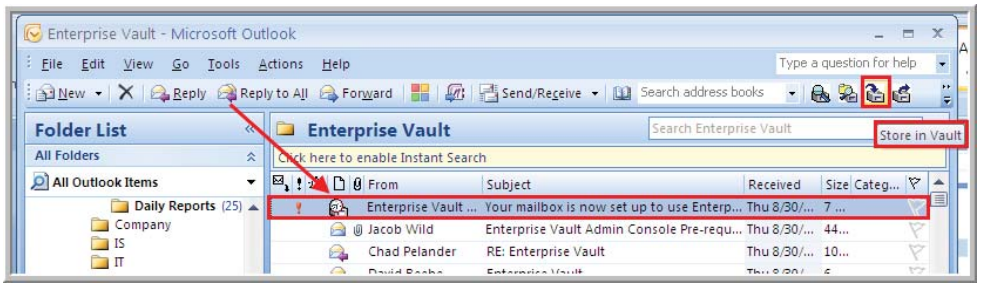
Prior to Enterprise wide deployment of Enterprise Vault there will be a pilot group that will step through the following tests to ensure the overall functionality of the new Email Archive solution. When your mailbox was enabled for Enterprise Vault you should receive a welcome email informing you that your mailbox was archive enabled.

After this email is received close and re-open Outlook and confirm that you have the new toolbar icons and menu options as pictured below in red. If you have a laptop you should also see the options boxed in blue for Offline Vault, if not it may be necessary to contact the help desk to have this feature enabled.



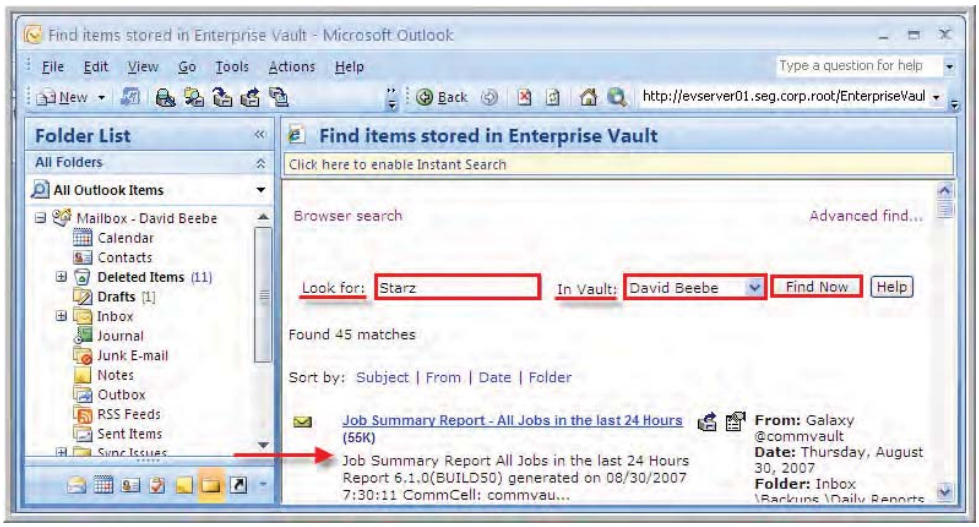
Highlight an email and click on the "**Store in Vault**" button in the upper right of Outlook and then click OK when prompted. You should see the icon next to the email

change to an Enterprise Vault icon (see red arrow in screenshot). Note that when you manually archive an email it will archive immediately, but it will not change to a "shortcut" in your mailbox until the nightly archive process runs, after which you will only see the first 500 characters of the body of the email as well as a link for any attachments. Until this nightly process runs after your mailbox has been enabled you will not have any email archived unless you manually select it to archive. Also remember that only email over 3 months will automatically archive each evening for the company and 6 months for the parent company.

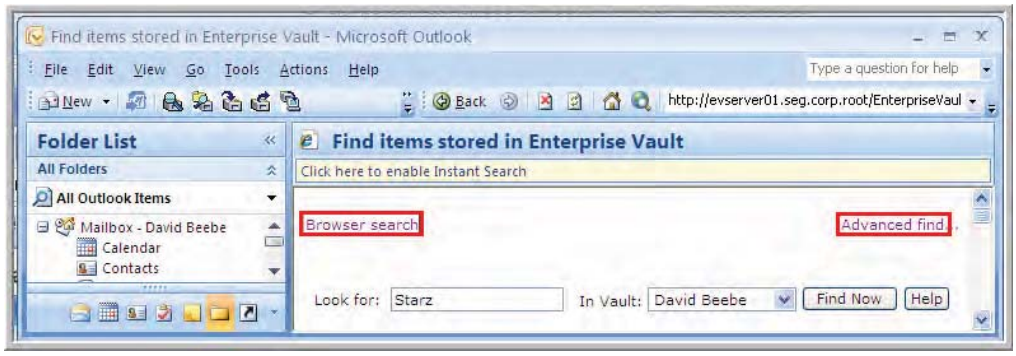


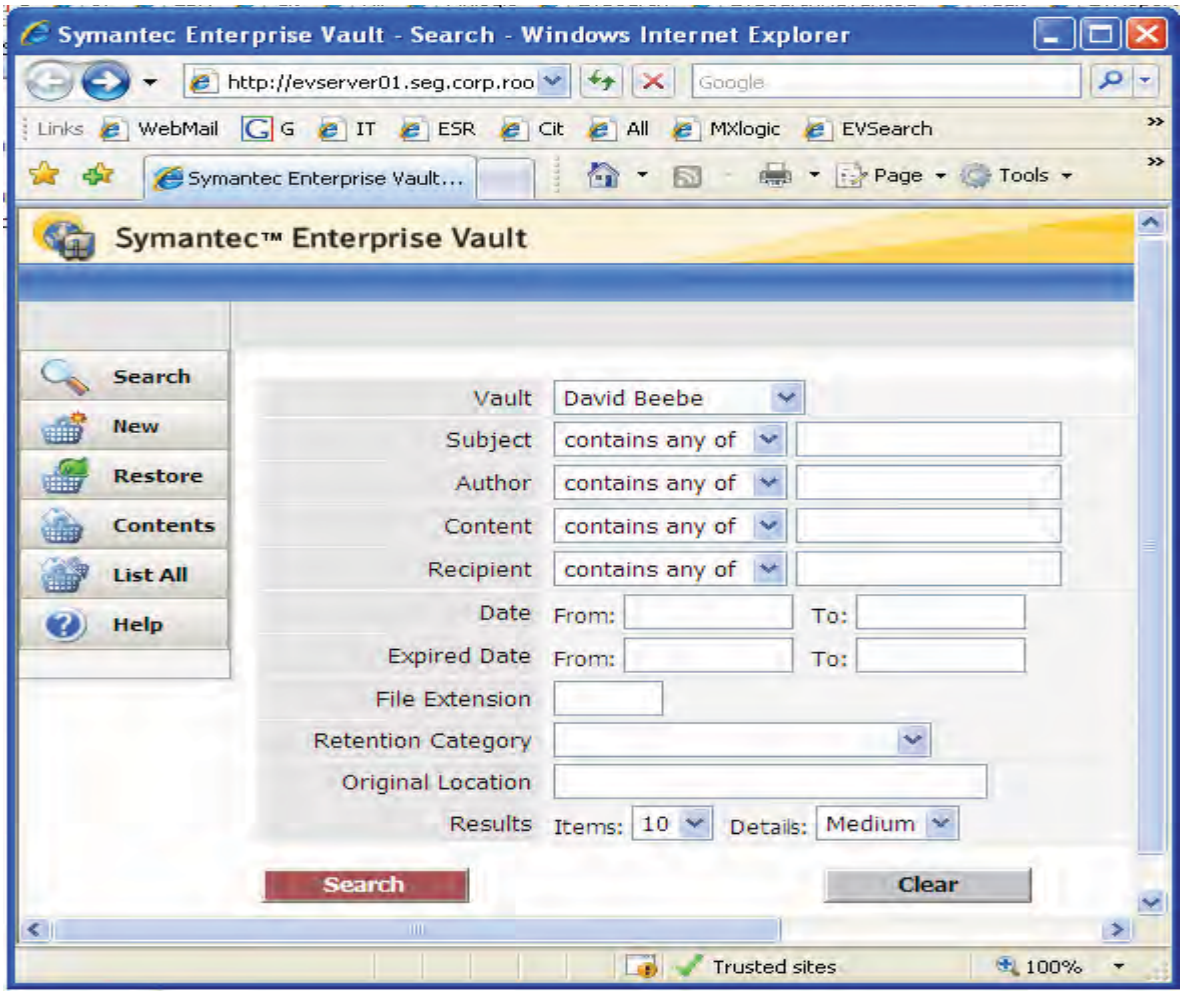
Click on the button "**Search Vaults**" on the upper right side of Outlook and in the "**Look For**" field enter criteria that matches an email that you manually archived or that was automatically archived in your Vault during the nightly archive process and then click "**Find Now**".

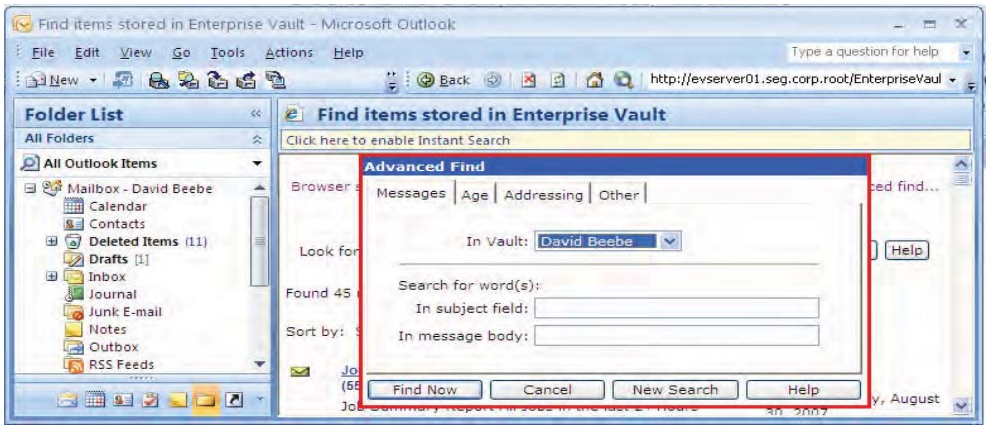




In the same search screen click on "**Browser Search**" and "**Advanced Find**" and you should see the screenshots below.



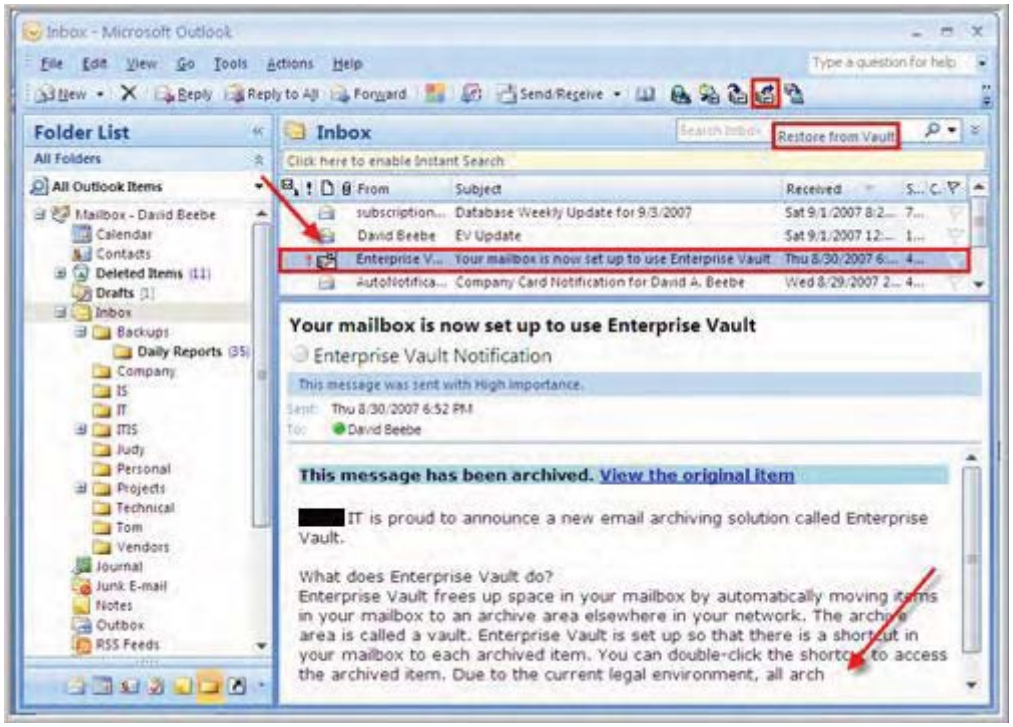




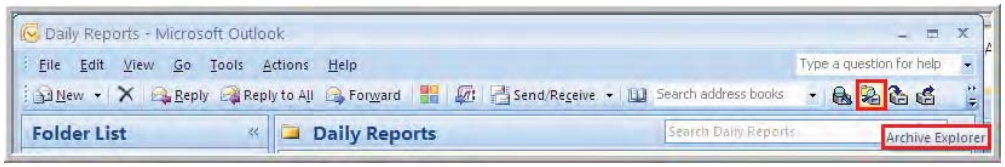
Highlight an email that was archived on a previous day. You can find these by noting the archive icon next to the email. Also notice that in the reading pane of the email that the text stops after 500 characters, as the rest of the email is archived. Note

that if you just archived the item it will not change to a shortcut until the nightly processes complete, so until that time you will see the whole email although it will still be stored in archive as well as in your mailbox. Then click on the "**Restore from Vault"** button and click OK. The email should restore within a few minutes, at which time the icon will change to a normal mail icon. Find another email stored in your archive and just double click on it and/or hit "**Reply**" and "**Forward**". This option doesn't restore the email from the archive, but allows you to read or email the entire message. Note that as a best practice this is what should usually be done, rather than restoring the email from the Vault. If you restore it from the vault it will not automatically archive again for 6 more months.



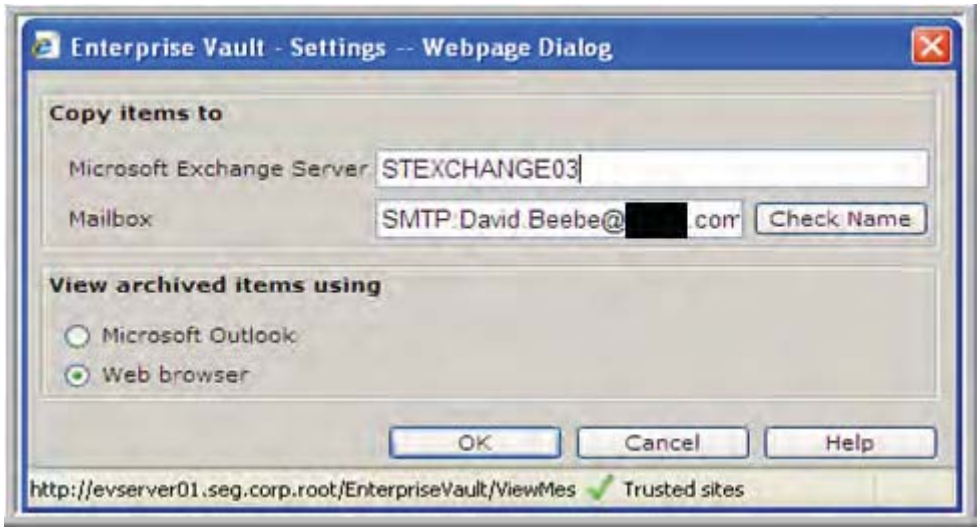


Click on the "**Archive Explorer**" button on the upper right side of Outlook. This will launch Internet Explorer like the screenshot pictured below. You should have the same folder structure on the left side as you have in Outlook as long as there are archived items present in that folder. Once again note that in the left pane you might see more than just your mailbox, this is due to the fact that any mailbox you currently have access to will be displayed there.

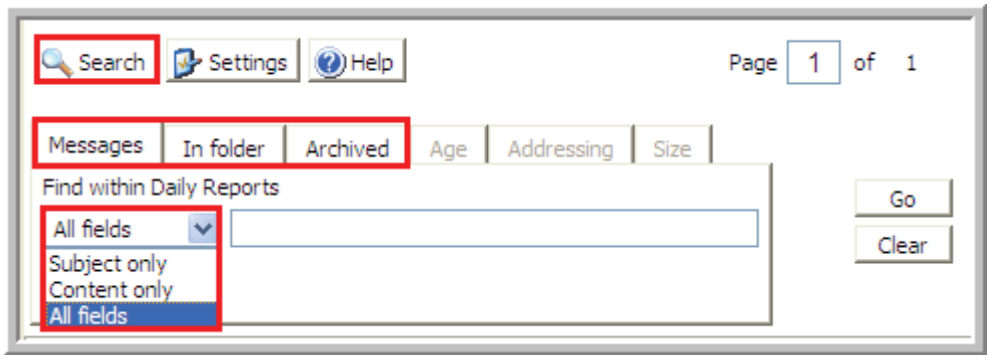




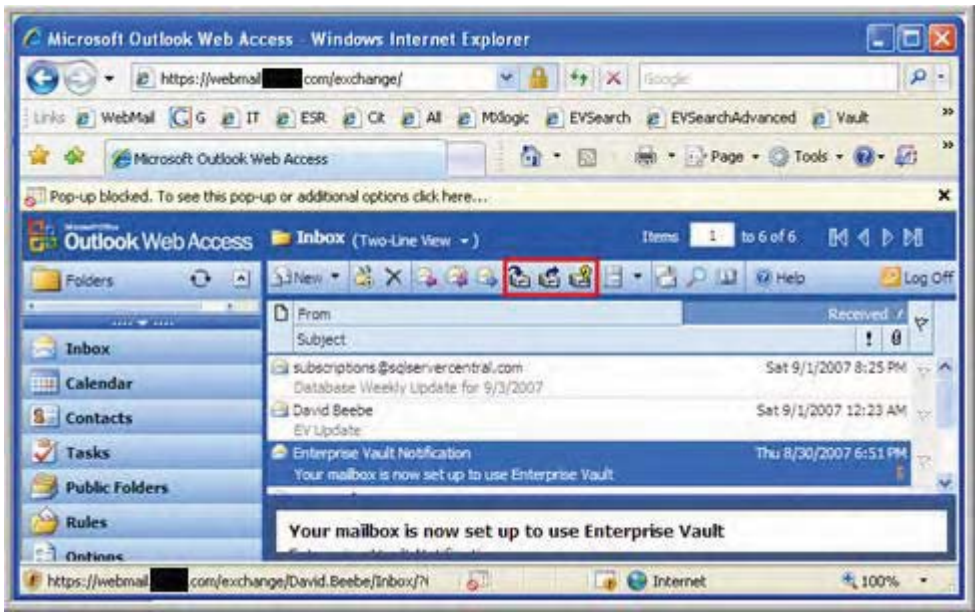
Click on the "**Settings**" button and you will see the screen pictured below and can select to view archived items in Outlook or in the Web Browser. Do not change the Exchange Server or Mailbox.



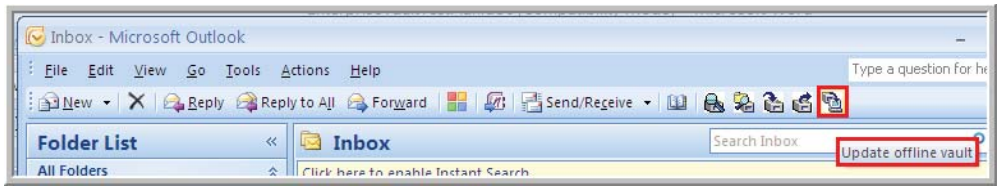
Click on the "**Search**" button and note that you have the three tabs available to choose from and that you can search Subject, Content and All. Select the "**In Folder**" tab and edit the search criteria to fit what you are looking for.

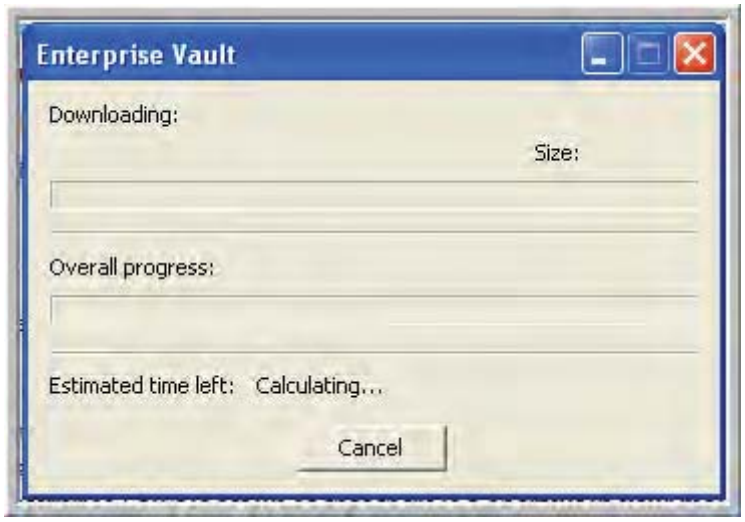


Open up a web browser and go to Outlook Web Access: https://webmail.company.com/exchange. Note that the three Enterprise Vault buttons show up like pictured below.

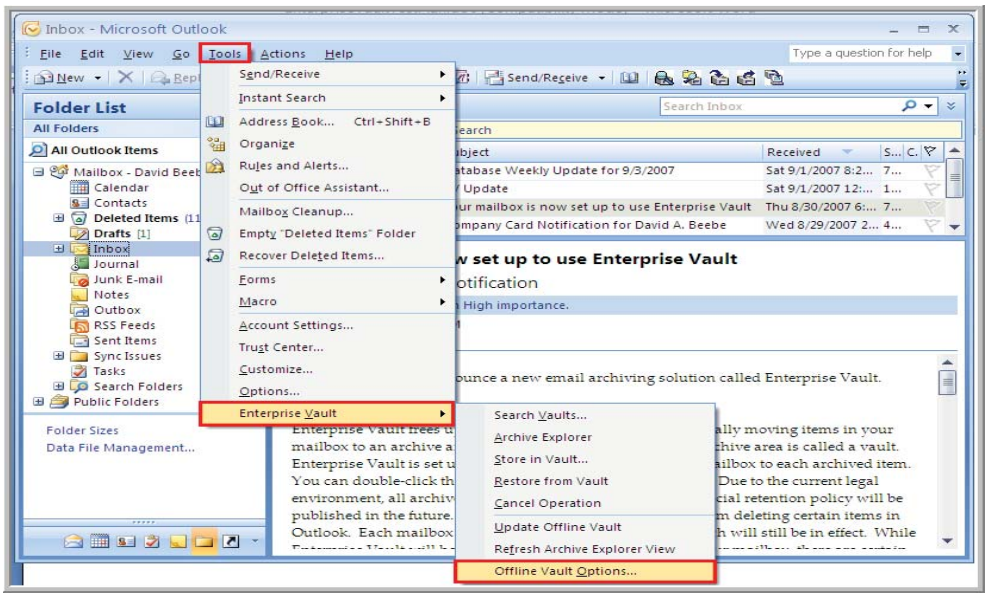

Microsoft Outlook Web Access - Windows Internet Explorer
https://webmail[redacted].com/exchange/
WebMail
Microsoft Outlook Web Access
Pop-up blocked. To see this pop-up or additional options click here...
Outlook Web Access
Inbox (Two-Line View)
Items 1 to 6 of 6
Folders
New
Help
Log Off
From
Subject
Received
Inbox
Calendar
Contacts
Tasks
Public Folders
Rules
Options
subscriptions@sqlservercentral.com
Database Weekly Update for 9/3/2007
Sat 9/1/2007 8:25 PM
David Beebe
EV Update
Sat 9/1/2007 12:23 AM
Enterprise Vault Notification
Your mailbox is now set up to use Enterprise Vault
Thu 8/30/2007 6:51 PM
Your mailbox is now set up to use Enterprise Vault
https://webmail[redacted].com/exchange/David.Beebe/Inbox/?
Internet
100%

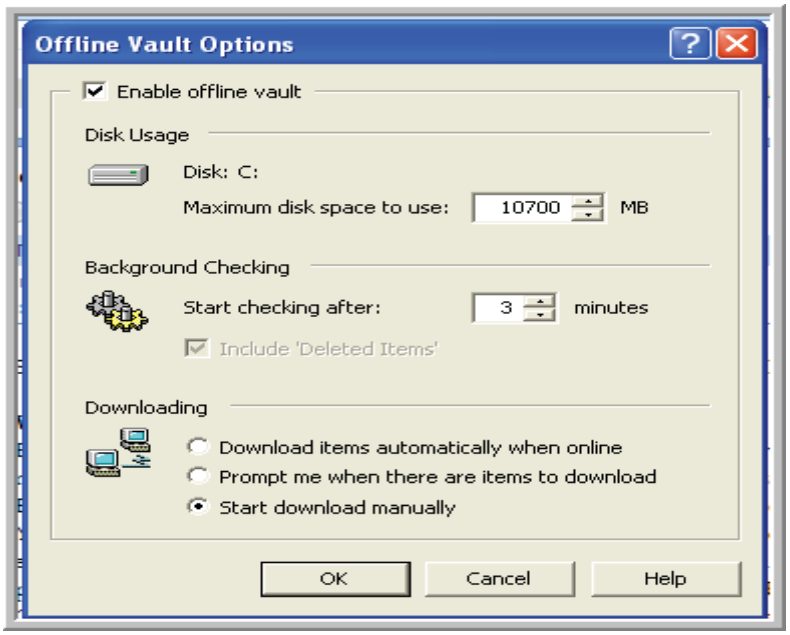
NOTE: If you are not using a laptop then do not continue with the following Offline Vault checks. Click on the "**Update Offline Vault**" button and verify you see the status screen below. This will download a copy of all of your archived email to your laptop. Note that Offline Vault is updated often, so the status screen below might only be visible for a second or less.





Click on **Tools > Enterprise Vault > Offline Vault Options** and note that you can view and edit the settings like pictured below.





Appendix B

Enable Mailbox Email

This following email is automatically sent to all newly enabled users of Enterprise Vault, with the Overview above attached as a word document.

The company and parent company are implementing a new email archiving solution called Enterprise Vault.

What does Enterprise Vault do?

Enterprise Vault frees up space in your mailbox by automatically moving items in your mailbox that are over six months old to an archive area on our company network. The archive area is called a "vault". Enterprise Vault is configured so that it leaves a shortcut link in your Outlook mailbox that connects you to each item that has been moved to the vault. Because we are reducing the size of your mailbox by moving older items to the vault, you will get better performance from Outlook with less clutter.

At this time, we will not be deleting any archived items from the vault. Once we are up and running with all aspects of the electronic records portion of our Records Management Policy, we will begin dropping off older email (generally email older than two years). You will receive advance notice of the implementation of this email retention period so that you can store (pursuant to the retention periods in the Records Management Policy) any email that would be subject to deletion.

What does Enterprise Vault archive?

Enterprise Vault archives all types of information stored in your private folders on the Microsoft Exchange Server computer. This includes mail messages, documents, spreadsheets and graphics. Enterprise Vault does not archive any information that is held in your personal folder (PST) files or documents on the hard disk on your computer.

What else does Enterprise Vault do?

In addition to its archiving functions, Enterprise Vault keeps a copy of all email that crosses the Company's email network on a real time, chronological basis. Any email that is

received or sent over the Company network will be retained by the Company in this database for at least two years and cannot be deleted from the vault.

Please continue to follow the Company's guidelines re the proper use of the email system and proper communications. Those guidelines can be found in the Records Management Policy, a copy of which is on the Company's intranet site.

Outlook AutoArchive Settings

Outlook's AutoArchive archiving is different from Enterprise Vault archiving. AutoArchive archives items to a personal folder file (PST file) on your computer hard disk. Enterprise Vault archives items to a storage area on the network so that the items can be safely backed up and you can easily view, search, or restore them as needed. If you currently have Outlook AutoArchiving turned on, we recommend you turn it off.

How to turn off AutoArchive in Outlook

1. On the Tools menu, click Options.
2. Click the Other tab.
3. Click AutoArchive.
4. Clear the Run AutoArchive every check box.

Searching for Archived Items

Enterprise Vault has two different ways for you to search for archived items:

- A search that appears within Outlook:
- Click on the "Search Vaults" Icon in Outlook. Below is what the icons look like.



- A search that you use in a web browser: http://ev/enterprisevault/

The Enterprise Vault search enables you to find an archived item easily and quickly. You can enter text to search for and, if you want, specify other details such as the age of the item or the folder that it was in before being archived. Having found an item that you want, you can view it immediately without restoring it to your mailbox. You can then print or reply as normal.

Want to learn more about how Enterprise Vault Email Archiving can help you?

If you are interested in getting more familiar with the features and functionality of Enterprise Vault, please refer to the attached document “Overview of Email Archiving".

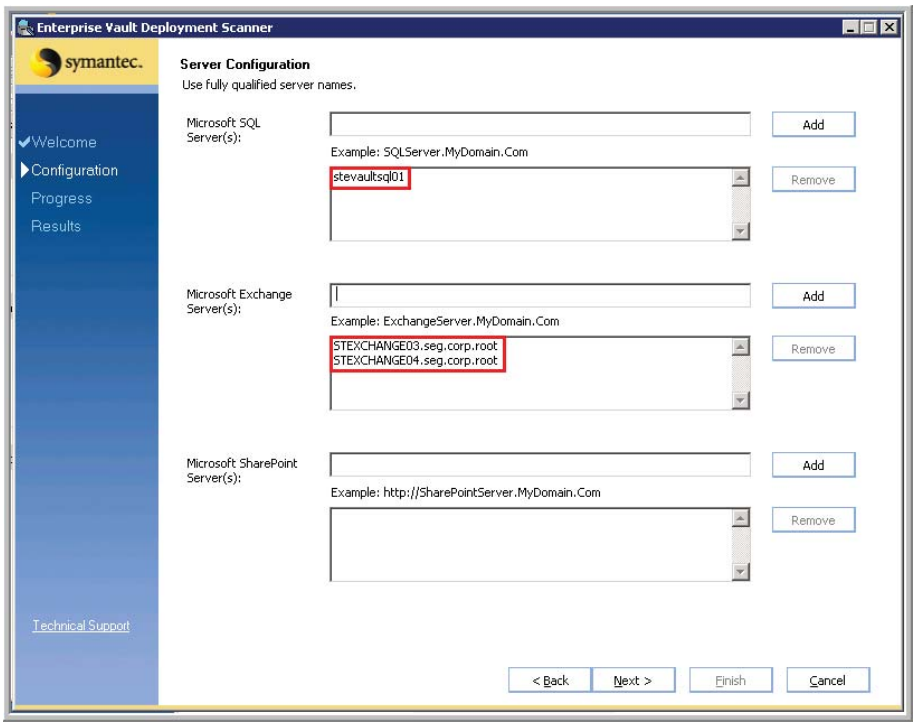
Please contact IT if you have any questions or concerns.

Appendix C

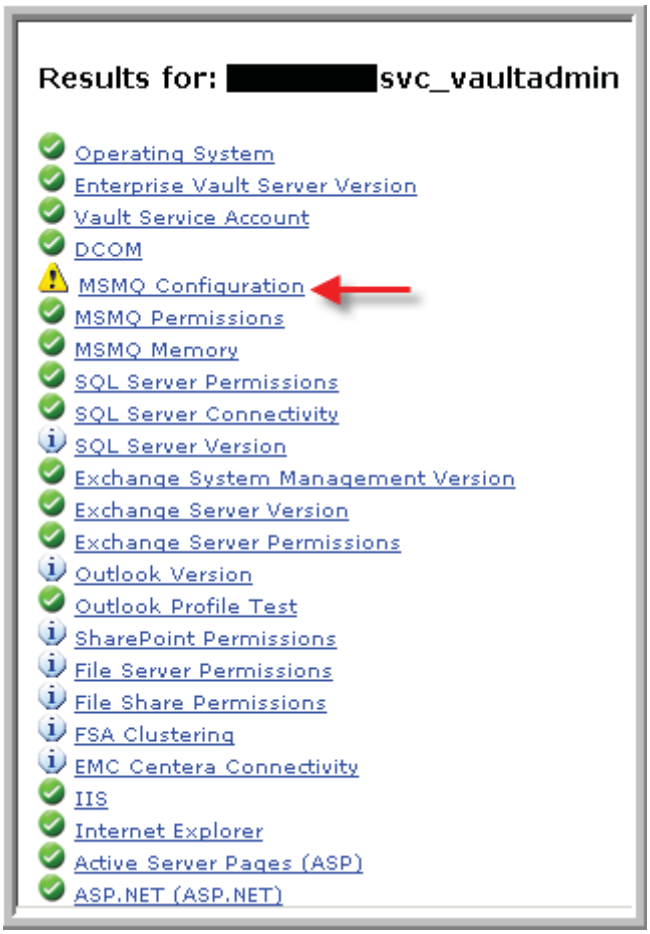
Prerequisites

Confirm hardware requirements are met, including the HBA’s being configured and LUN’s presented and configured on the servers.

Install the deployment scanner on the Enterprise Vault servers (STEVAULT01 and STEVAULT02). This application will identify any prerequisite installation requirements. Confirm that the proper Exchange and SQL servers are added to the deployment scanner configuration screen.



Confirm that you have all green checkmarks next to the prerequisites. Note that MSMQ might show with a caution, but if that is because it is not active directory enabled or based on the location of the storage then it is not a concern.



Add MSMQ by going into Add/Remove programs in the control panel and select details for Application Server. Select Message Queue and then select details and deselect the AD integration option. Also go into the application server and select ASP.NET and then into the details of IIS, then the details of worldwide web and check Active Server Pages. Complete the install by pointing to the I386 directory which should be located at the root of the Operating System install. NOTE: For the initial installation we are not separating the Operating System and Application on separate drives, to increase performance this should be done and the MSMQ queues should be moved to the application drive as well as the page file.

Install Outlook 2003 and do a custom install and select collaborative data objects.

Install Exchange System Manager Tools and then upgrade the tools to SP2 if the install doesn't include the service pack.

Install the .NET framework 2.0.

Load a new Exchange profile under the VaultAdmin account.

Install registry keys for the following errors: Error when a client connects to a Windows 2003 alias name. Refer to http://support.microsoft.com/kb/281308. Error when you browse a website that uses Integrated Authentication and is hosted on IIS 6.0. Refer to http://support.microsoft.com/kb/896861/. Error logged for Server service when server is under heavy load. Refer to http://support.microsoft.com/kb/312362. Error with Message Queuing and memory utilization. Refer to http://support.microsoft.com/kb/811308 and http://seer.support.veritas.com/docs/273228.htm. Error with name limit. Refer to http://support.microsoft.com/kb/319504/en-us

Go to windows update and download and install all high priority updates.

SQL Server Prerequisites

Confirm hardware requirements are met in the documentation above, including the HBA's being configured and LUN's presented and configured on the servers

These steps need to be completed on the Enterprise Vault SQL server STEVAULTSQL01. Make sure the VaultAdmin account is a local administrator on the server. Confirm that IIS 6.0 is installed and patched.

Install SQL 2005 Standard 32 bit with the following options: Database Services, Analysis Services, Reporting Services, Workstation Components, Books Online and

Development Tools all in the default instance, although a named instance can be used as well. Use the built-in system account and under services make sure you setup SQL Server, Analysis Services, Reporting Services and SQL Server Agent in mixed mode and enter the password for the SA account. Use the default SQL collations and configuration and don't select options for error and usage report settings.

Install SQL 2005 SP2 and leave all program features selected. Apply to all instances and leave the services running and reboot after the install.

Install the SQL 2005 SP2a patch – see the following references:

- MS SQL SP2a patch:

  http://www.microsoft.com/downloads/details.aspx?FamilyId=e2c358a1-ecc4-4c49-8f65-daa6b7800eec&displaylang=en

- KB 933508

  http://support.microsoft.com/kb/933508

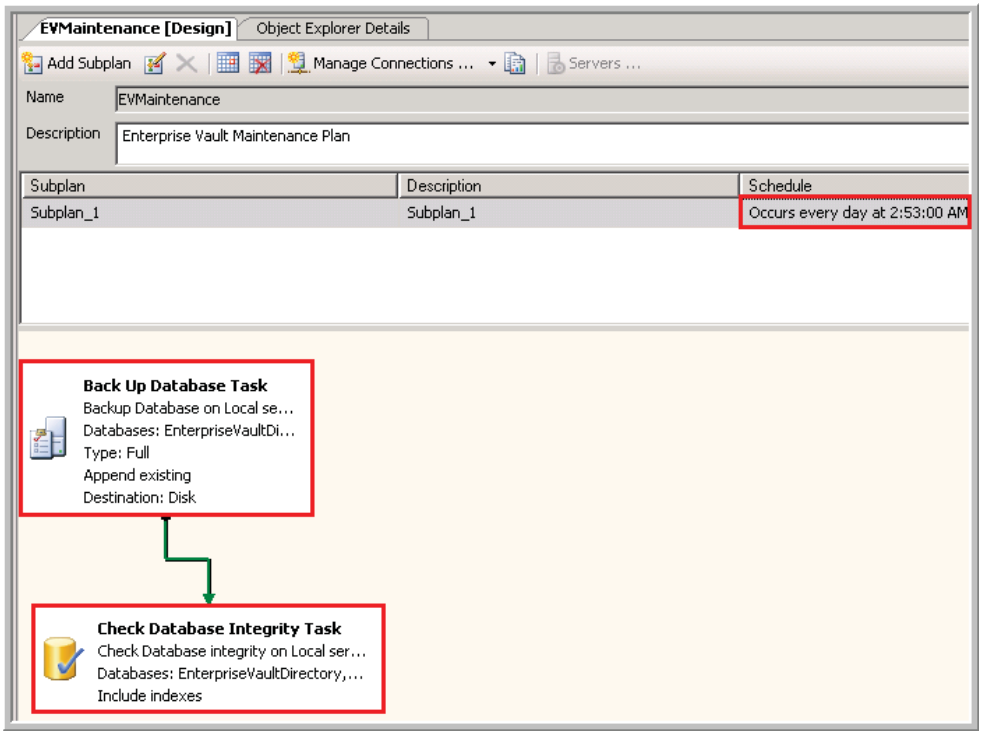
Open up SQL Server Management Studio and grant the dbcreator role to the VaultAdmin domain account.

Create the following two directories: L:\MSSQL_LOGS and Z:\MSSQL_DATA

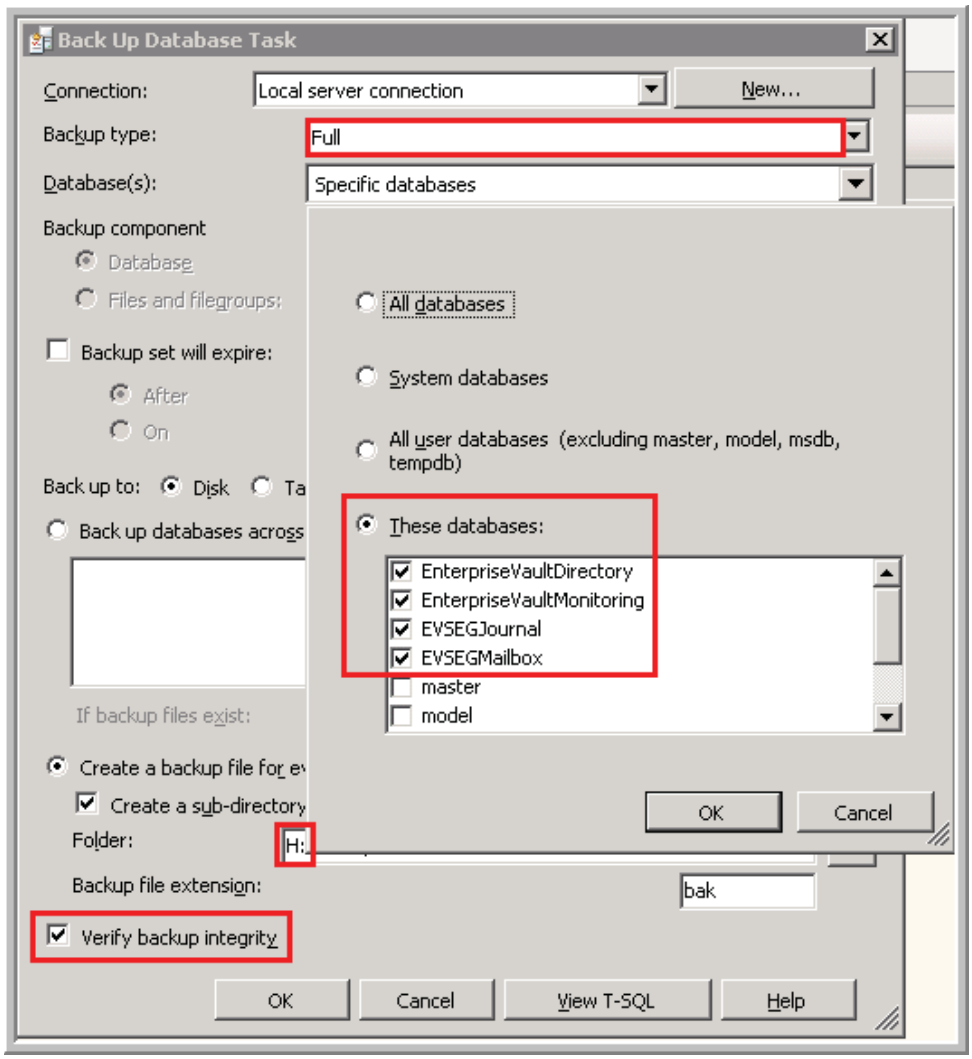
Go to Windows Update and install any critical patches that need applied.

Configure a maintenance plan called EVMaintenance on STEVAULTSQL01 that includes a backup of the Enterprise Vault databases, transaction logs and an integrity check that runs daily at 2:53 AM. Note that you should come back after all the installation steps are complete and confirm that all databases are being backed up. Also

this should be reviewed by a DBA to confirm all the proper database maintenance is being completed, i.e. cleaning up old database backups and such.



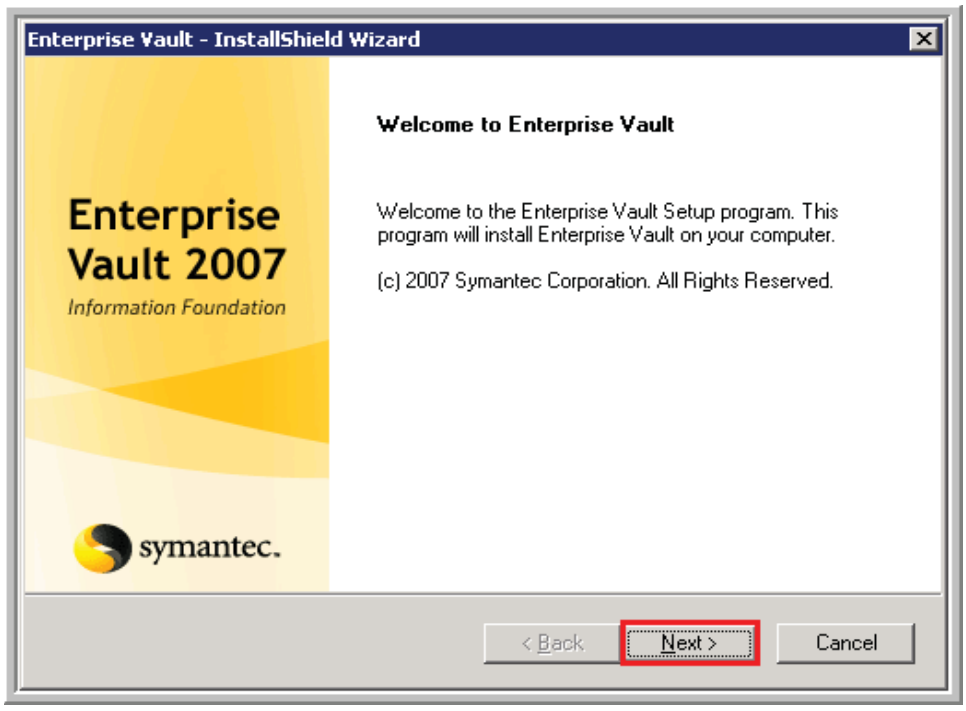
Configure it to be a full backup and be sure to include all of the Enterprise Vault databases. Set them up to backup to H:\backups and set to verify backup integrity.



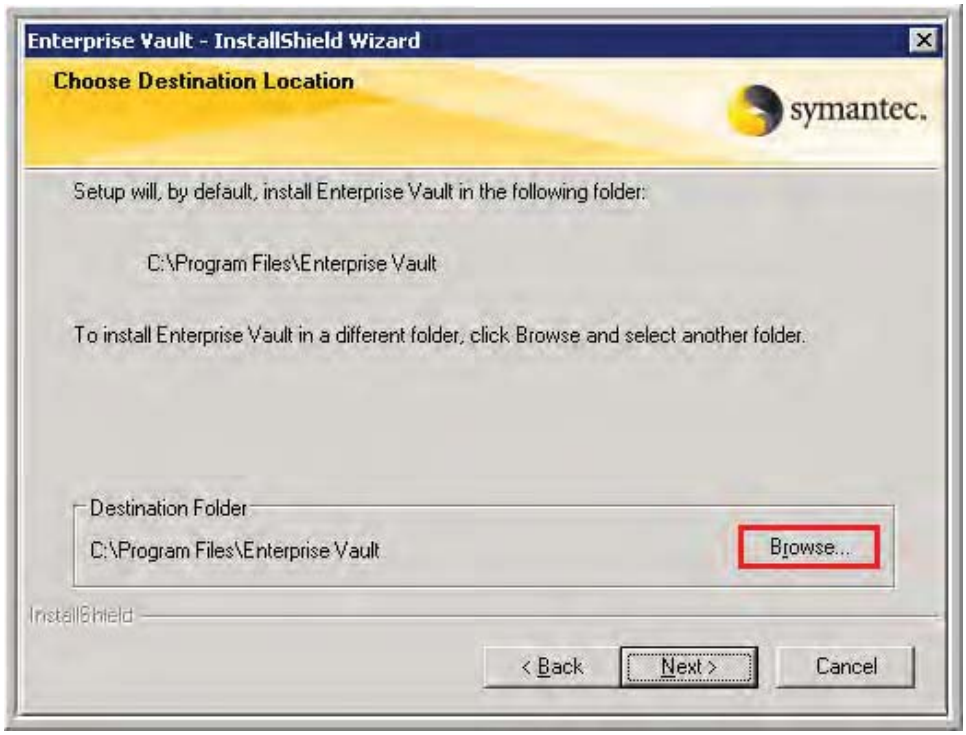
Exchange Server Extensions and Forms

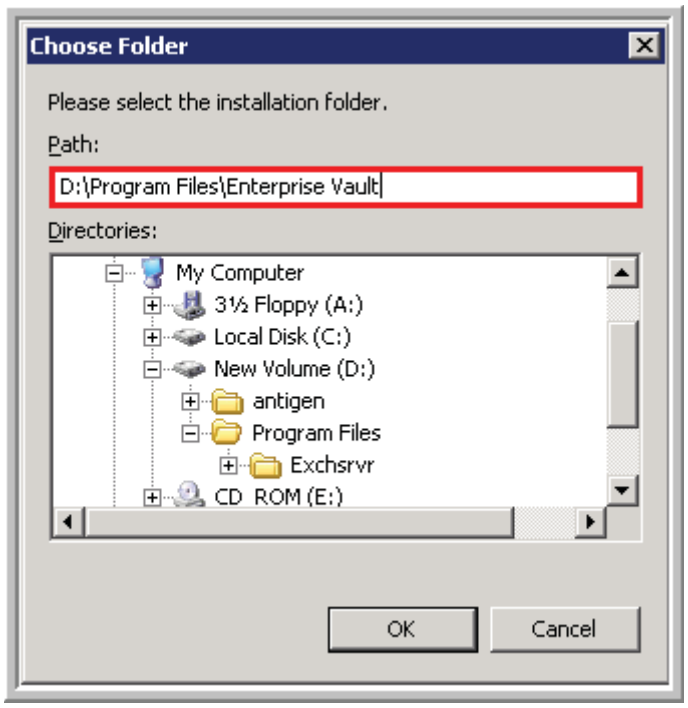
Logon to the Server with an Exchange Full Administrator account in the same domain as the Exchange Server resides, local administrator on the server and ensure that it is a member of the Exchange Domain Servers group.

Run setup.exe for Enterprise Vault 2007 (Version 7.5) and click on Next and accept the Software License Agreement.

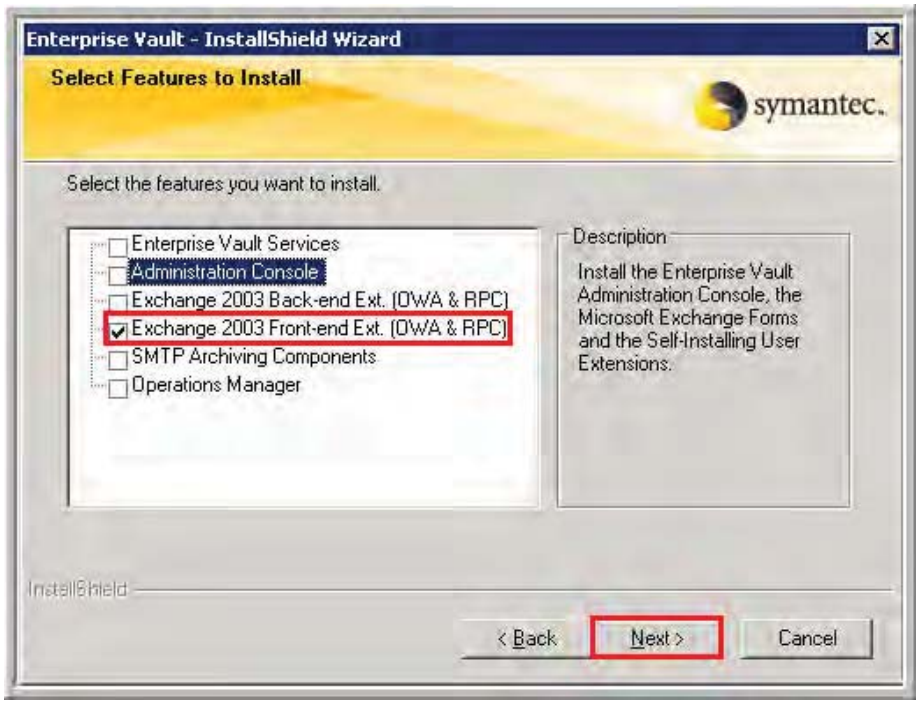


Click on Browse and install the files on the application drive, if it exists, and then click on Next.

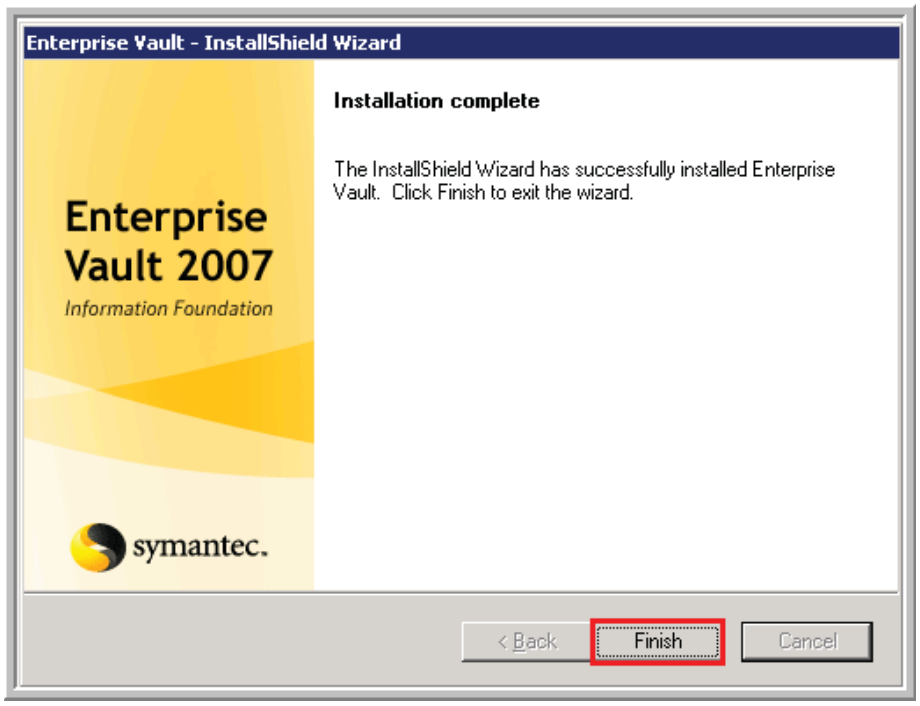




Check to install either “Exchange 2003 Front-end Ext” or “Exchange 2003 Back-end Ext” depending on the server functionality and click Next.

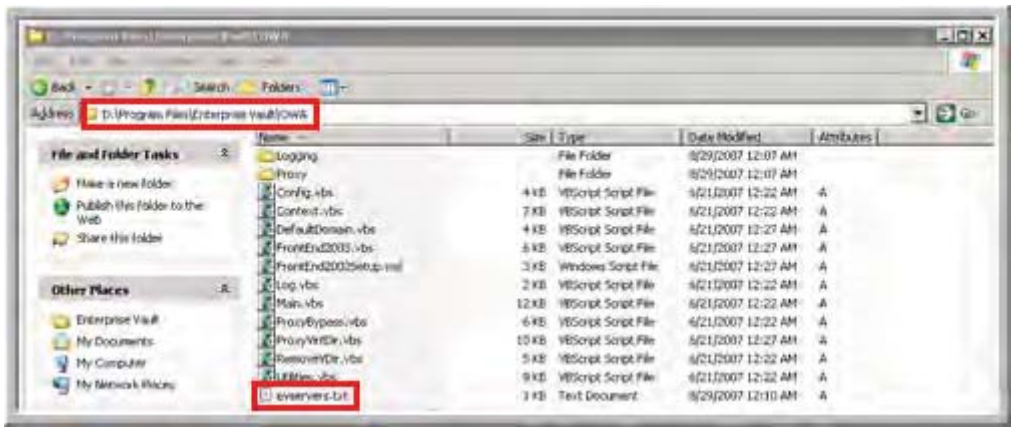


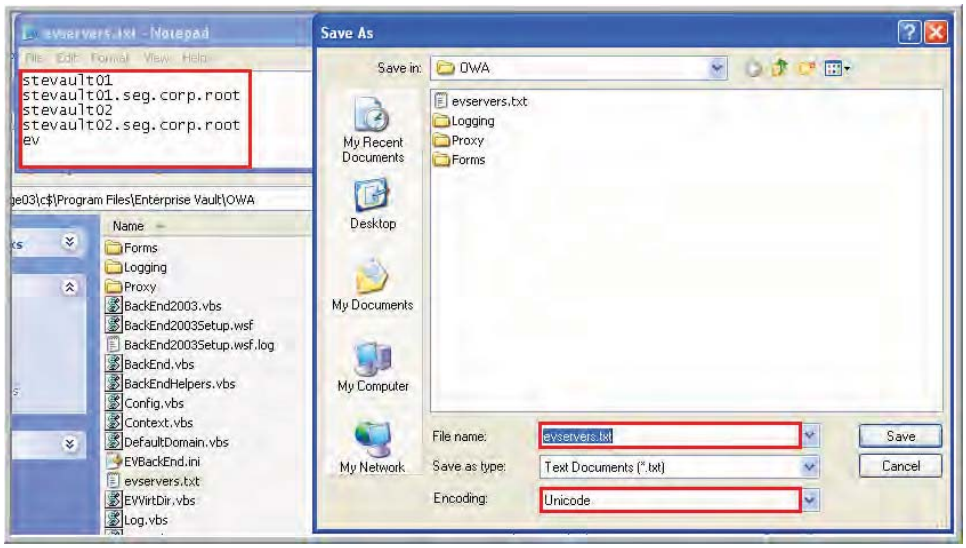
Click on Finish.



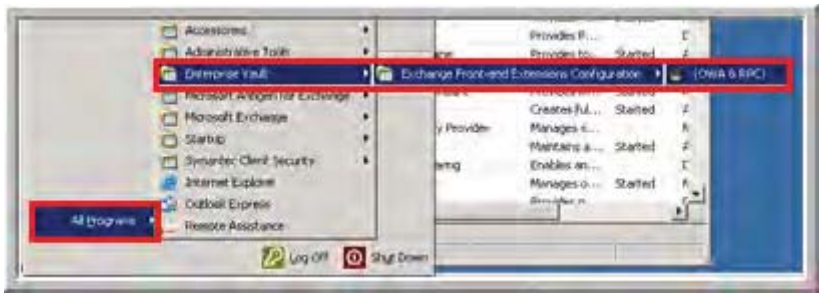
NOTE: Only complete this step on the backend exchange servers. Create a new text file called evservers.txt and save it in the application install directory, D:\Program Files\Enterprise Vault\OWA. Include the text below and save the file as Unicode.

```
stevault01
stevault01.seg.corp.root
stevault02
stevault02.seg.corp.root
evserver01
evserver01.seg.corp.root
evserver02
evserver02.seg.corp.root
ev
```

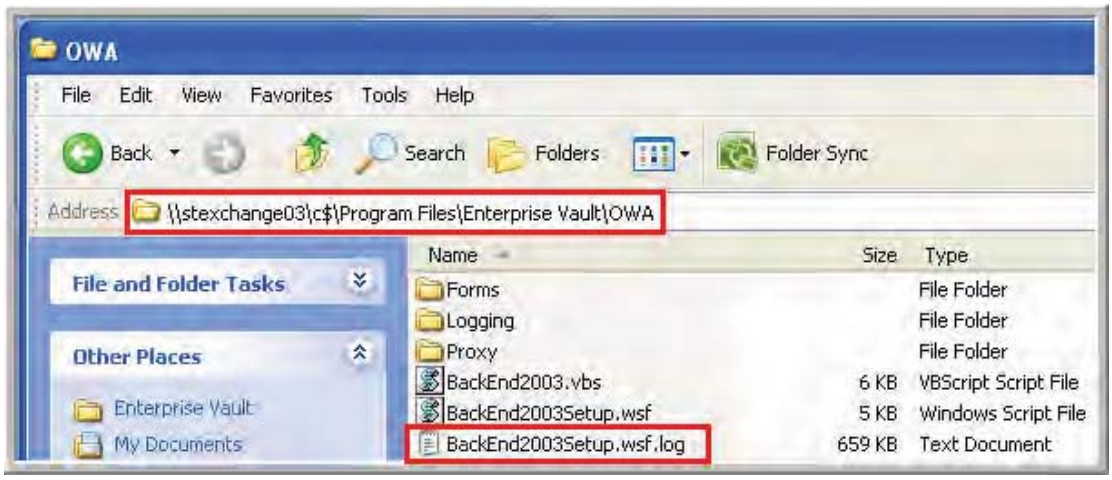


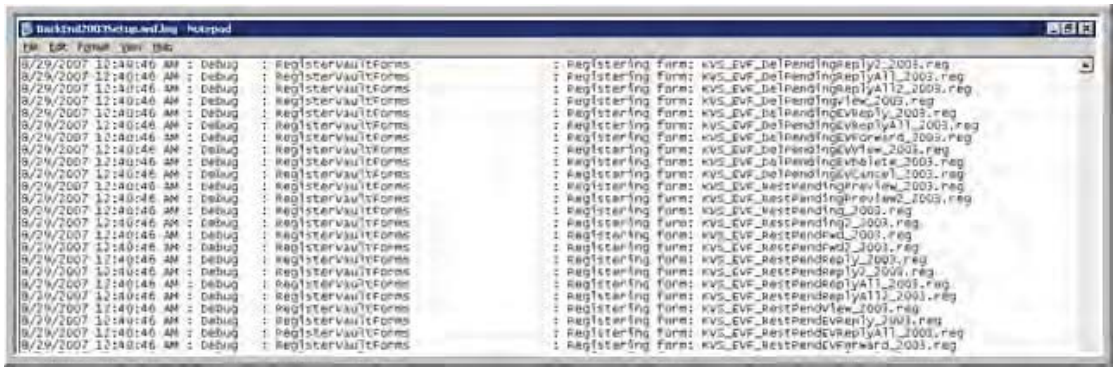


Run the Exchange configuration utility by going to Start –> All Programs –> Enterprise Vault –> Exchange Front-end Configuration (or Back-end) –> OWA & RPC. Cycle the Exchange services or reboot the server after completion.



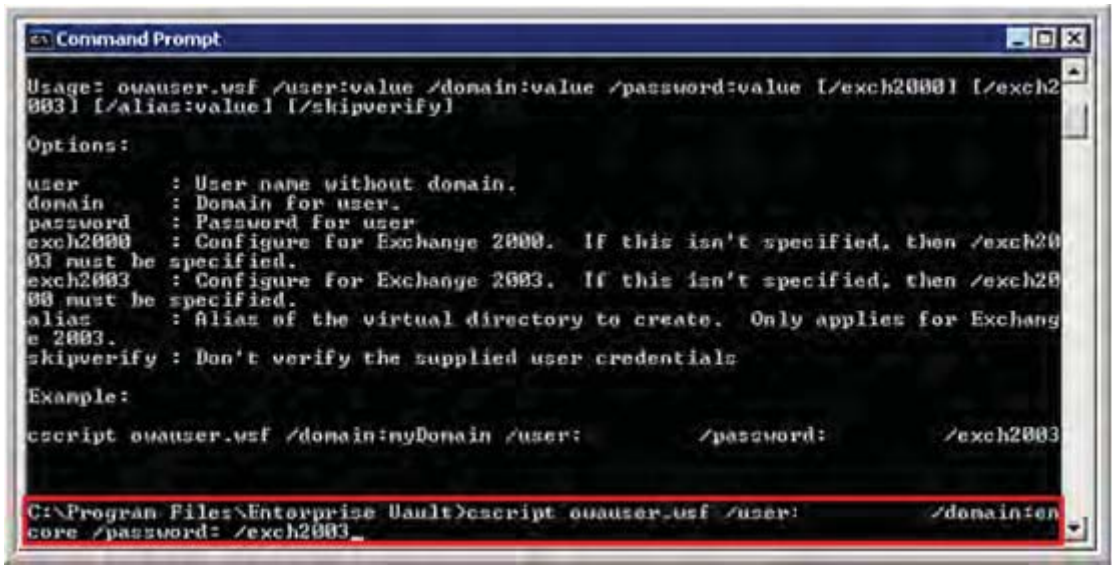
Verify on any back-end servers that forms have registered – see screenshot below. The log is called BackEnd2003Setup.wsf.log and is located in the install directory – C:\Program Files\Enterprise Vault\OWA.



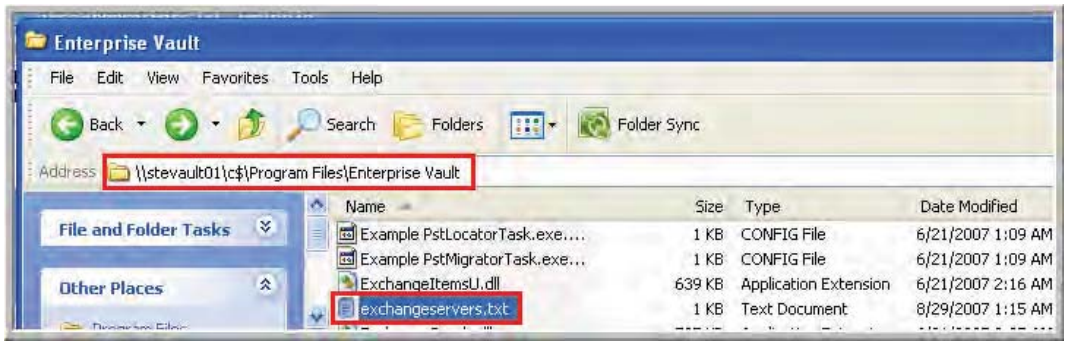


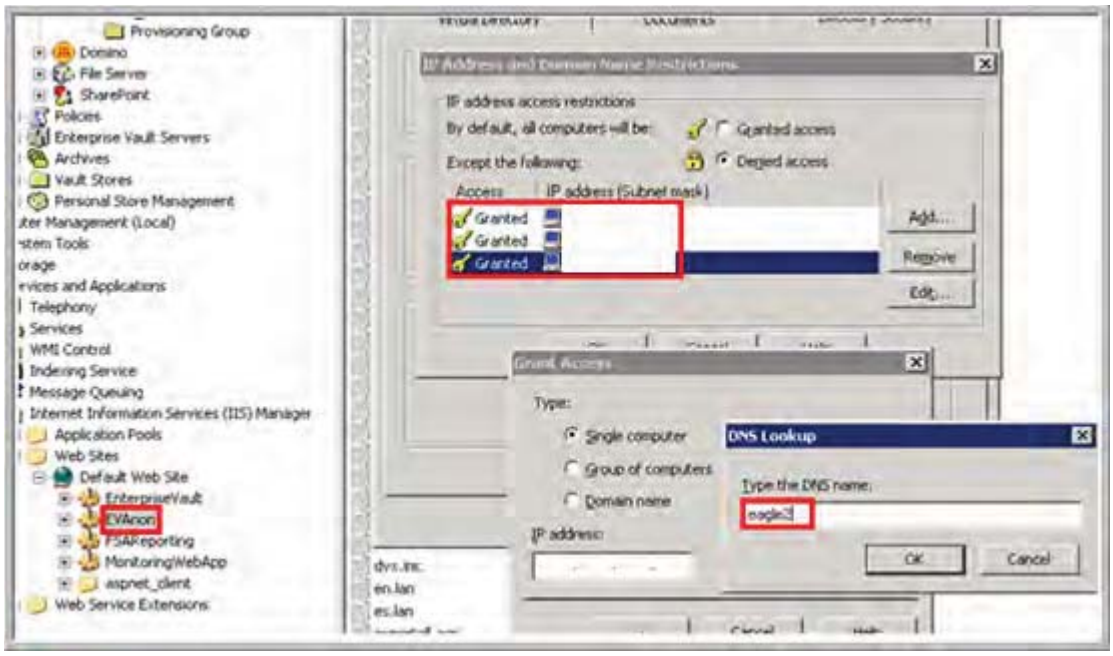
NOTE: You only need to complete this once per exchange organization.

Complete the installation on the Enterprise Vault server – STEVAULT01. Browse to the Enterprise Vault directory and run the command "cscript owauser.wsf /user:EVOWA /domain: /password:XXXXX /exch2003".

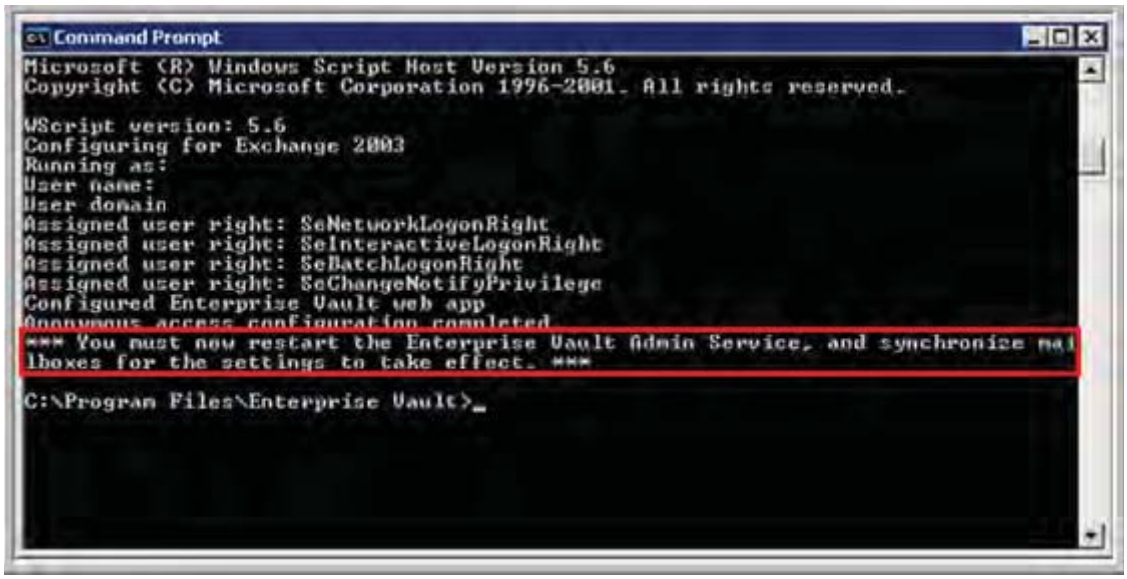


Browse to the install directory C:\Program Files\Enterprise Vault and create the file called exchangeservers.txt. In the file put in the IP addresses of the back-end exchange servers. Note the screenshot needs to include the parent company exchange servers. You can also go to the properties of the IIS site and confirm that the IP addresses are added there, see screenshot below.

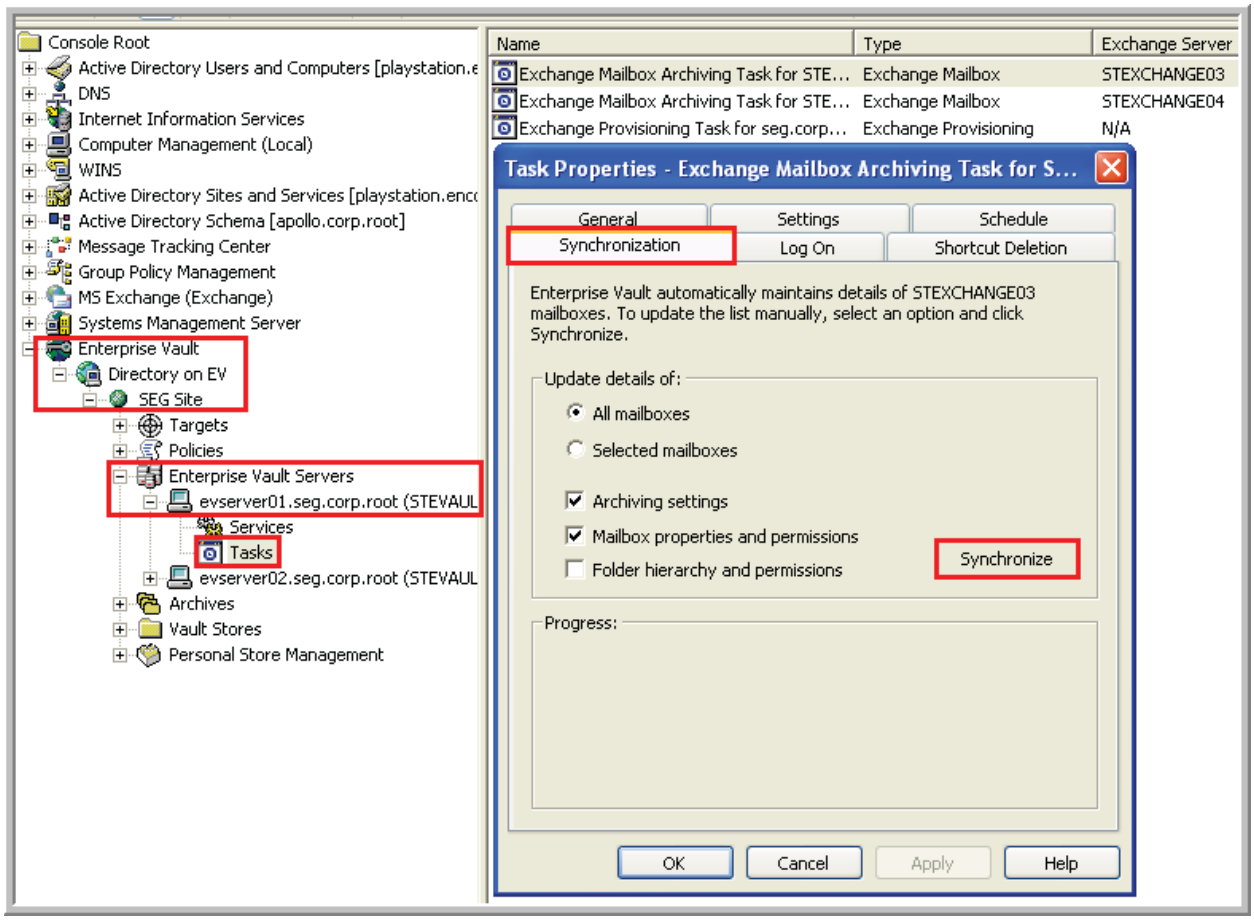




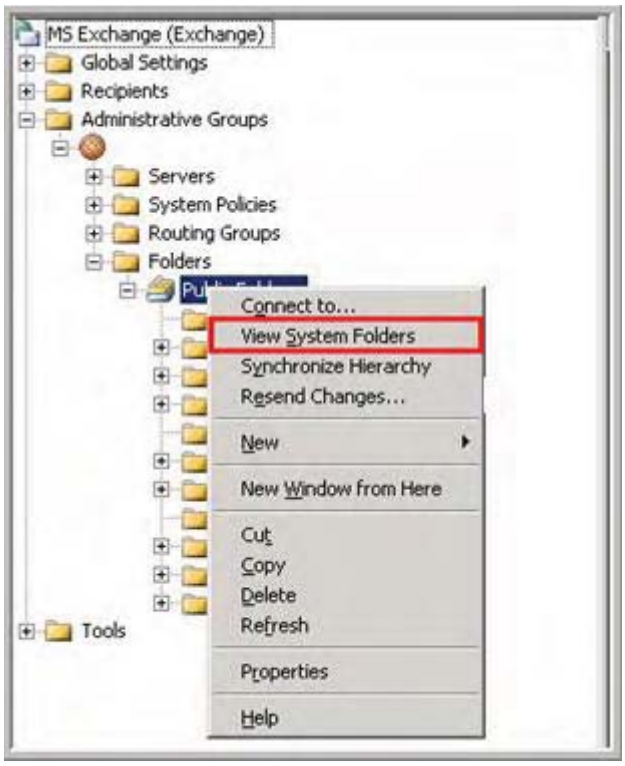
Cycle the Enterprise Vault Admin service and then synchronize the mailboxes.



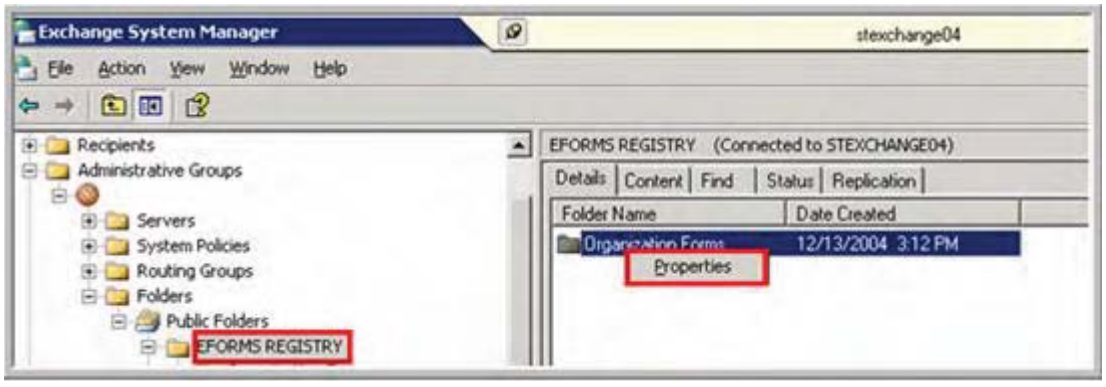
To Synchronize the mailboxes go to the Site –> Enterprise Vault Servers –> Tasks and right click on mailbox archiving task and select Properties, then select the Synchronization tab and click on Synchronize. This task runs every 12 hours, so you can also wait for this to run.



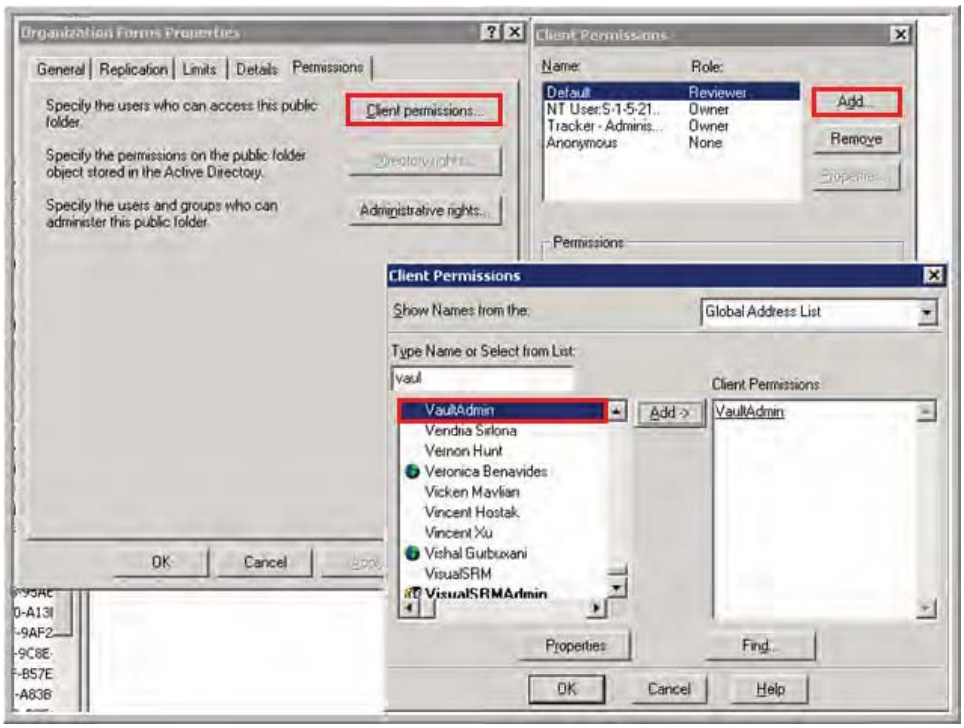
Next install the Forms on the exchange servers. Open up Exchange System Manager and browse to Company –> Folders –> Public Folders –> and right click on Public Folders and select View System Folders.



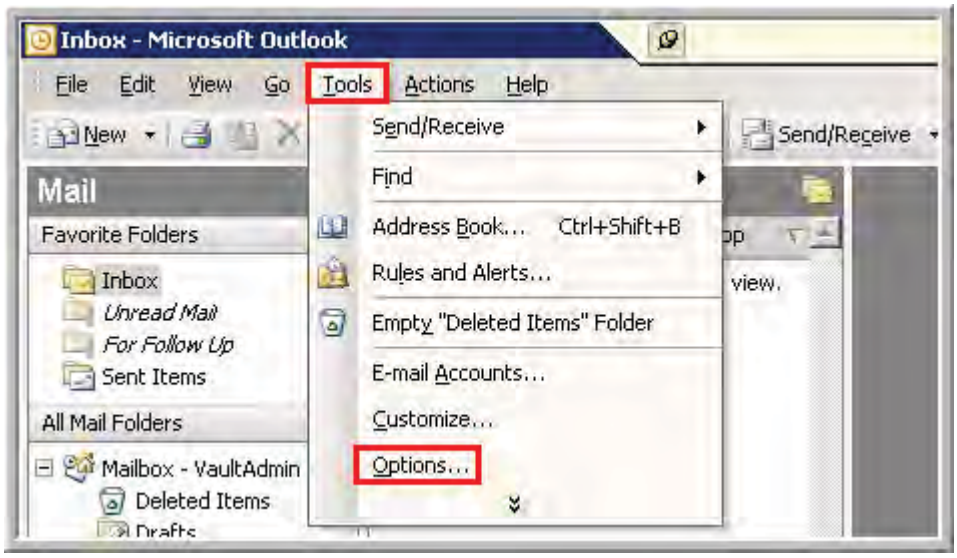
Highlight EFORMS REGISTRY and in the right pane right click on Organization Forms and select Properties.



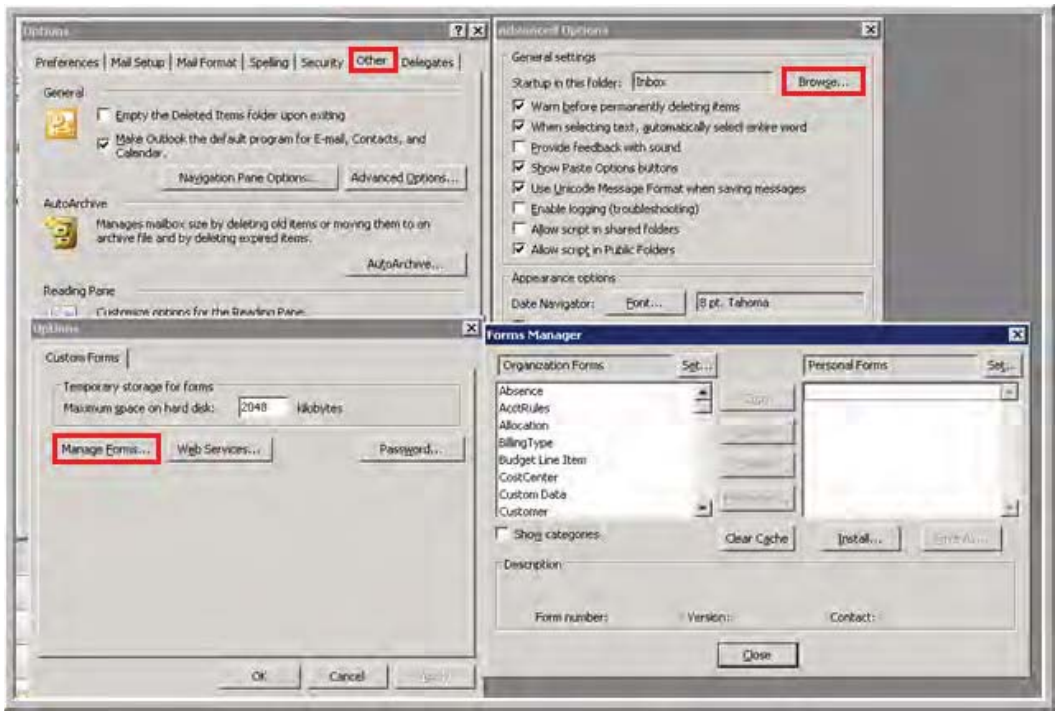
Click on Client Permissions and then Add and add the VaultAdmin account with Owner privileges and then Click OK twice to exit.



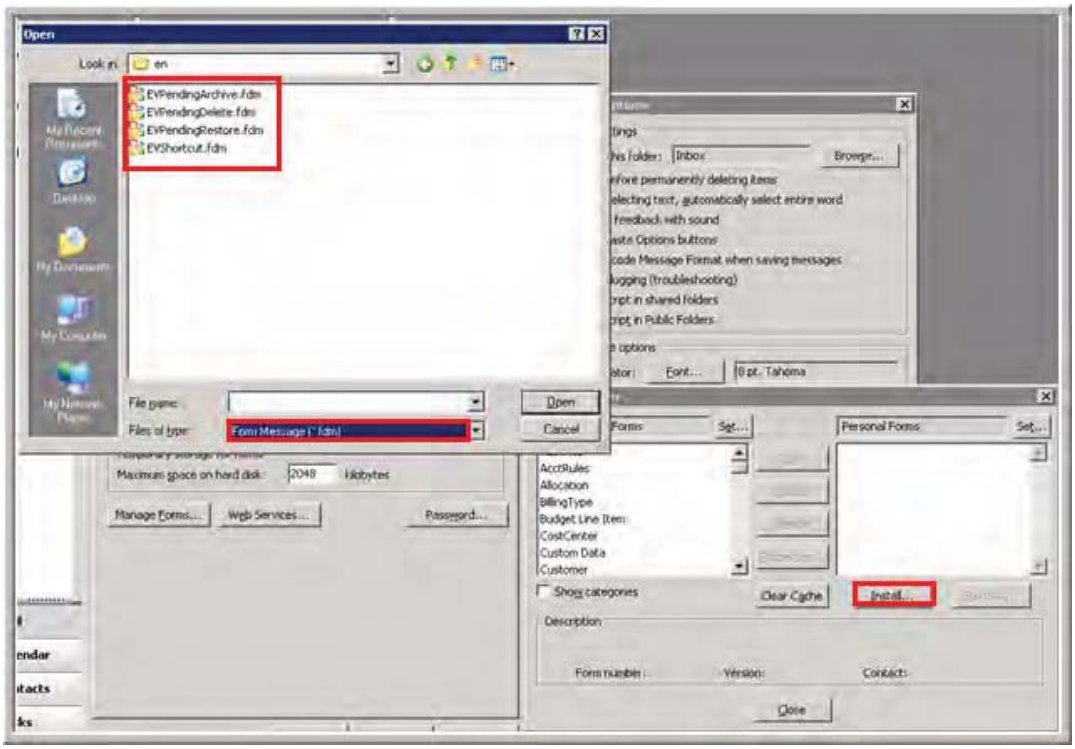
Add the forms to Exchange so the Enterprise Vault icons can be seen in the mailboxes. Open up Outlook using the VaultAdmin profile. Click on Tools –> Options.



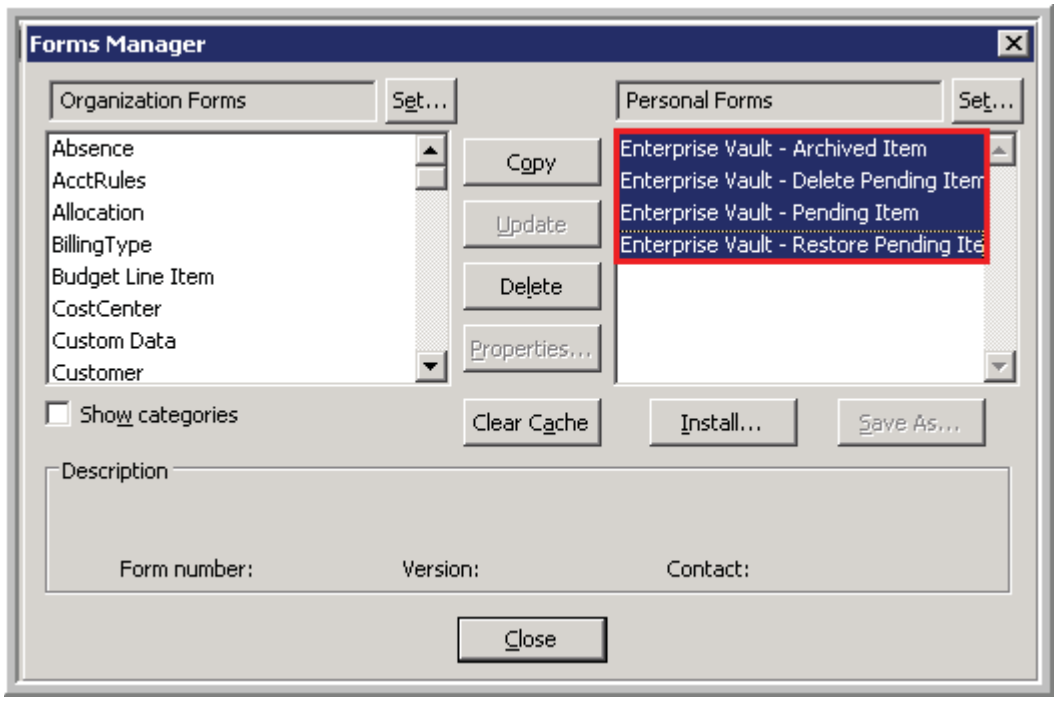
Click on the Other tab –> Advanced Options –> Custom Forms –> Manage Forms.



Then click on Install and browse to c:\program files\enterprise vault\languages\forms\en and change the view type to FDM.



Add the four Enterprise Vault forms then click Close and OK 3 times.

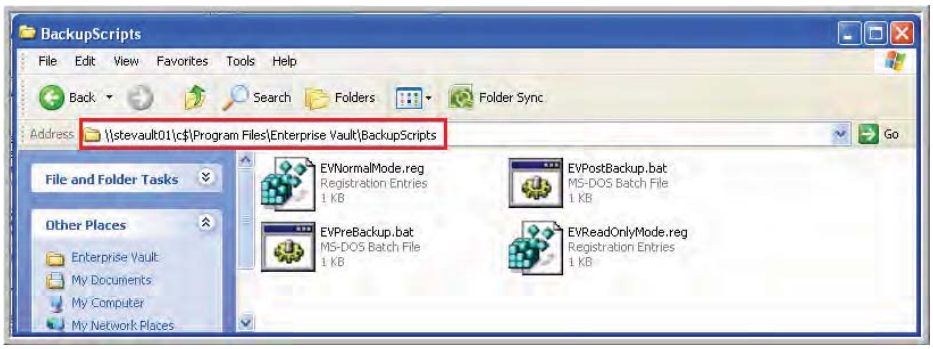


Last you need to configure ISA so the Outlook Web Access buttons are visible from external. See configuration documentation on this piece.

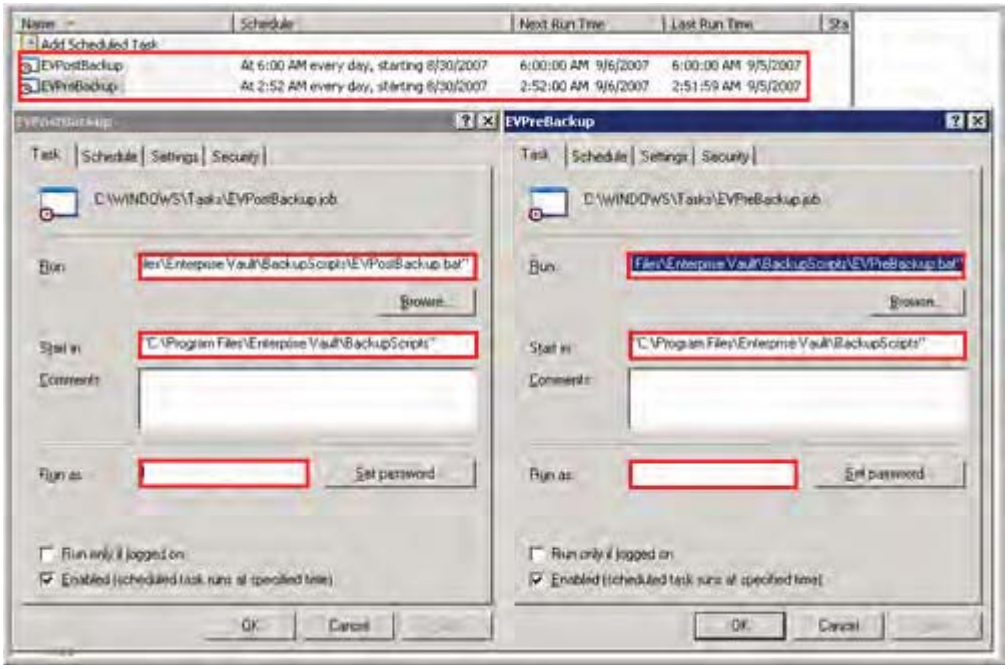
Vault Server Backups

Setup backups for all Enterprise Vault servers ensuring that the Index and Vault drives are being backed up. Note that these backups must be setup to reset the archive bit otherwise Enterprise Vault will not know it was backed up and therefore won't delete the safety copy and create the shortcut. With TSM you have to have the following entry in the dsm.opt file: "RESETARCHIVEATTRIBUTE YES"

Next copy the backup scripts from the installation files for Enterprise Vault to both STEVAULT01 and STEVAULT02.



Setup scheduled tasks on both servers with the pre-backup running at 2:45 AM daily and the post running at 6:00 AM daily using the VaultAdmin account to run.



The backup process for Enterprise Vault needs to be run in a specific order to ensure the successful restore if necessary. When exchange is upgraded or backups are changed the following order needs to be followed. Backup exchange and complete prior to archiving → Archiving Runs (currently from 12:00 AM – 2:45 AM) → Specific EV services are stopped (currently happens at 2:50) → SQL Database Dump is completed

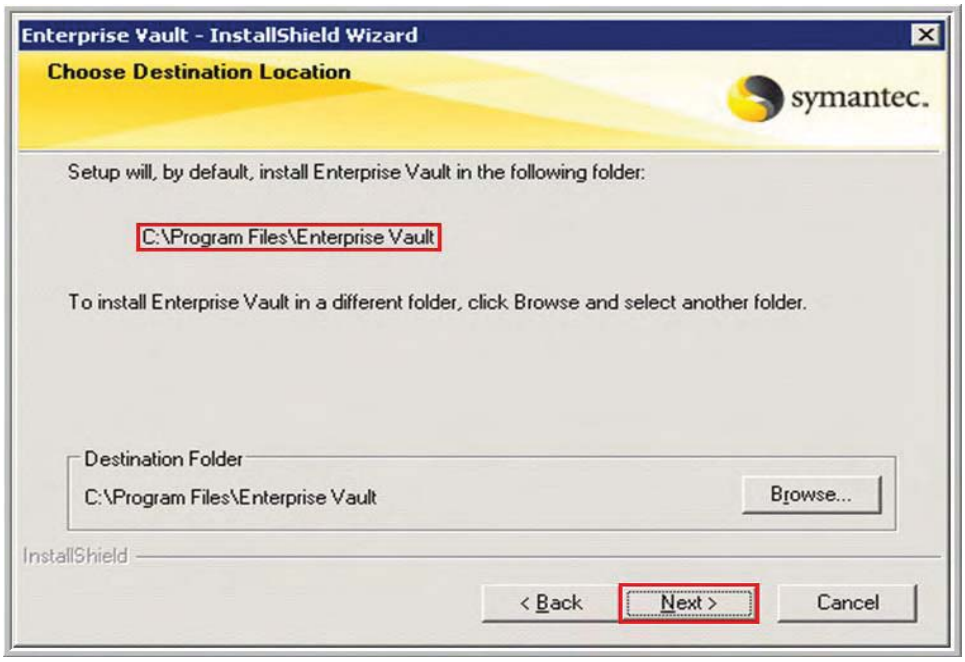
(currently happens at 2:52) → EV Servers are backed up (Currently happens at 3:00 AM) → SQL services are restarted via the scheduled task at 6:00 AM.

Appendix D

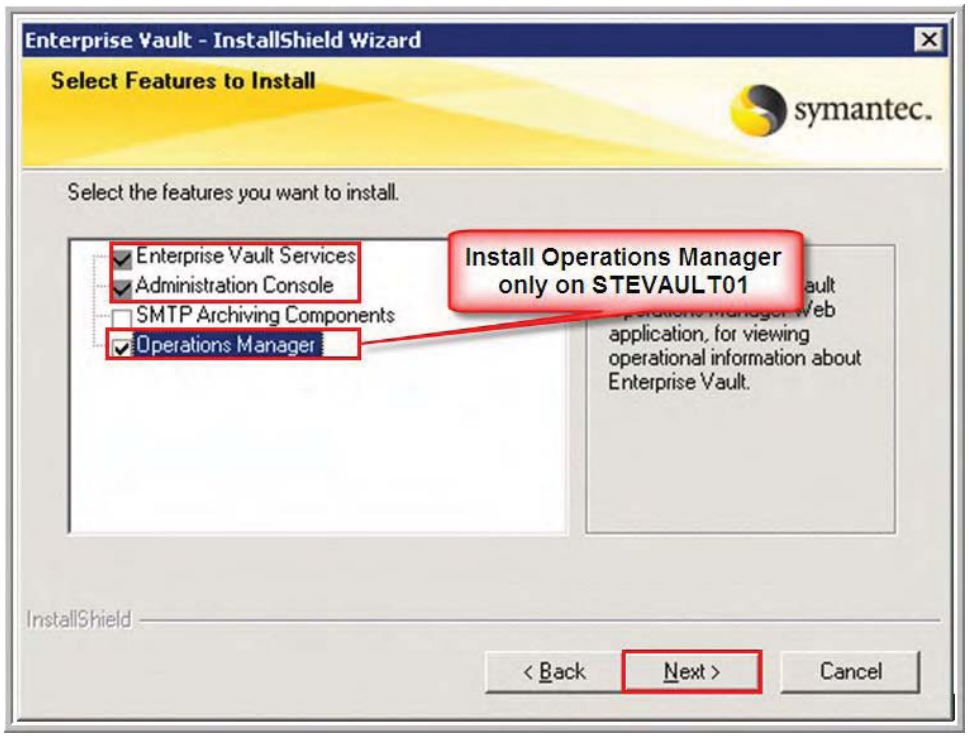
Enterprise Vault Mailbox Installation and Configuration

NOTE: Complete these steps on Enterprise Vault servers, STEVAULT01 and STEVAULT02.

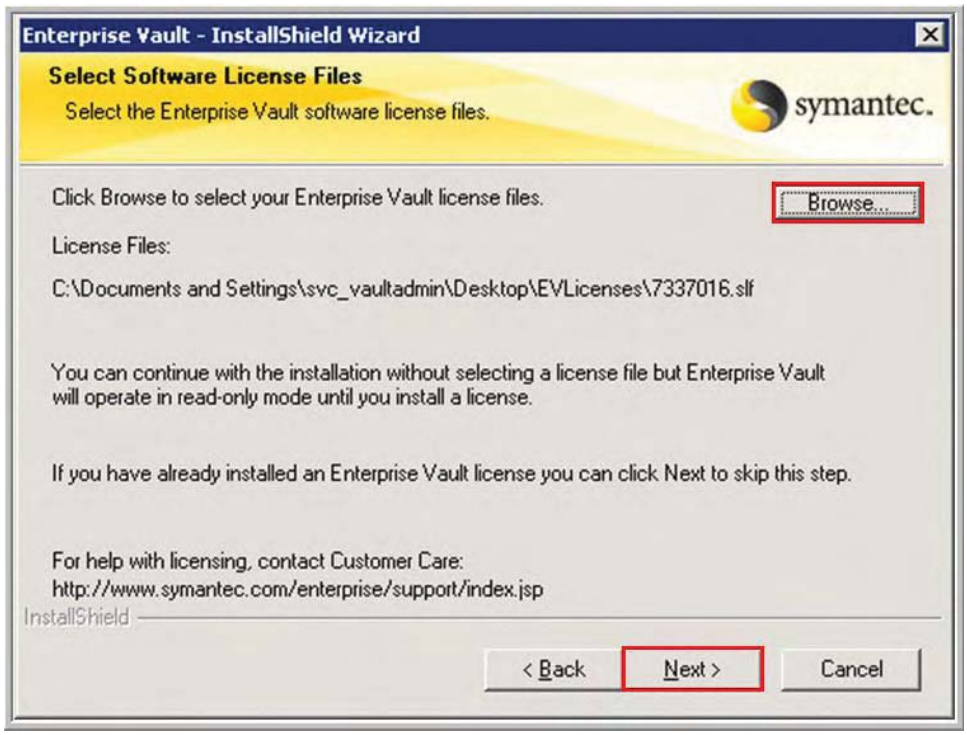
Run setup.exe for Enterprise Vault 2007 (Version 7.5) and keep the default install location unless there is an application partition you can use and then click on Next.

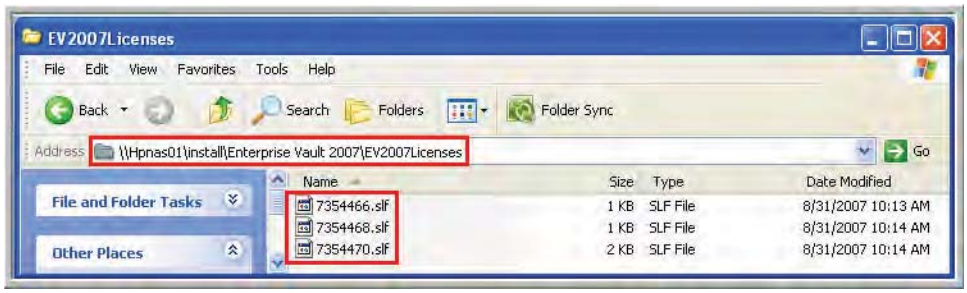


Install Enterprise Vault Services, Administration Console and Operations Manager. Only install Operations Manager on STEVAULT01, not on STEVAULT02.

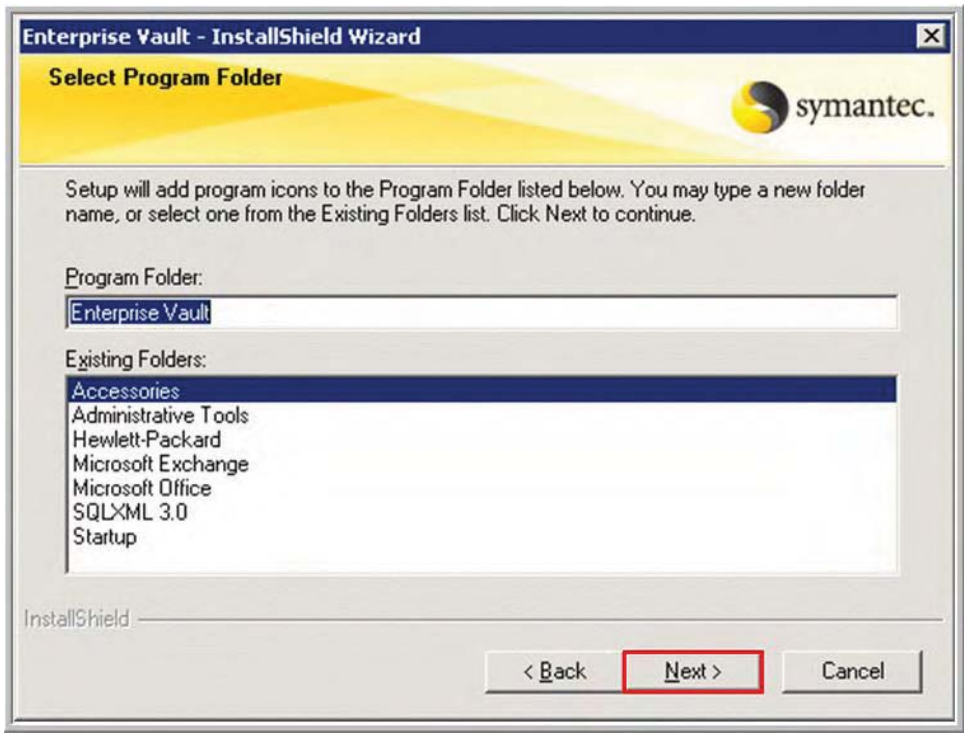


Browse to the Enterprise Vault 2007 licenses and copy over the .SLF files. Click on Next.

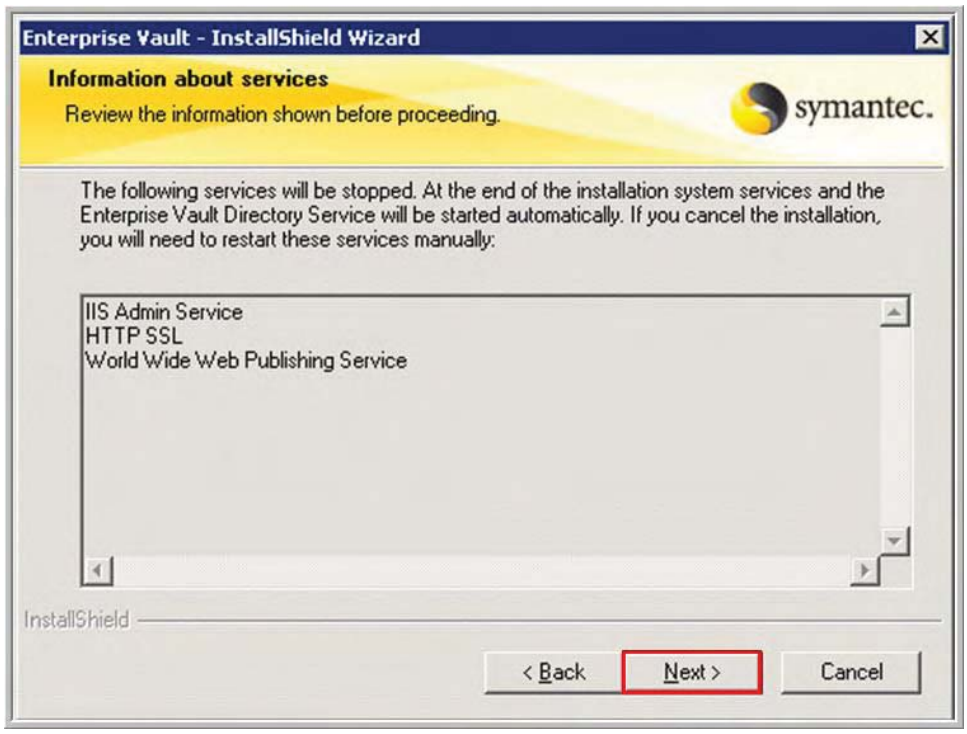




Accept the defaults and click on Next.



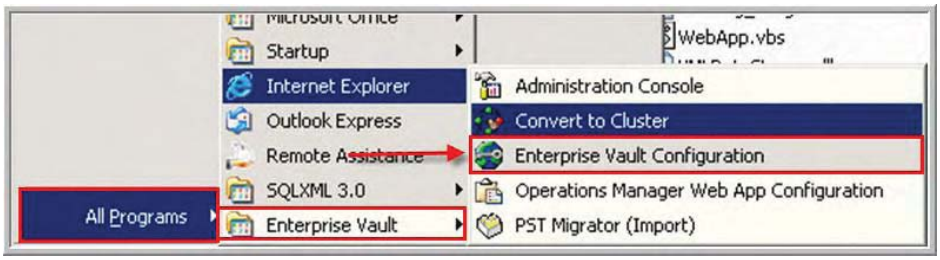
Click on Next for the services to be restarted.



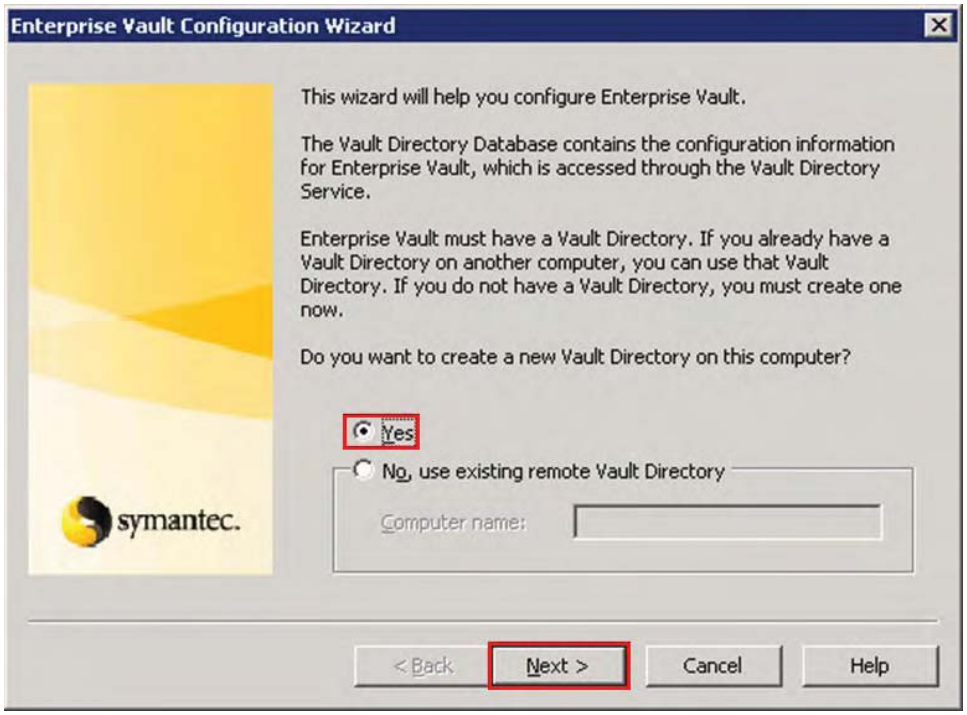
Uncheck show information on configuring installed components and then click on Finish to complete the installation.

Complete the Site Configuration

Go to Start > All Programs > Enterprise Vault > Enterprise Vault Configuration.

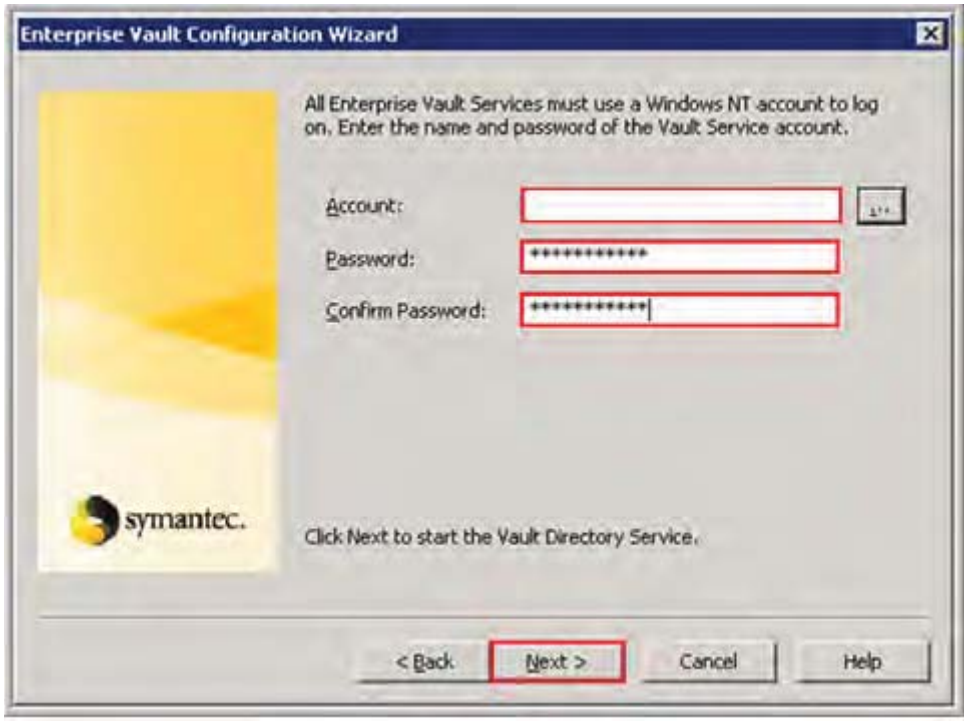


Click on Yes and then Next to create a new Vault Directory. Note on STEVAULTS02 you would join the existing site already created and enter “EV” for this site and then select the SEG Site on the next screen.



Install it in English and click on Next.

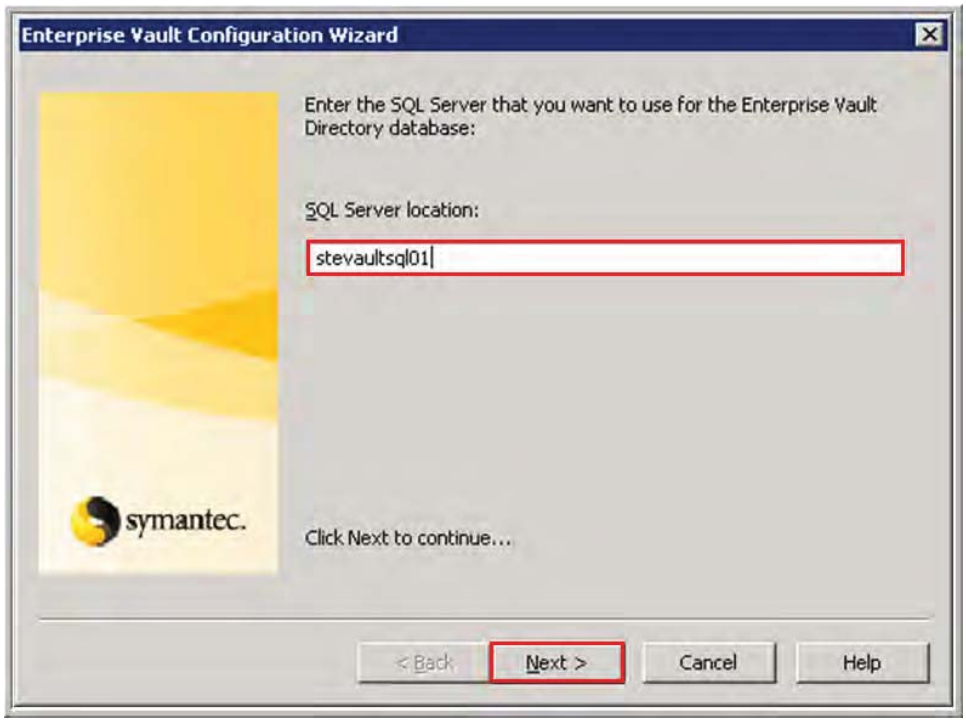
Enter the VaultAdmin account name and password and click on Next.



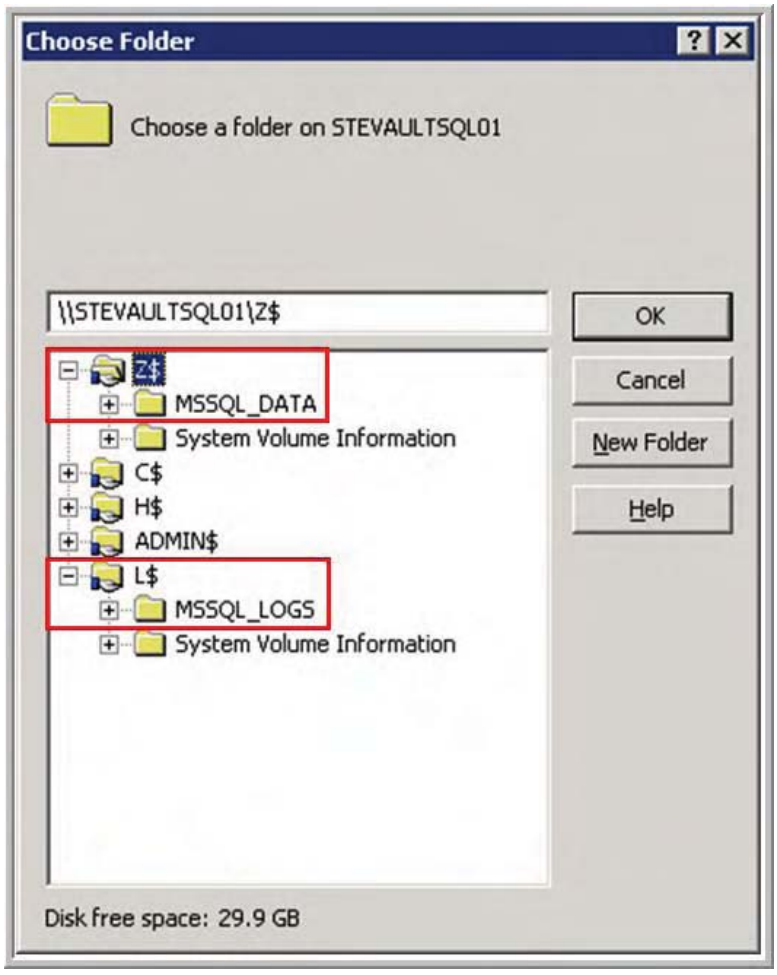
Click on OK on the screen notifying of the rights granted.

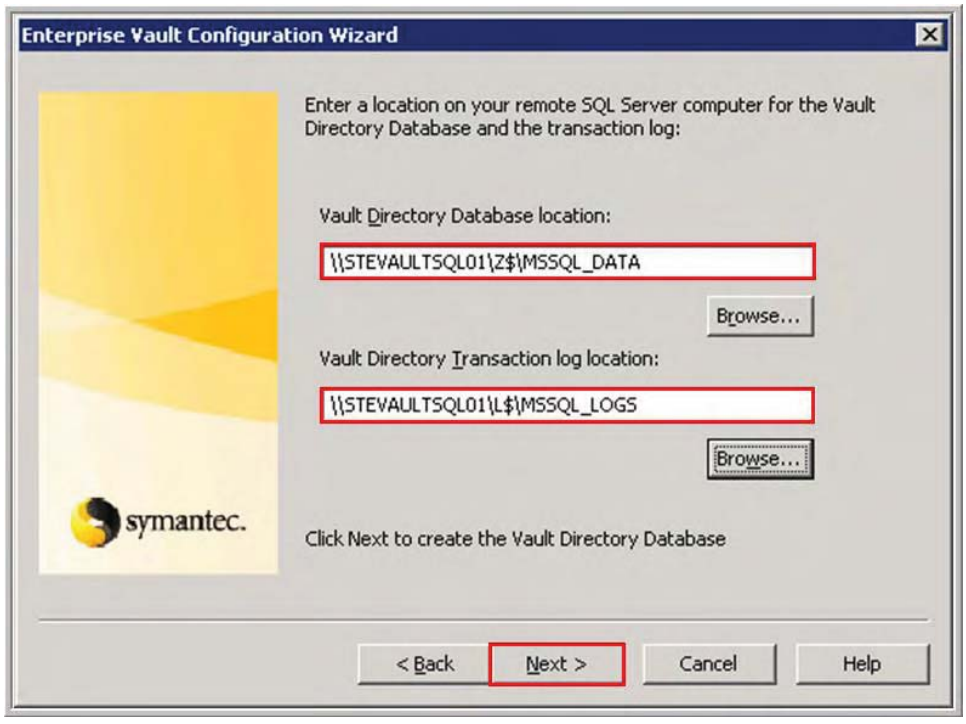


Enter the SQL server information, STEVAULTSQL01, and then click on Next.

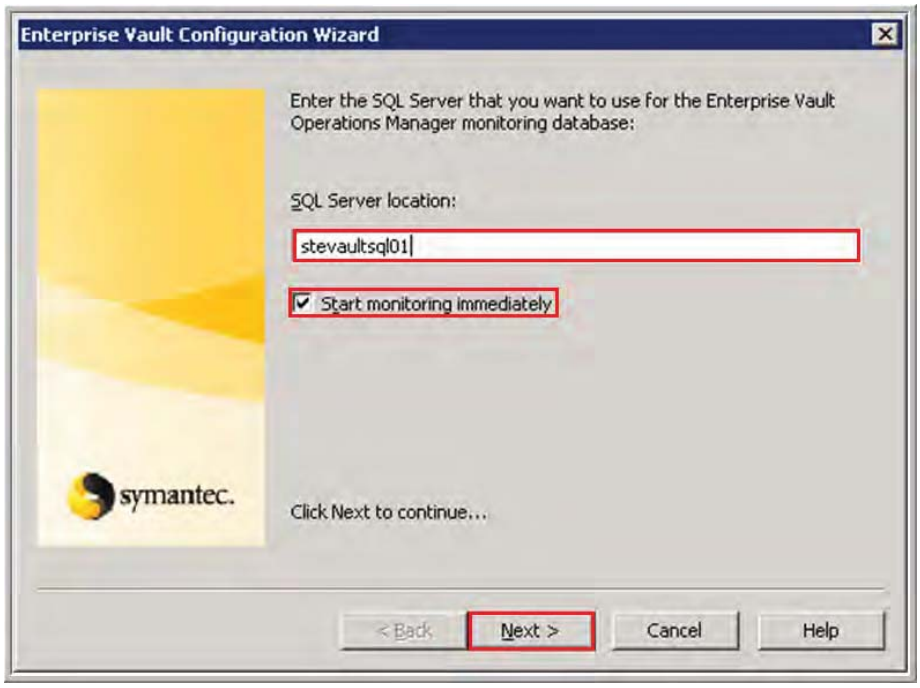


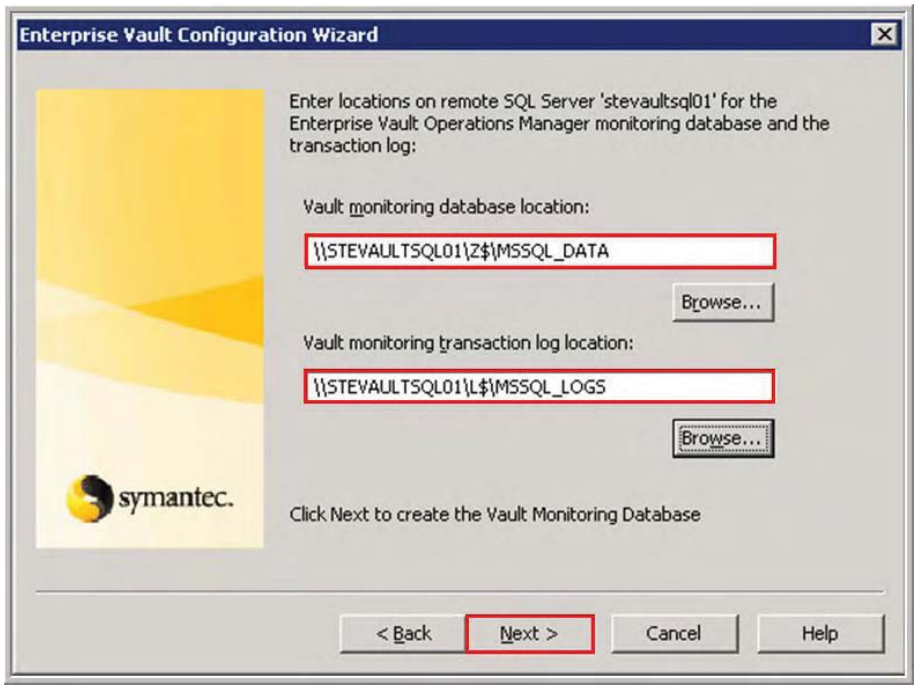
Choose the SQL folders that were created during the SQL installation and click on OK and then Next.


Choose Folder
Choose a folder on STEVAULTSQL01
\\STEVAULTSQL01\Z$
OK
Cancel
New Folder
Help
Z$
MSSQL_DATA
System Volume Information
C$
H$
ADMIN$
L$
MSSQL_LOGS
System Volume Information
Disk free space: 29.9 GB

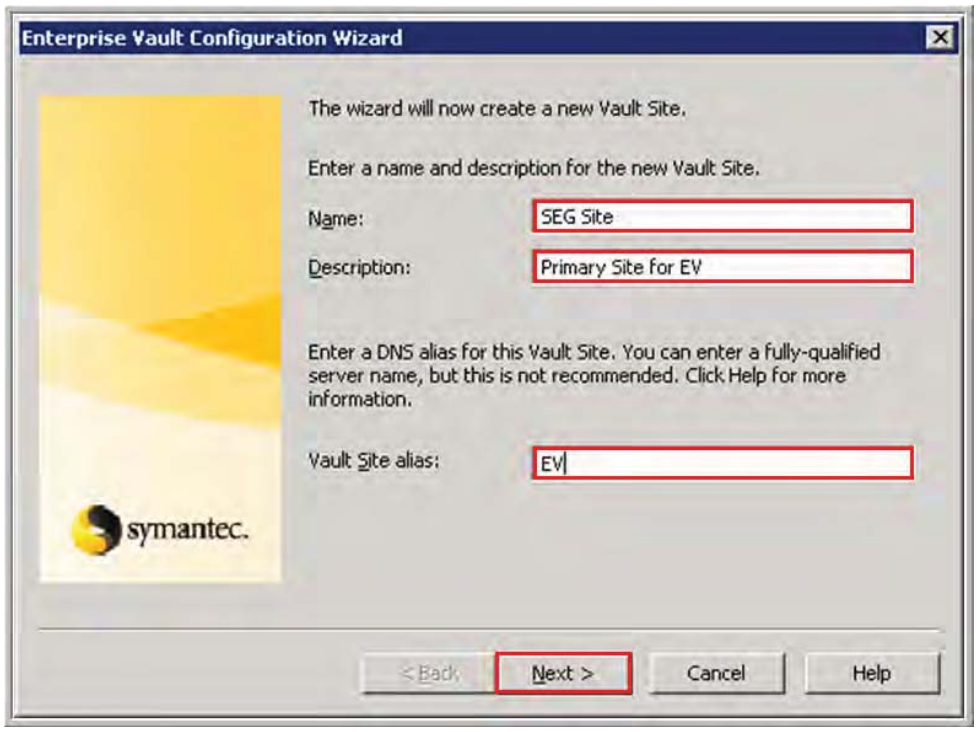

Enterprise Vault Configuration Wizard
Enter a location on your remote SQL Server computer for the Vault Directory Database and the transaction log:
Vault Directory Database location:
\\STEVAULTSQL01\Z$\MSSQL_DATA
Browse...
Vault Directory Transaction log location:
\\STEVAULTSQL01\L$\MSSQL_LOGS
Browse...
symantec.
Click Next to create the Vault Directory Database
< Back
Next >
Cancel
Help

For monitoring configuration enter the SQL server and select the locations created during the SQL installation.

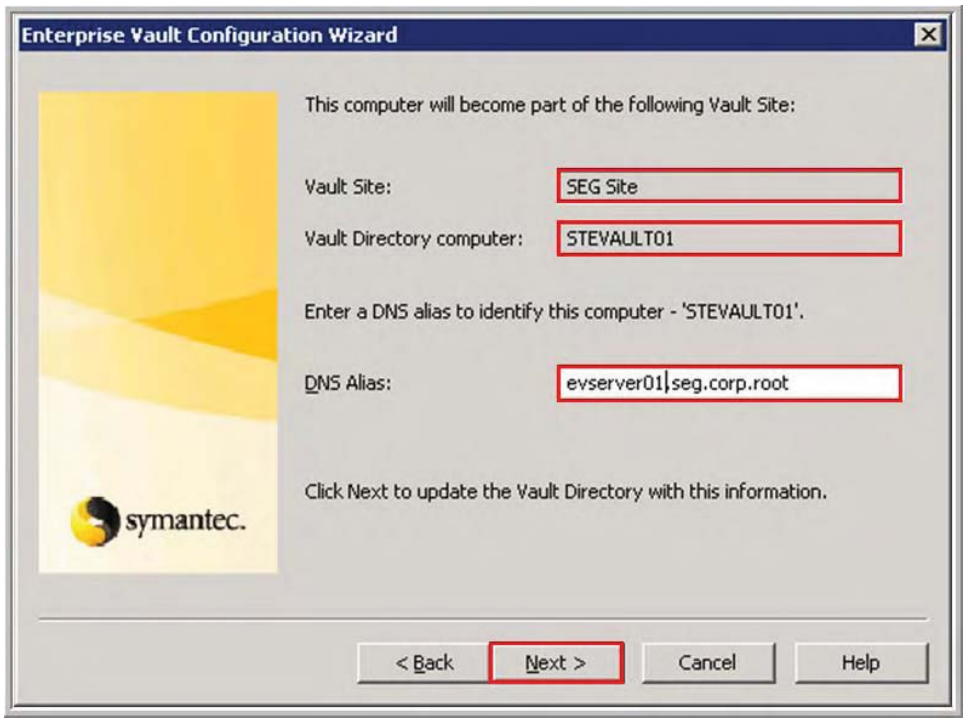




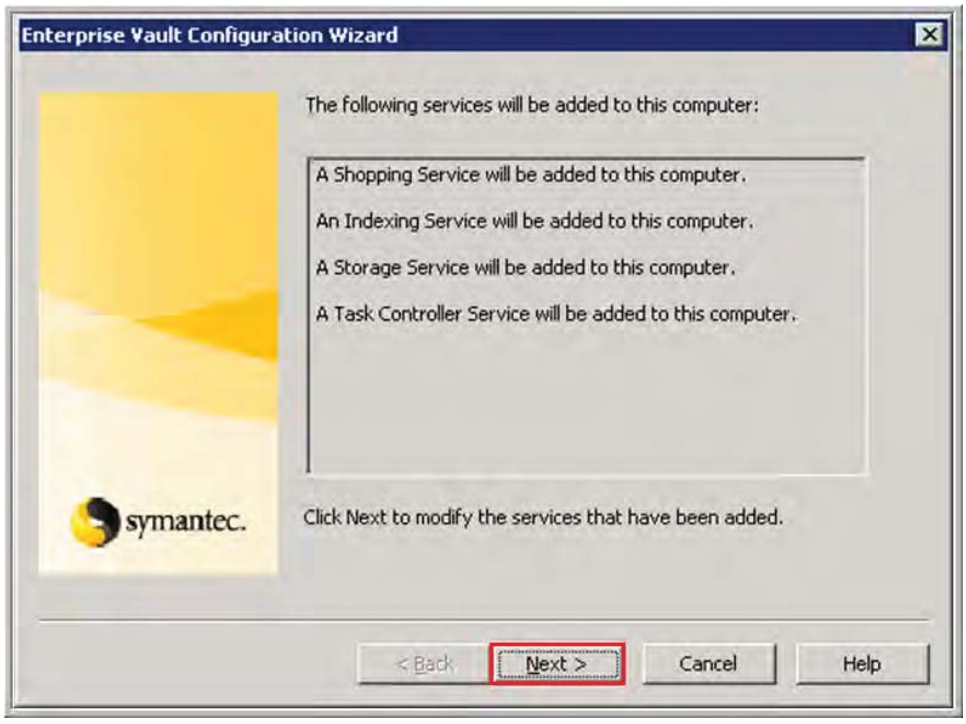
Enter the site name “SEG Site” for the company and the description “Primary Site for EV” and enter the vault site alias as EV.



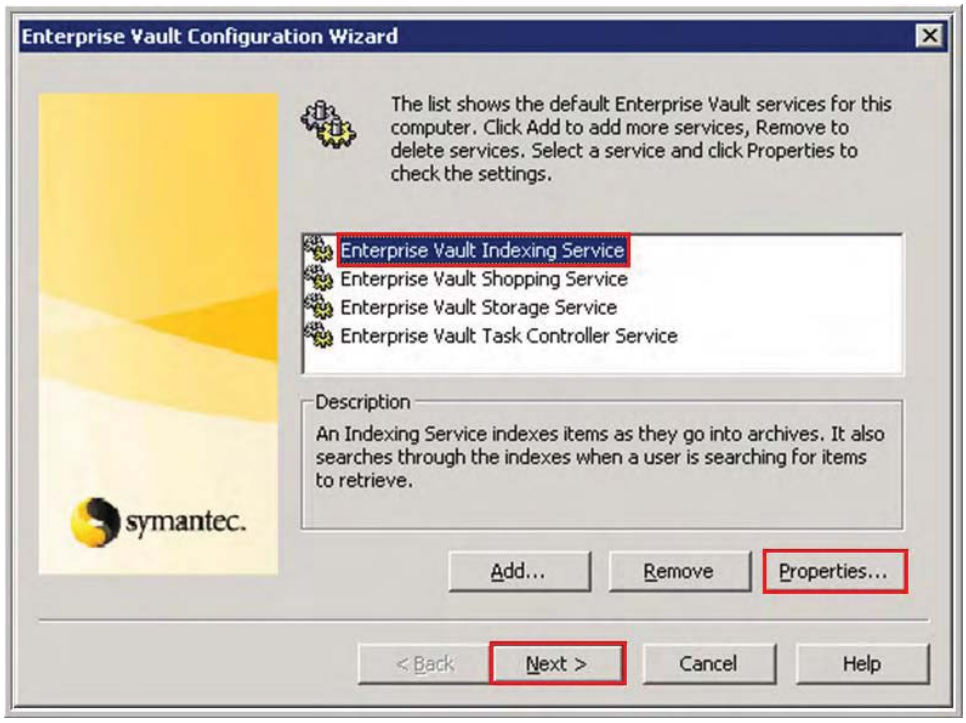
Confirm that the Vault Site shows “SEG Site” and that the Vault Directory computer is STEVAULT01. Enter the DNS alias for the computer, evserver01.seg.corp.root, or whatever EV server you are managing. So for STEVAULT02 enter evserver02.seg.corp.root.

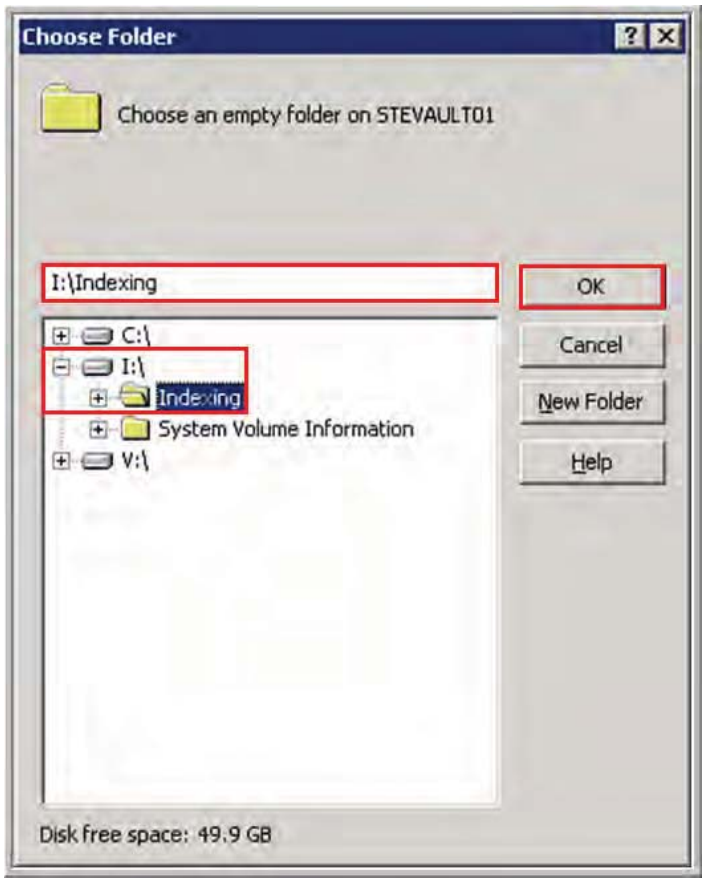


Click on Next at the screen confirming the services added. For other Enterprise Vault configurations that you did not create a new site in, i.e. STEVAULT02, you will need to Add the Index and Storage service by clicking on the Add button.

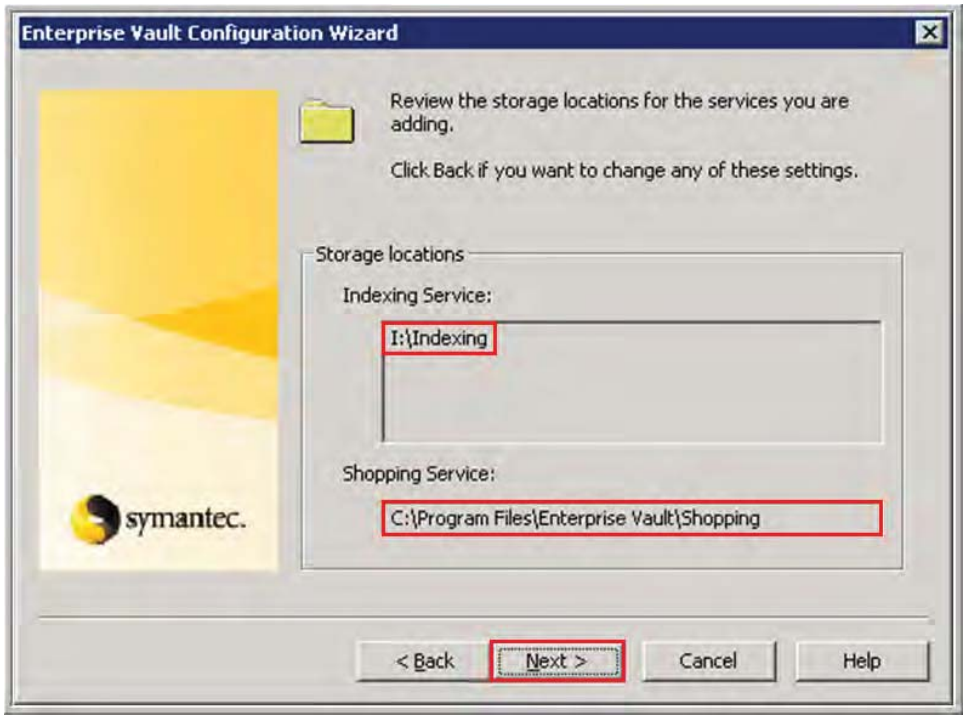


Highlight the Enterprise Vault Indexing Service and select Properties and click on the Indexing Locations tab and change the Index location to I:\Index. Hit OK and Next to continue the configuration. Be sure to change this on other Enterprise Vault services as well.

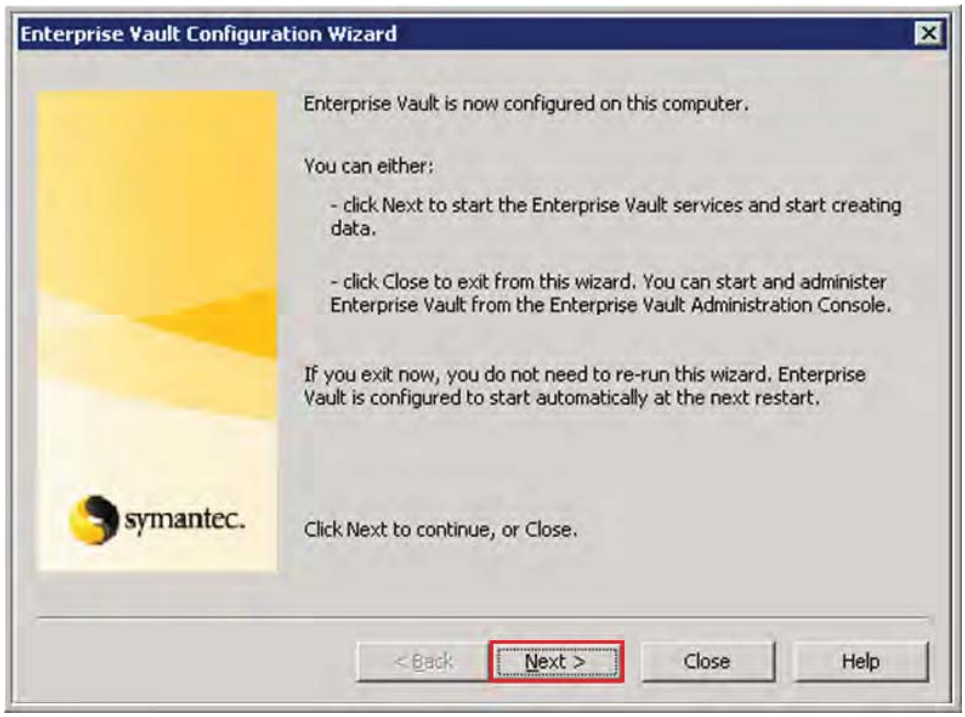




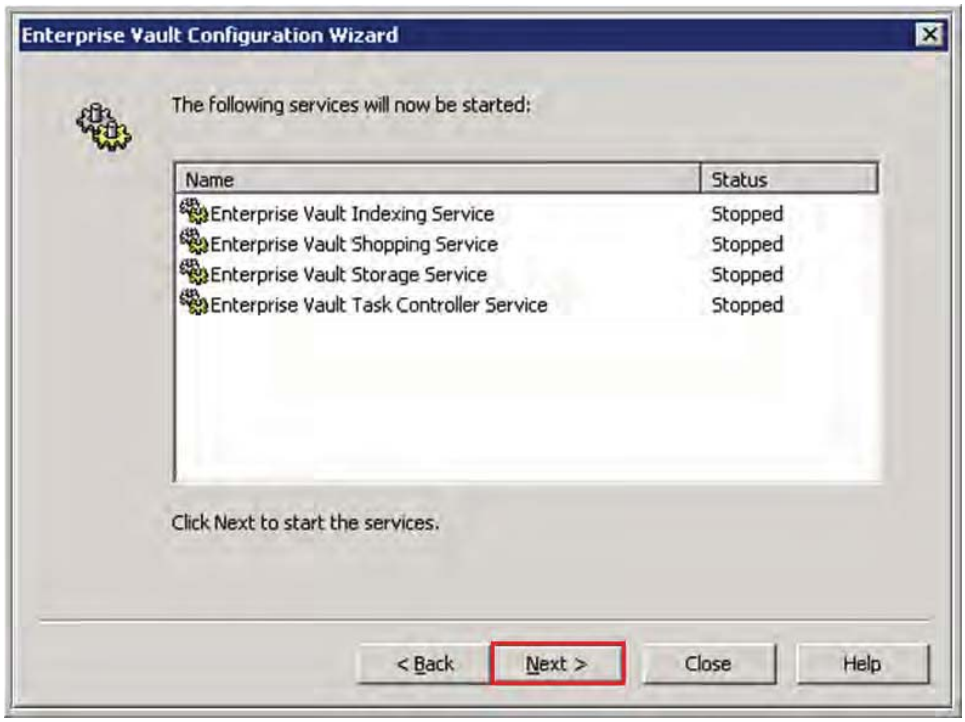
Confirm the storage locations and click on Next.



Click on Next to confirm the configuration.

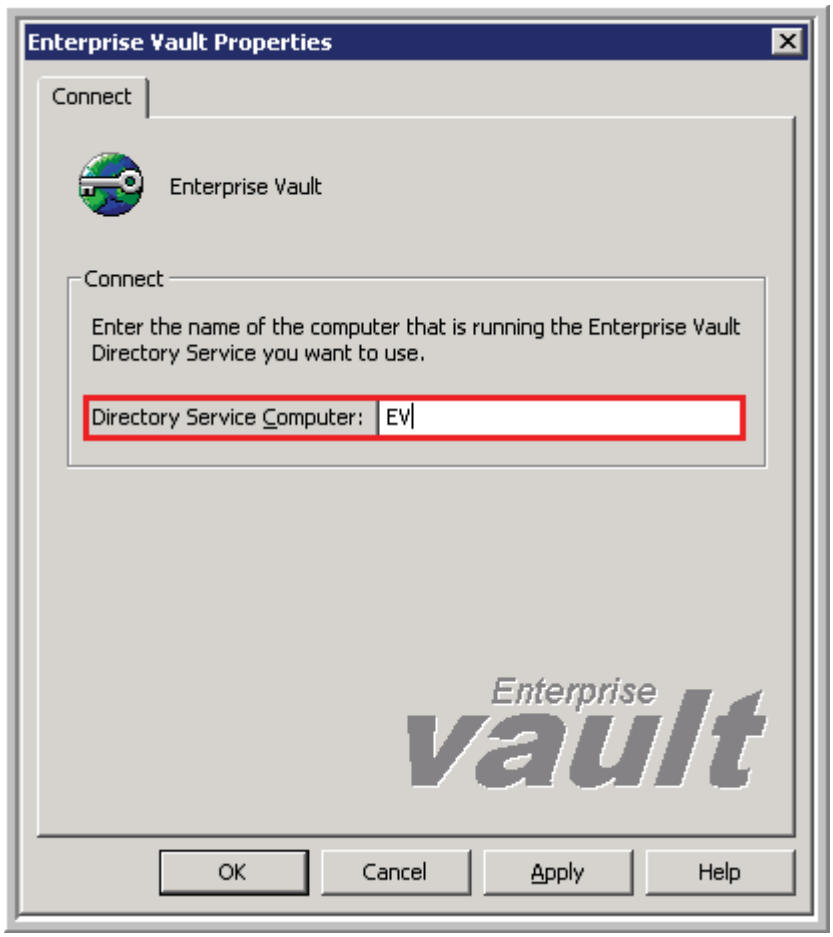


Click on Next and then Finish.





To begin administering Enterprise Vault launch the Administration Console and enter “EV” in Directory Services Computer.



Configure the Vaults and Partitions

Refer to the table for the Vault stores that will be created for archive storage. Note that Public Folder, File System and Sharepoint stores will be created at a later date.

Vault Store one: EV1 Mailbox Archiving - SEGMailbox

Includes all Mailbox Archives for the company

Vault Store two: EV1 Mailbox Archiving – PARMailbox

Includes all Mailbox Archives for the parent company

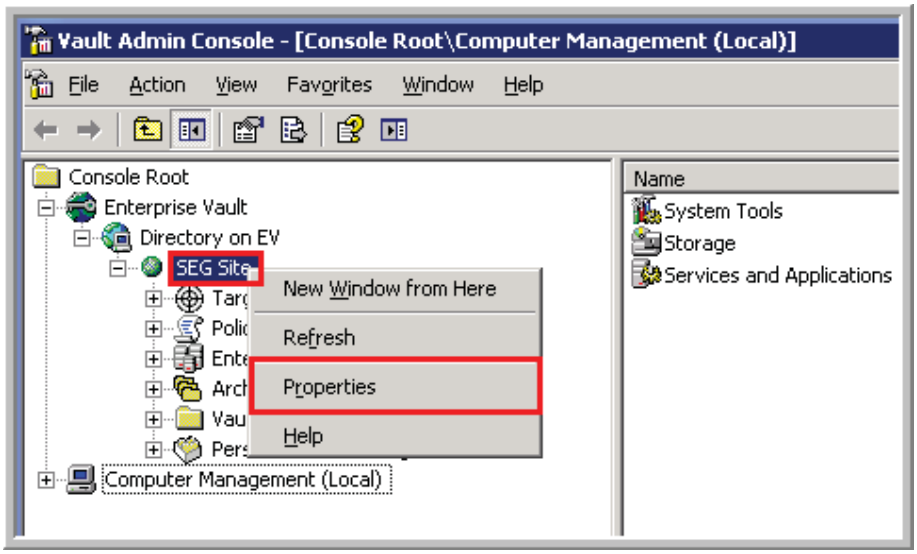
Vault Store three: EV2 Journaling – Company Journals

Includes all Journaling Archives for the company

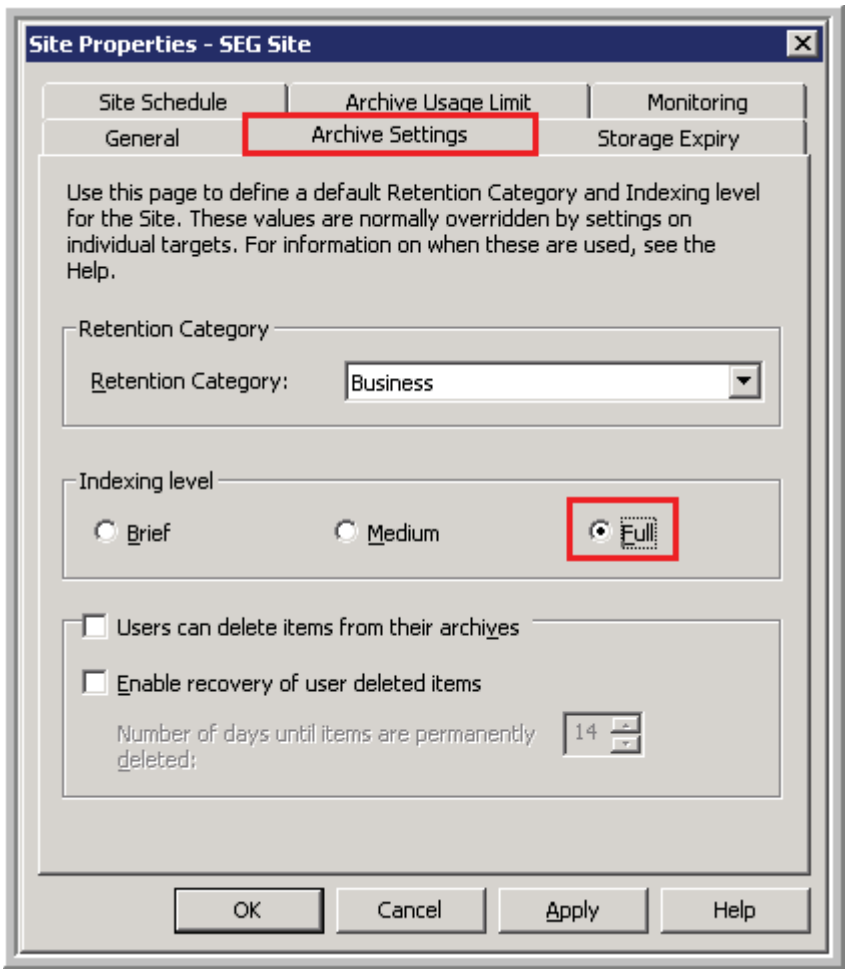
Vault Store three: EV2 Journaling – Parent Company Journals

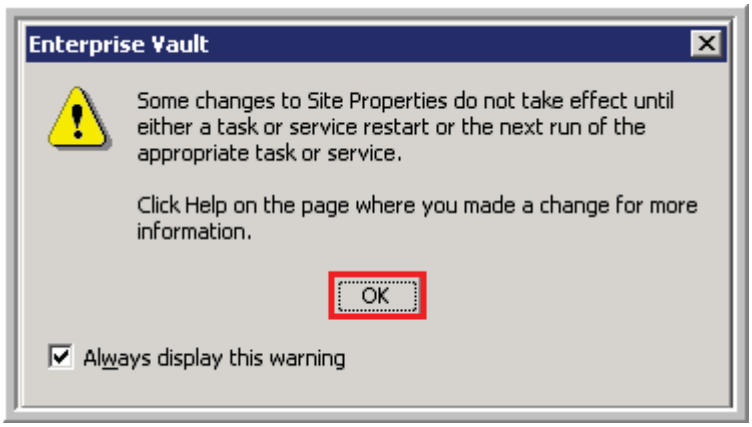
Includes all Journaling Archives for the Parent Company

Open up the Enterprise Vault Administrator console and expand the Directory on EV and right click on the SEG Site and select Properties.

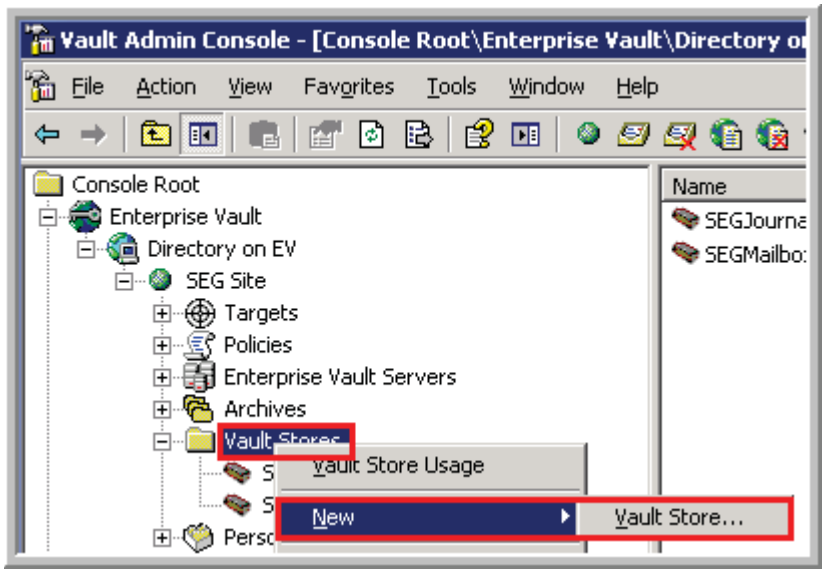


Click on the Archive Settings tab and select Full for the Indexing Level. Click on OK when the warning comes up and then OK again to close the site settings.

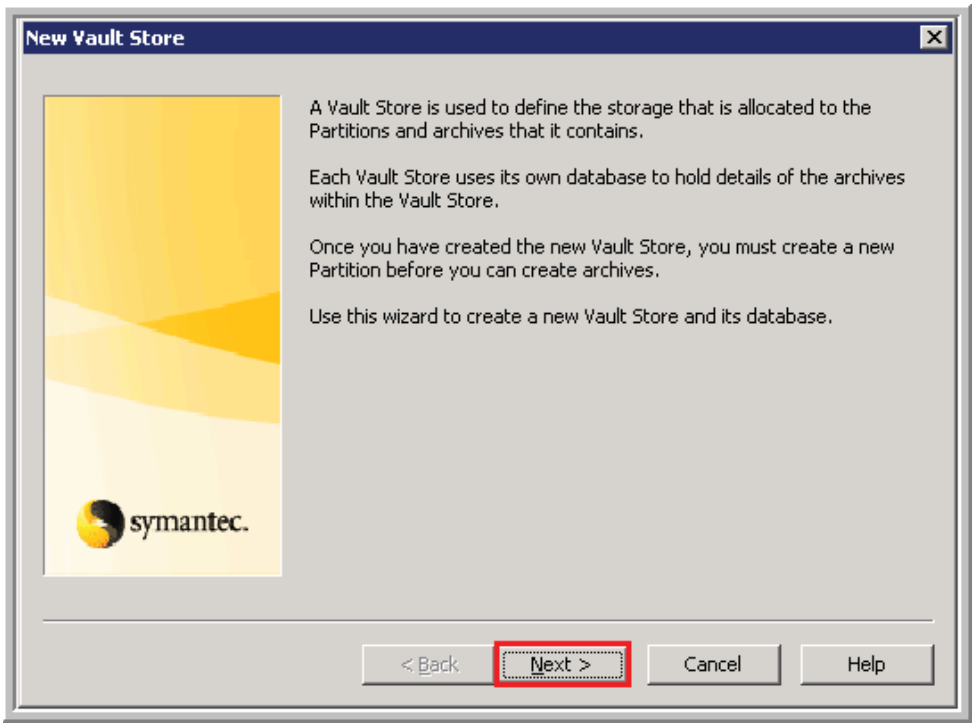




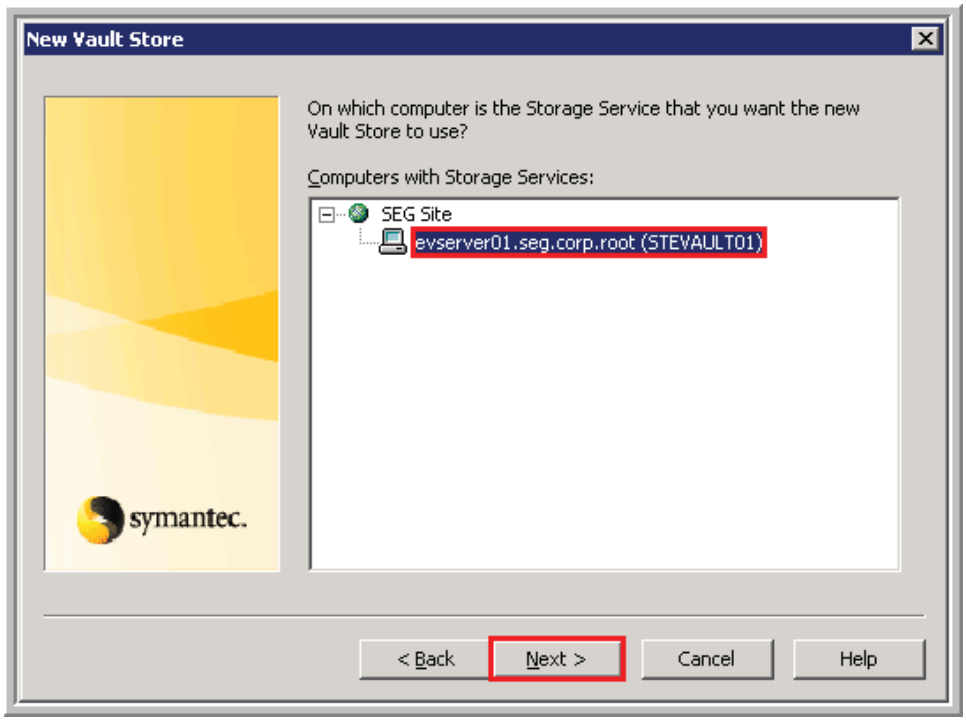
Create a vault store for STEVAULT01 for mailbox archiving and a vault store on STEVAULT02 for journaling. Open up the SEG Site and right click on Vault Stores and select New > Vault Store.



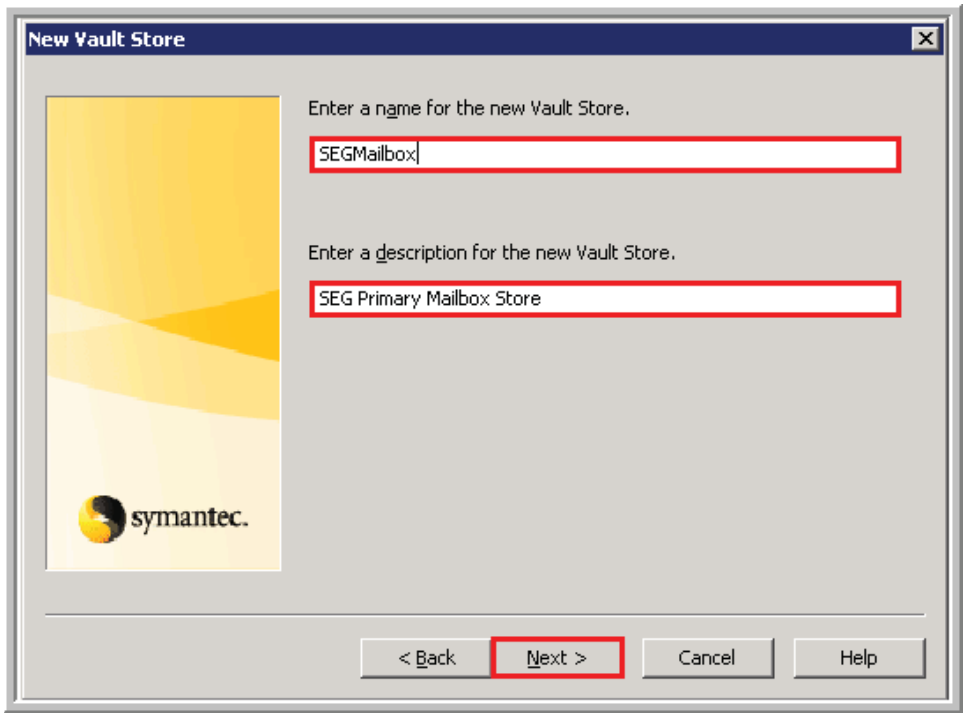
Click on Next.



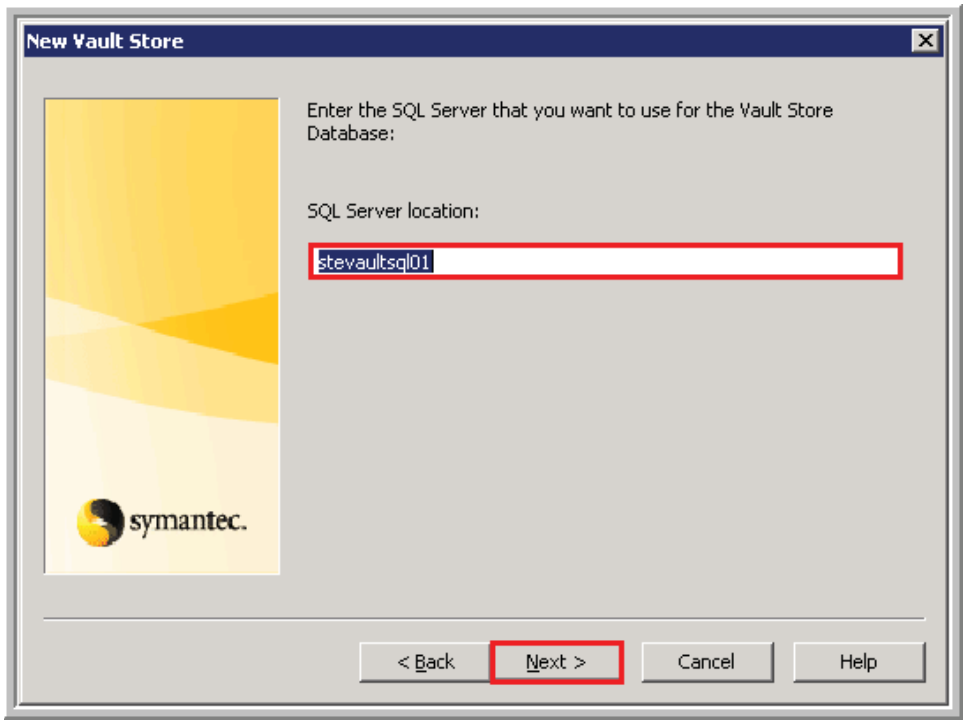
Select the server you are using the storage service on – evserver01 for the SEGMailbox store and evserver02 for SEGJournal store.



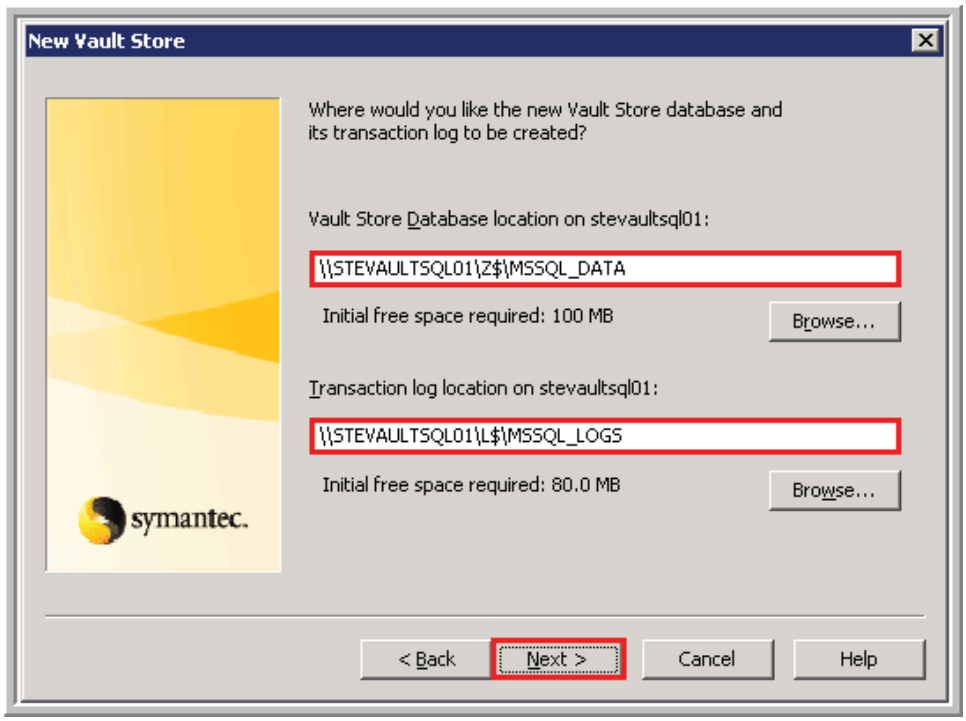
Enter the name for the new vault store, SEGMailbox for evserver01, which will be used for all end user mailboxes and SEGJournal for evserver02, which will be used for journaling of all mail. Enter the description SEG Primary Mailbox Store for the mail vault and SEG Journal Vault Store for the journal vault.



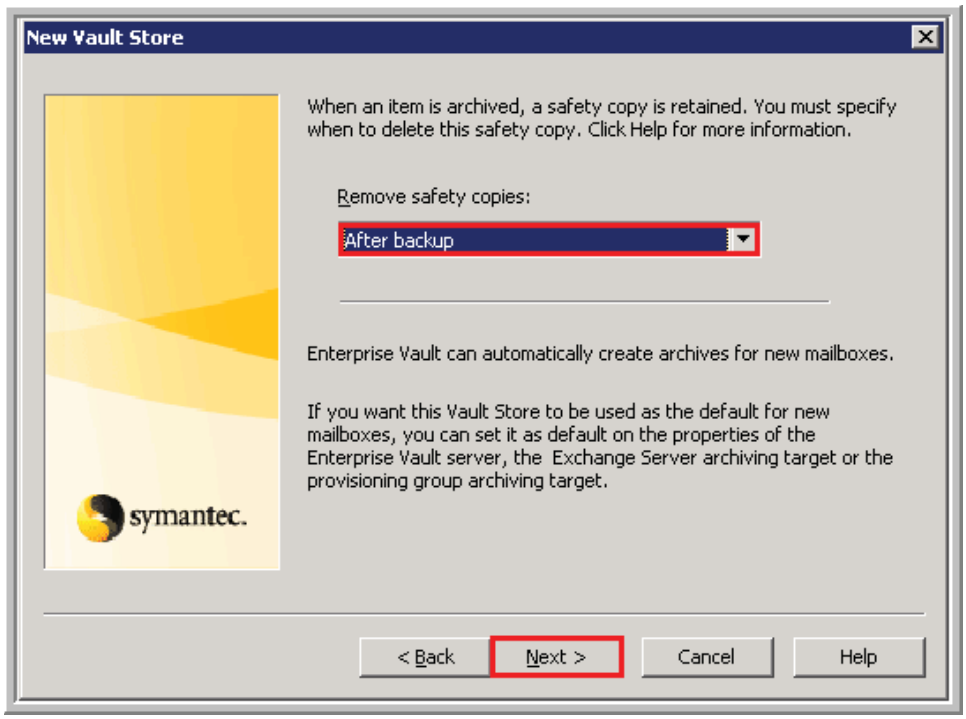
Enter the SQL Server name which is the same for all Enterprise Vault servers.



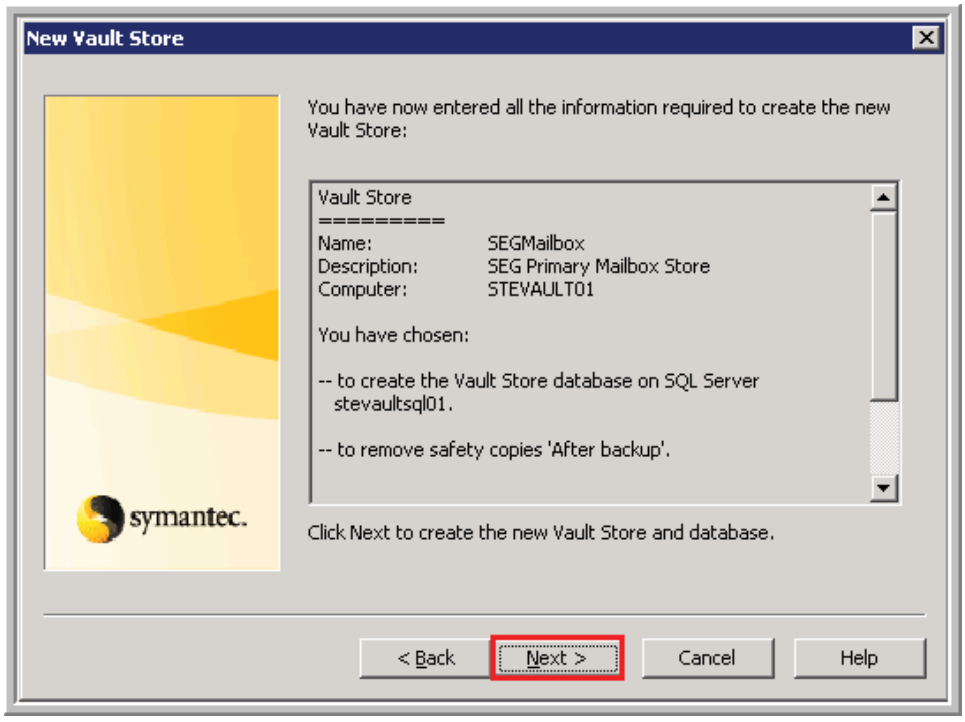
Enter the database and log location created during the SQL installation - see screenshot below.



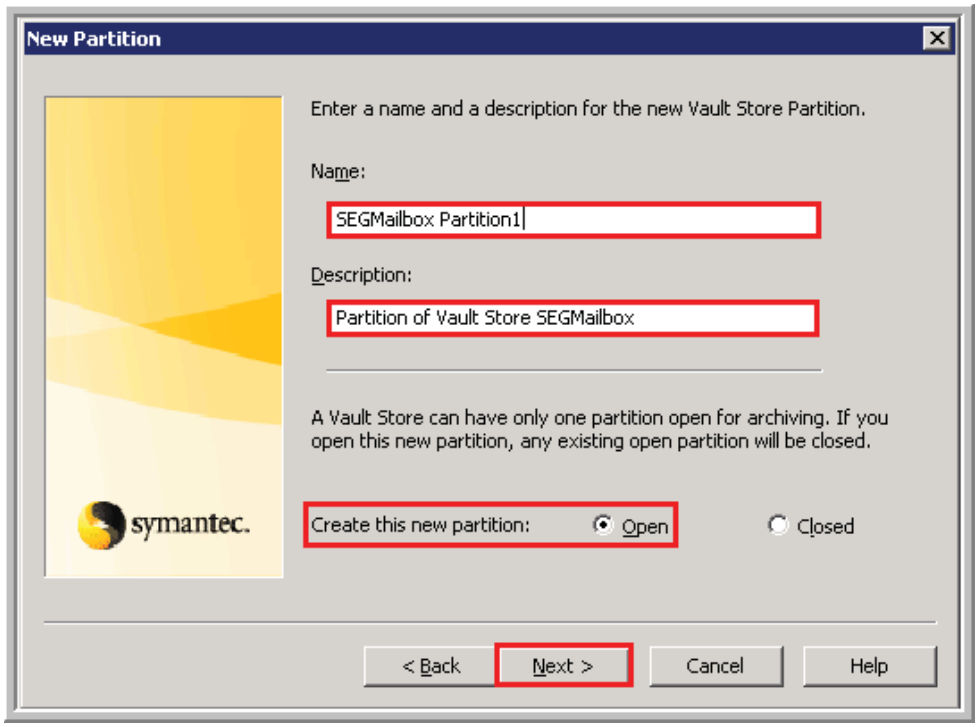
For Remove Safety Copies select After Backup for SEGMailbox and After Backup (immediate for journaling) for SEGJournal. The after backup setting means that a shortcut will not be created for the email in the end users inbox until the backup job completes at night and resets the archive bit of the .dvs file.



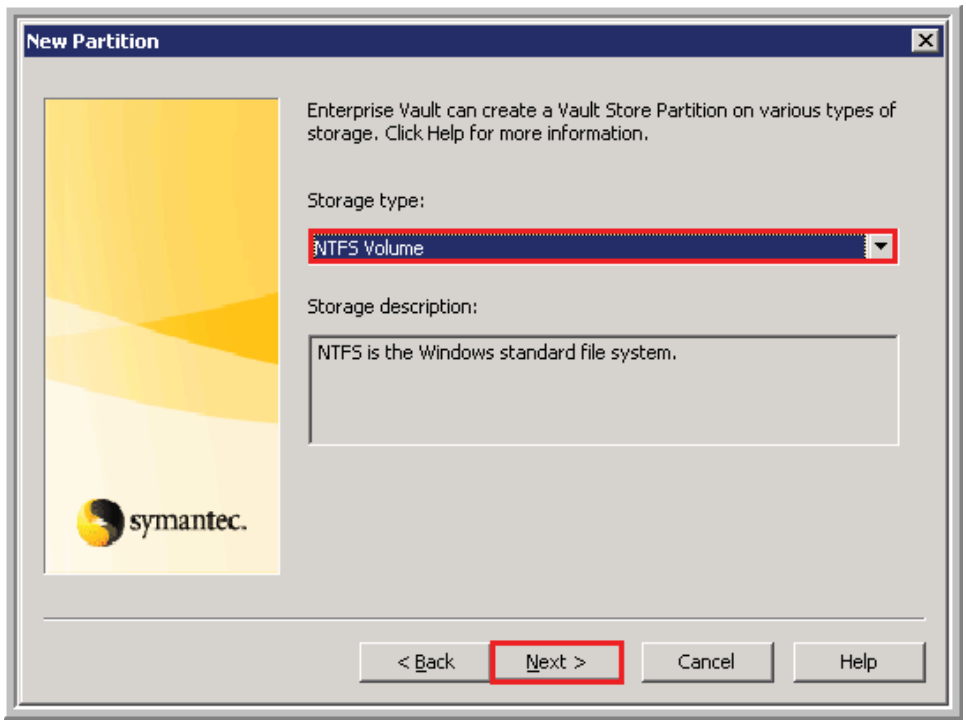
Confirm the settings and click on Next and then Next on the following two screens to configure the partition for the new Vault Store.



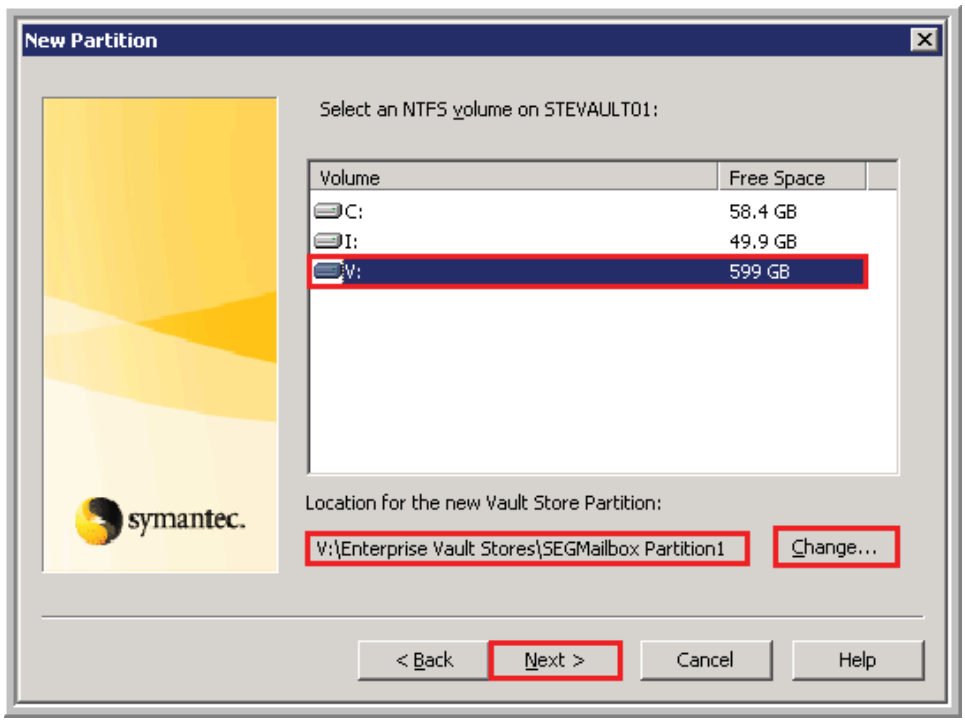
Enter the name for the partition, either SEGMailbox Partition1 or SEGJournal Partition1. Enter the description below for either the mailbox or the journal partition. Confirm that the partition is Open.



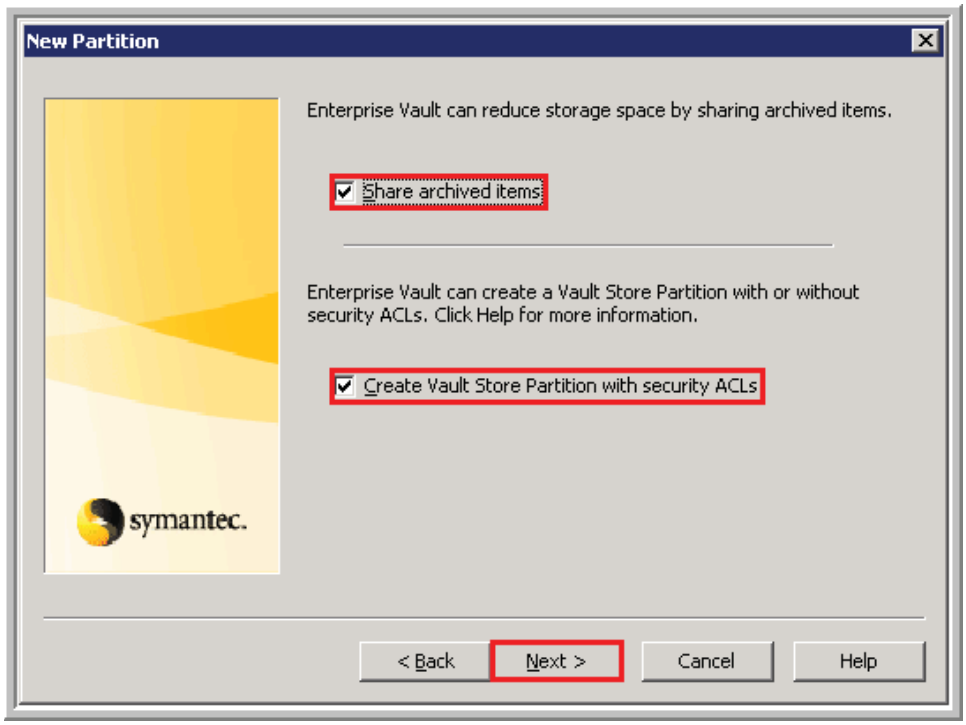
Select NTFS Volume for the Storage type and then Next.



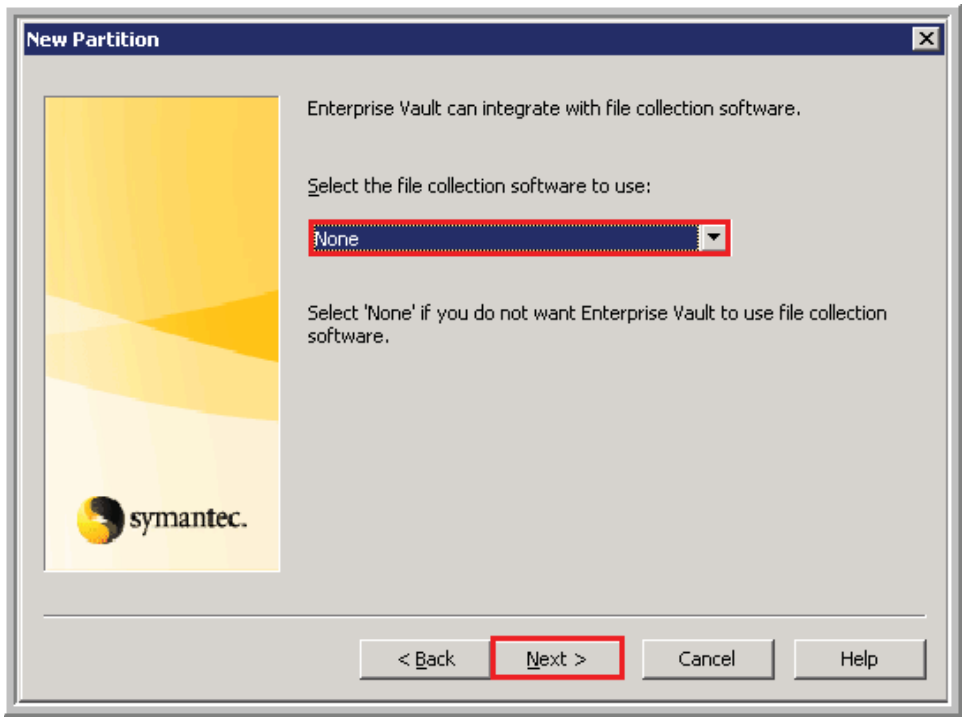
Click on Change and select the V directory to store the partition on.



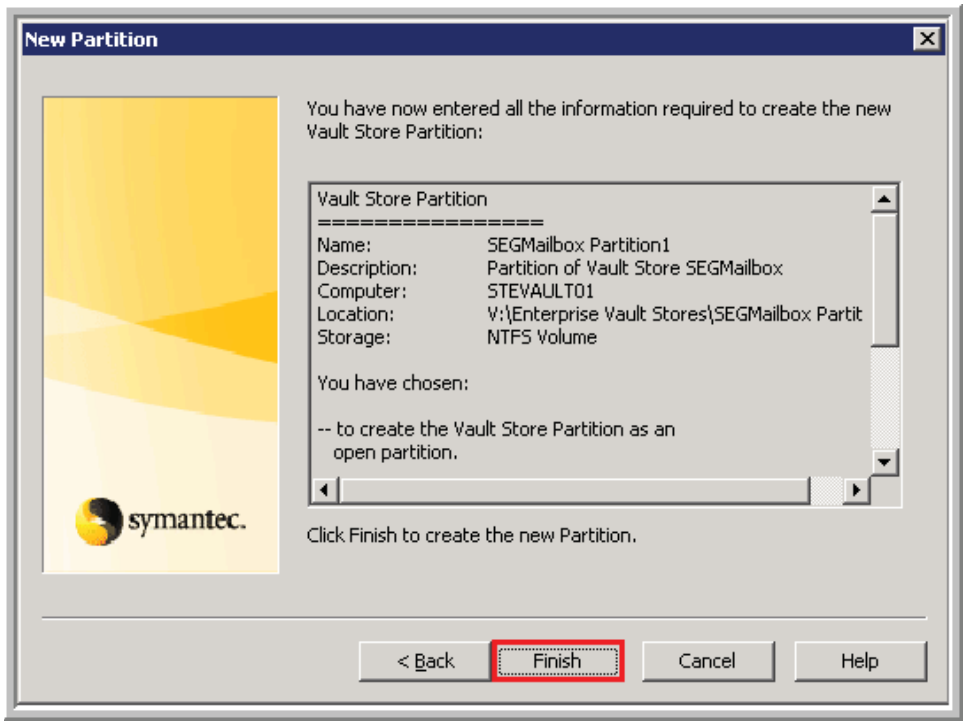
Confirm that Share archived items and Create Vault Store Partition with security ACLs and then click on Next.



Select None for the collection software and then click on Next.

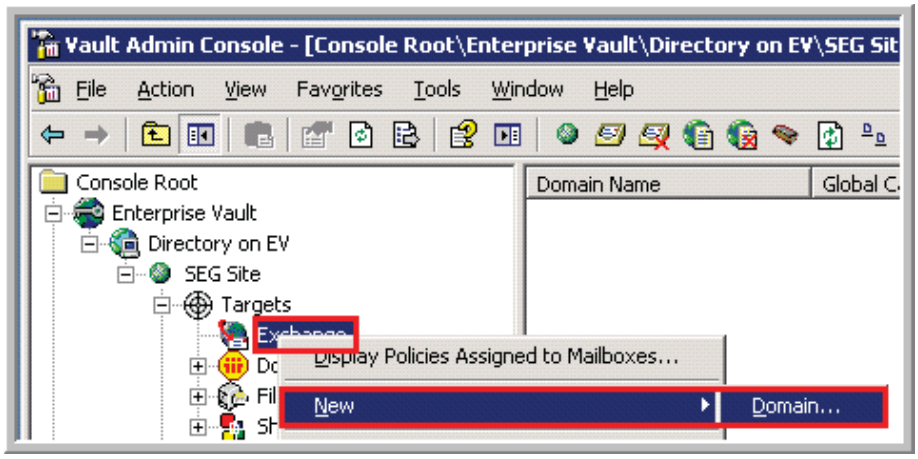


Confirm the settings and click on Finish and then Close on the final confirmation window.

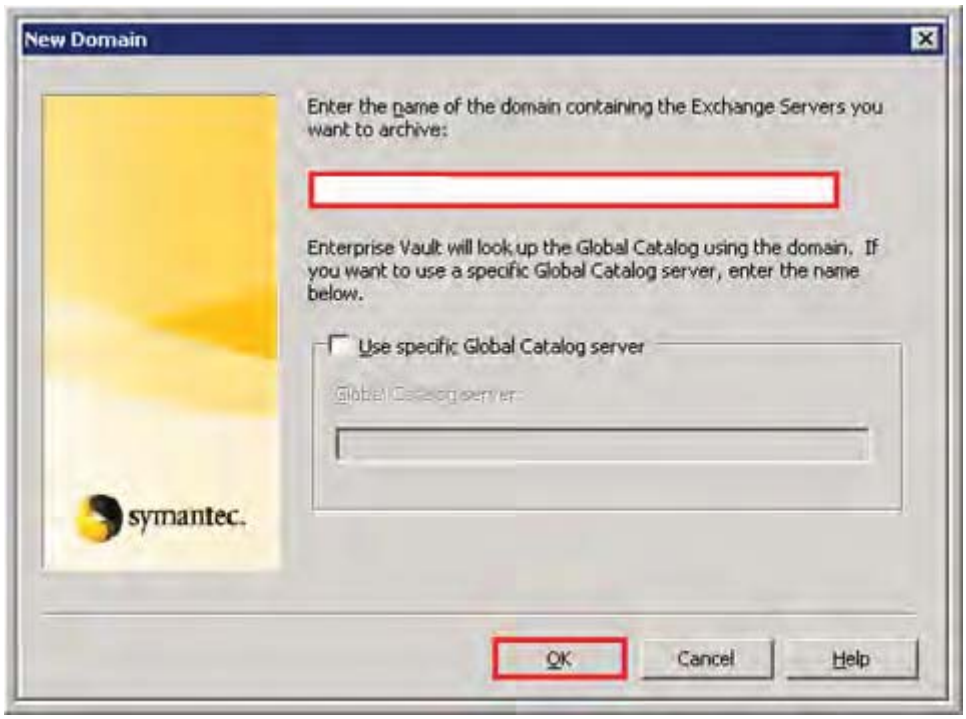


Configure the Target and Exchange Server

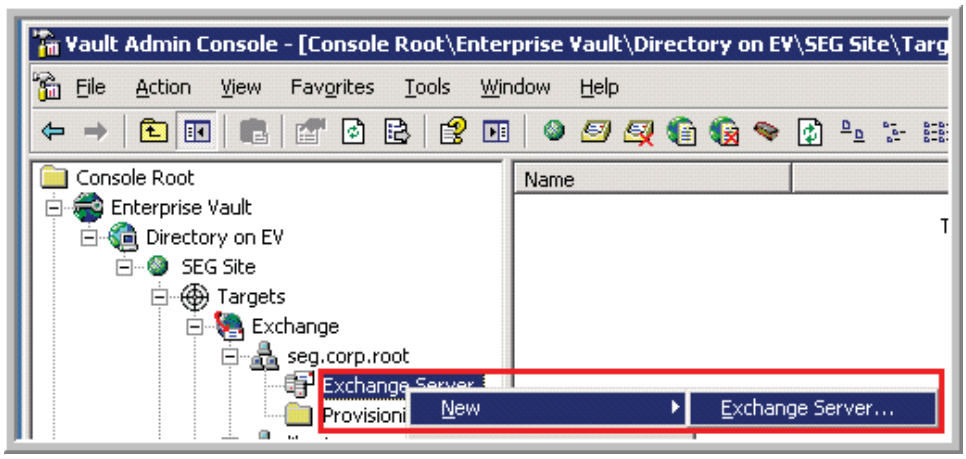
Expand the SEG Site > Targets and right click on Exchange and select New > Domain.



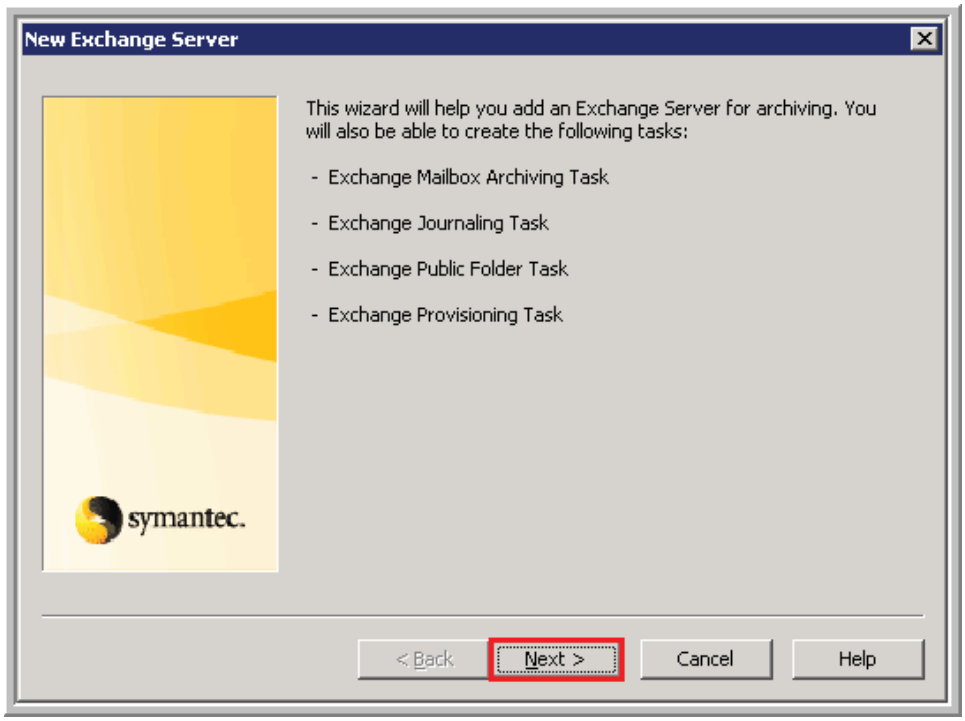
Enter the domain of the Exchange servers we are managing for the company and parent company.



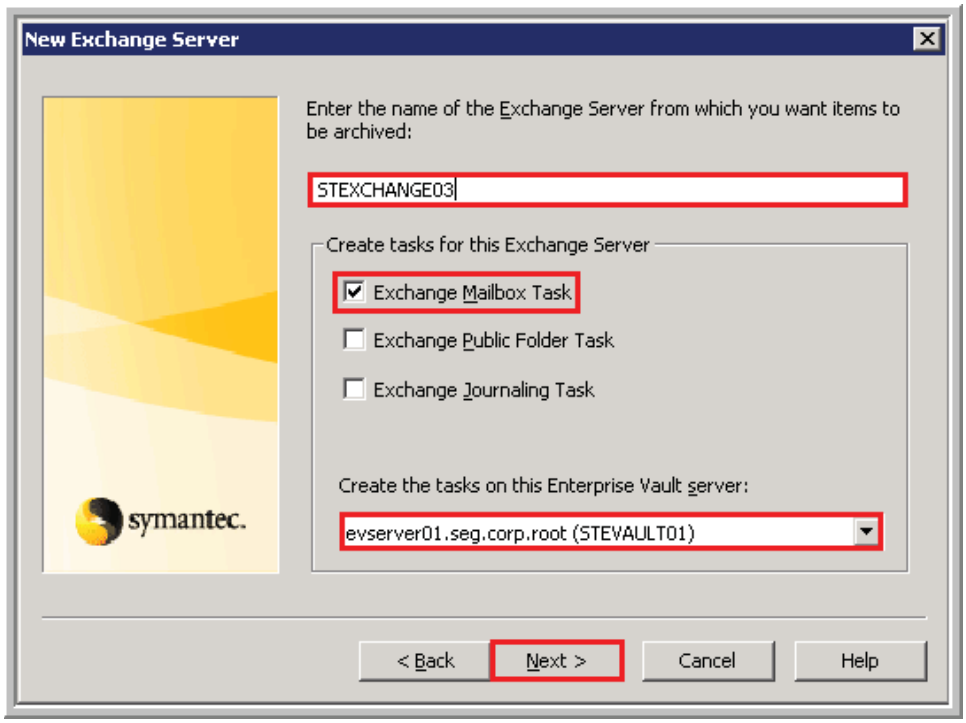
Expand the new domains added to the site and right click on Exchange Server and click on New > Exchange Server.



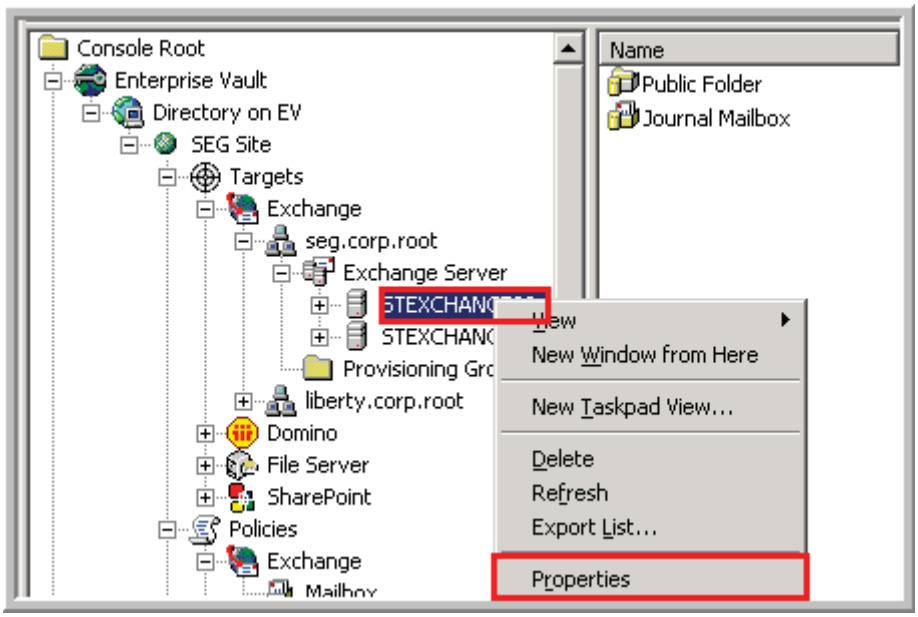
Click on Next



Enter the Exchange Server and check Exchange Mailbox Task and select the proper Enterprise Vault Server. STEVAULT01, STEVAULT02, EAGLE1 and EAGLE2 will all be servers exchange servers added. EAGLE1 and EAGLE2 will be added to the parent company's domain. Click on Next and complete the configuration.

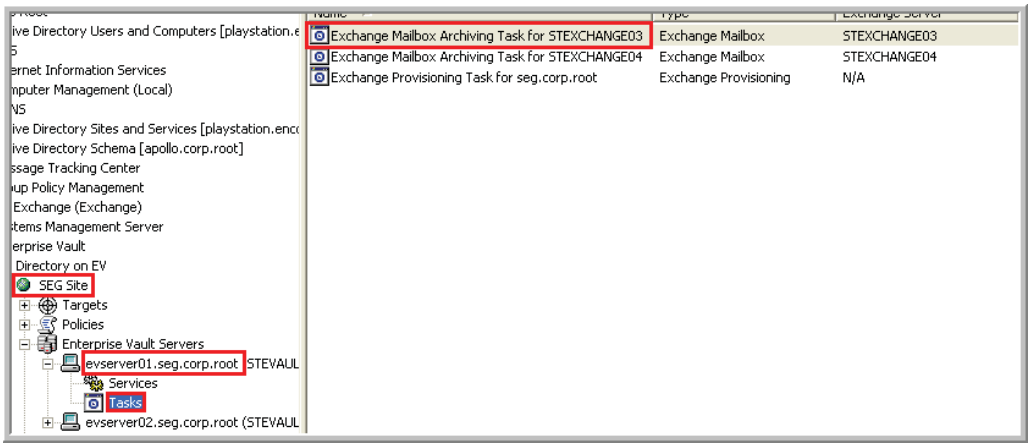


Next setup the default for archiving by browsing to the server and right clicking on it and selecting properties.

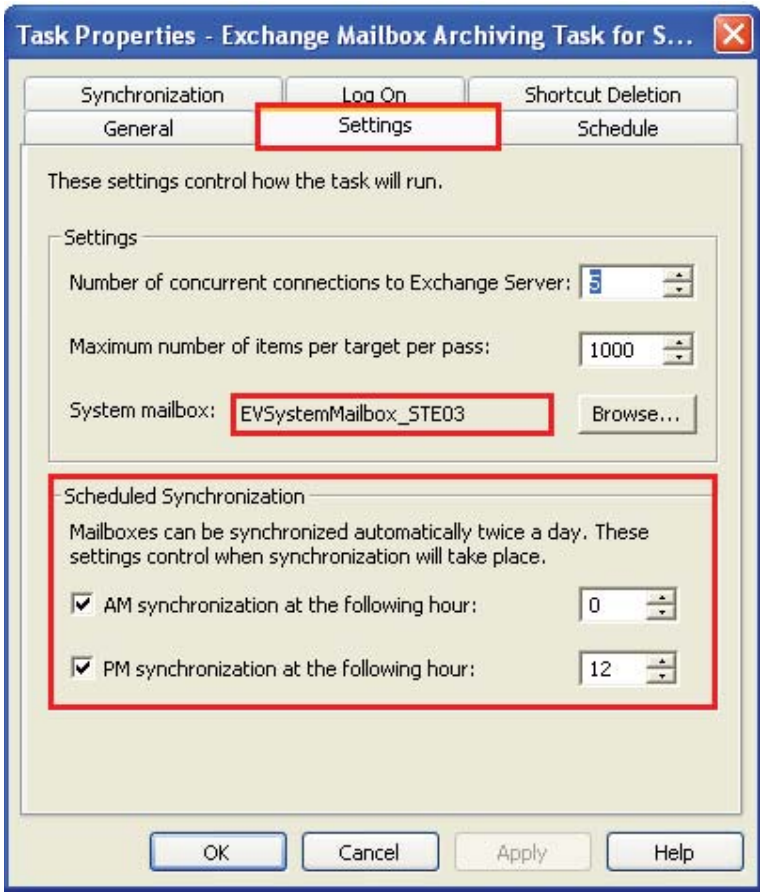


Check override for the Vault Store and Indexing Service and click on OK.

Browse to the Site – Enterprise Vault Servers – evserver01 and click on tasks. Then right click on the Exchange Mailbox Archiving task on the right for all Exchange servers and click on properties.



Click on the Settings tab and then configure the System mailbox to the mailbox created in the prerequisites and confirm that synchronization is set for 0 AM and 12 PM like pictured below.



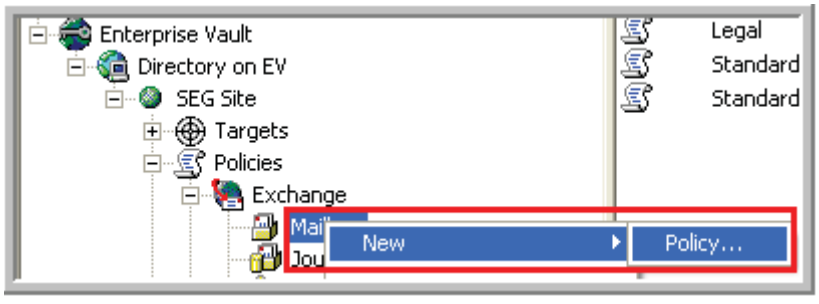
Setup the Policy Configuration

Use the following table to create the necessary Policies, Retention Categories and Provisioning Groups. These groups will be applied to the distribution lists listed to manage the users Enterprise Vault Archive settings.

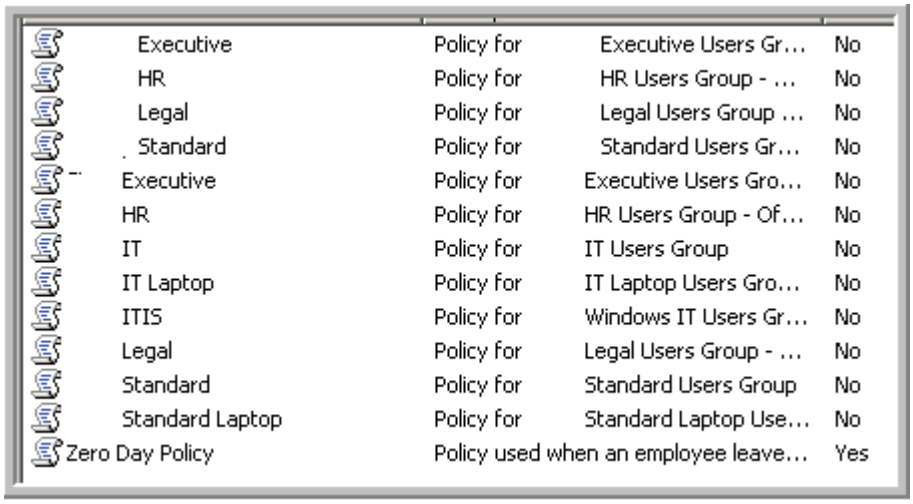
Policy	**Retention Category**	**Provisioning Group**	**Distribution List**
Parent Executive	Parent Executive	Parent Executive	DL - LMC - EVault - Executive
Parent Legal	Parent Legal	Parent Legal	DL - LMC - EVault - Legal
Parent HR	Parent HR	Parent HR	DL - LMC - EVault - HR

Parent Standard	Parent Standard	Parent Standard	DL - LMC - EVault - Standard
Company Executive	Company Executive	Company Executive	DL-SEG-EVault-Executive
Company Legal	Company Legal	Company Legal	DL-SEG-EVault-Legal
Company HR	Company HR	Company HR	DL-SEG-EVault-HR
Company Standard	Company Standard	Company Standard	DL-SEG-EVault-Company DL-SEG-EVault-Generic
Company Standard Laptop	Company Standard	Company Standard Laptop	DL-SEG-EVault-Company-Lap
Company IT	Company IT	Company IT	DL-SEG-EVault-IT
Company IT Laptop	Company IT	Company IT Laptop	DL-SEG-EVault-IT-Lap
Company ITIS	Company IT	Company ITIS	DL-SEG-EVault-IT IS
Company Zero Day	Zero Day	Company Zero Day	DL-SEG-EVault-ZeroDay

Browse to Policies – Exchange and right click on Mailbox and select New – Policy.

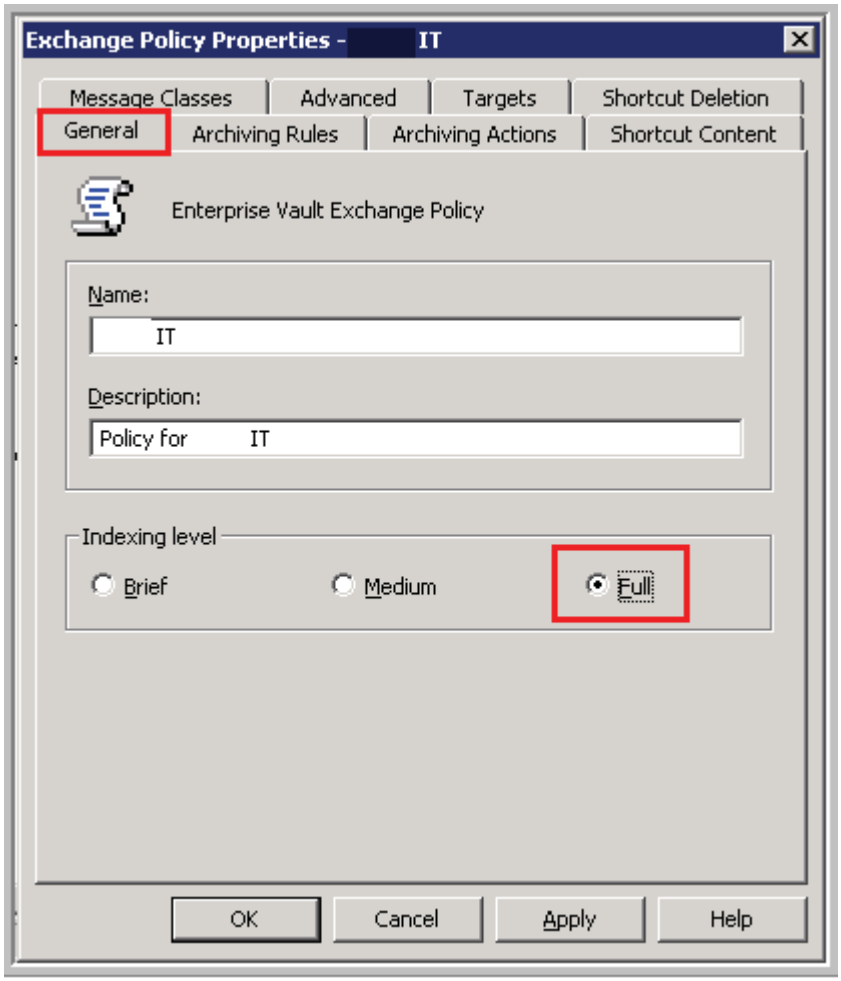


Create the policies listed in Step 1 with the descriptions listed below.

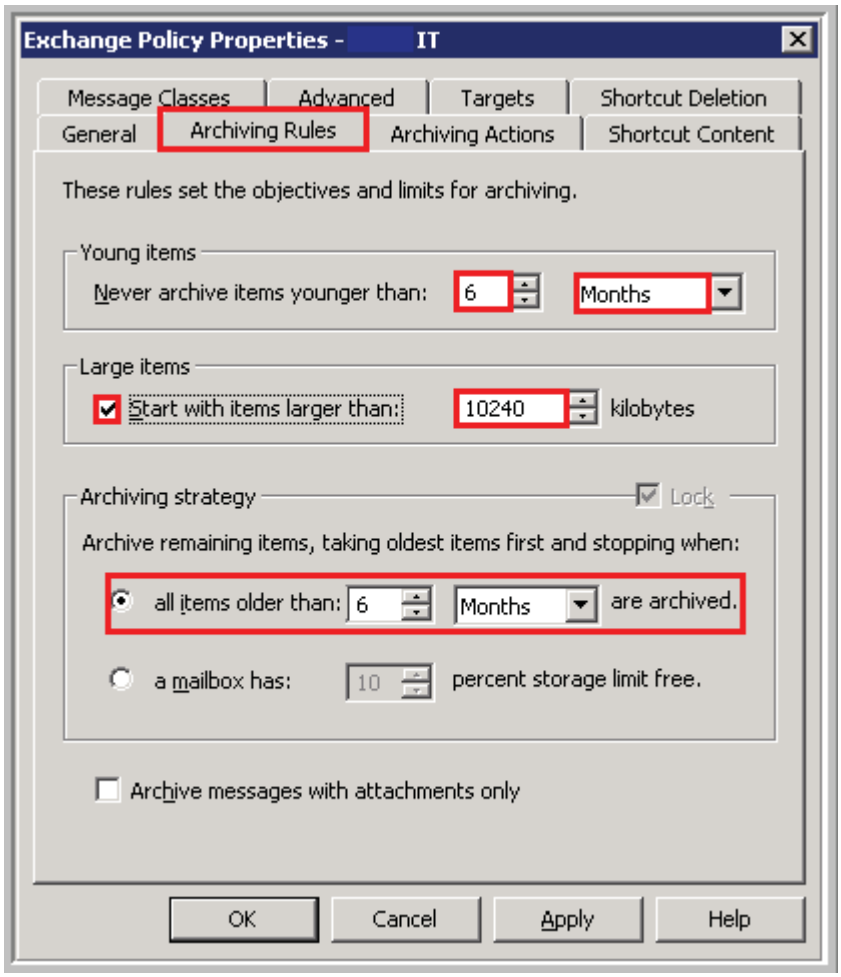


Executive	Policy for	Executive Users Gr…	No
HR	Policy for	HR Users Group - …	No
Legal	Policy for	Legal Users Group …	No
Standard	Policy for	Standard Users Gr…	No
Executive	Policy for	Executive Users Gro…	No
HR	Policy for	HR Users Group - Of…	No
IT	Policy for	IT Users Group	No
IT Laptop	Policy for	IT Laptop Users Gro…	No
ITIS	Policy for	Windows IT Users Gr…	No
Legal	Policy for	Legal Users Group - …	No
Standard	Policy for	Standard Users Group	No
Standard Laptop	Policy for	Standard Laptop Use…	No
Zero Day Policy	Policy used when an employee leave…		Yes

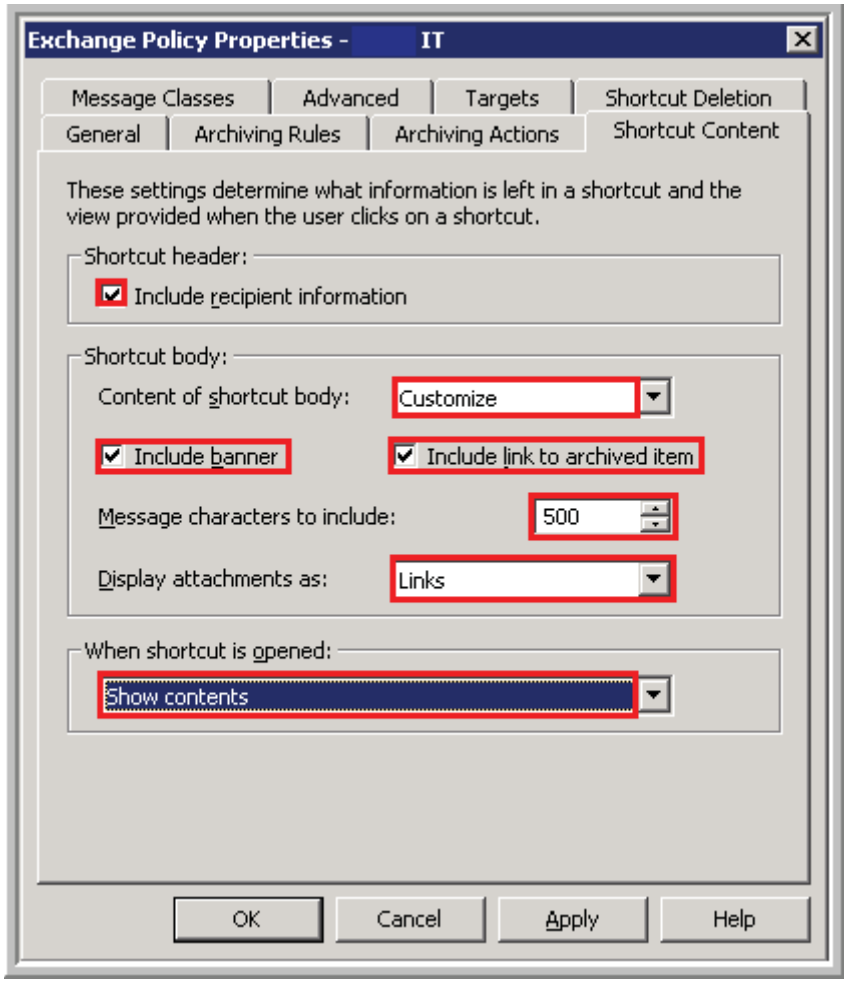
Click on each policy and change the Indexing level to Full. Currently the following policy settings will all be the same except for Offline Vault settings, since non-laptop users will not have Offline Vault like laptop users.



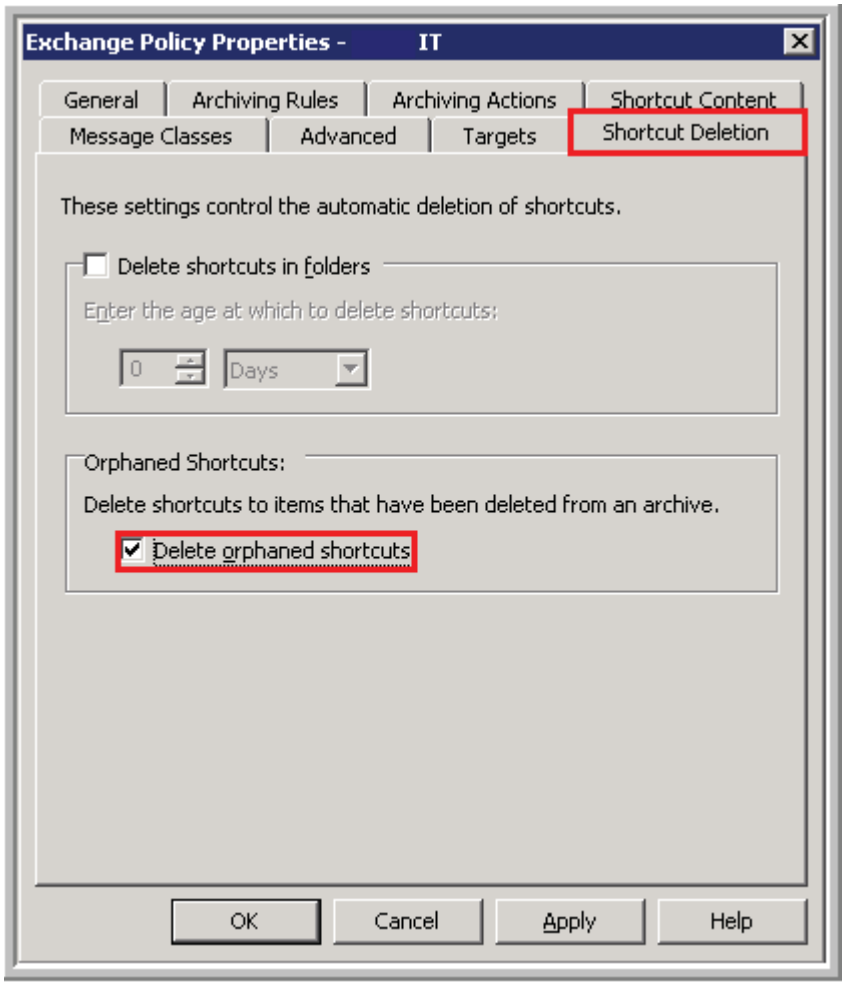
Configure the Archiving Rules tab so that you never archive items younger than 6 months and so you start with items larger than 10240 (1 month and 2024 for all company Policies). Also so all items older than 6 months are archived (3 months for all company Policies).



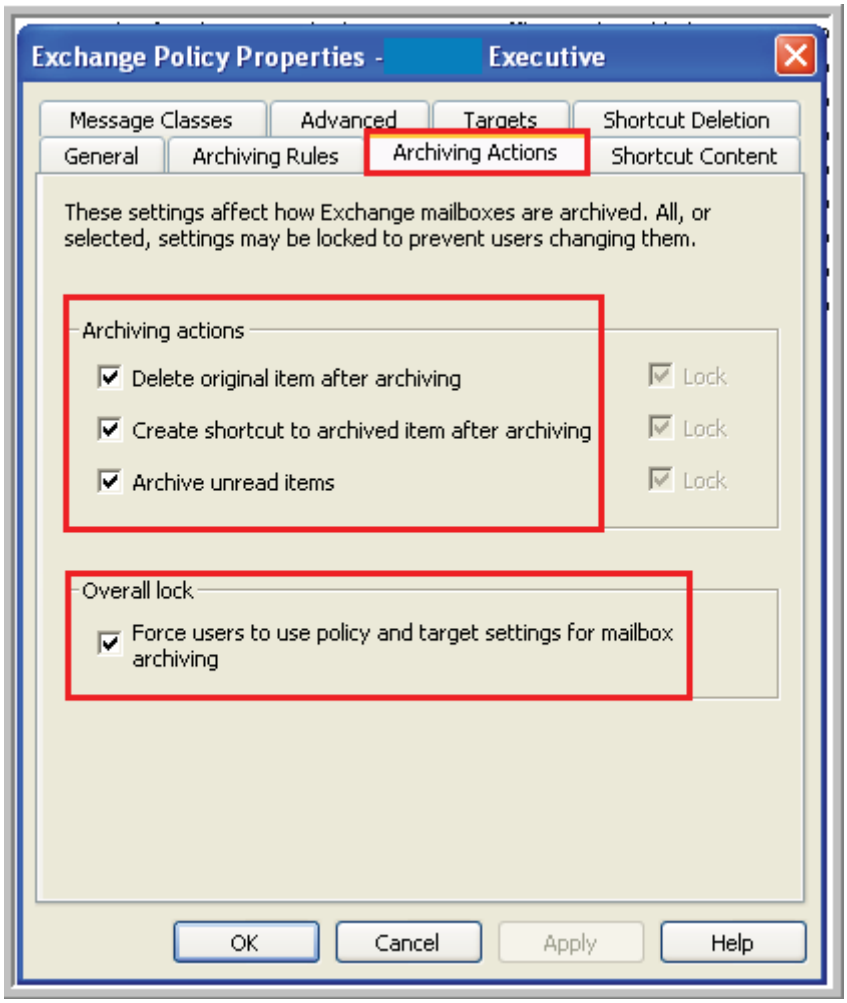
Next configure the shortcut properties so when mail is archived from an inbox the shortcut displays 500 characters of text in the body and links for attachments. To do these configure the settings like pictured below.



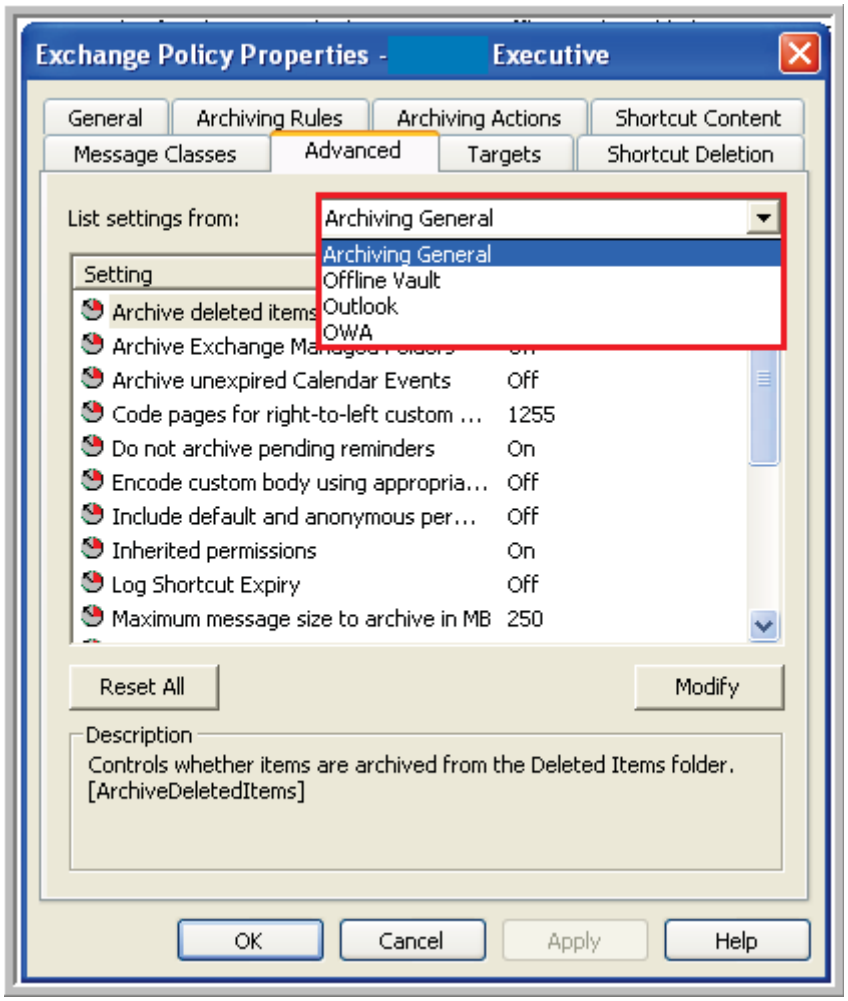
Click on Shortcut Deletion and check Delete orphaned shortcuts.



Click on the Archiving Actions tab and check the Overall lock and check all the archiving actions.



Click on the Advanced tab and change the settings listed in the table below for each of the listed settings.



Archiving General

- Turn on archive deleted items
- **Not Enabled** May need to enable default and anonymous permissions, but if someone mistakenly set everyone access then the problem is everyone will have access to that archive
- Turn on Inherited permissions
- Set pending shortcut timeout to 3 – that will revert it back to mail after 3

days

- Turn on set failed messages ‘Do Not Archive’

Offline Vault – Offline archives enabled state to none for policies that have this disabled

- Turn on deleted items in offline vault
- ‘Download Folder’ button visible – hide both
- Download item age limit is set to 180 (90 for company)
- Download reminder interval 180 (90 for company)
- Inactivity period is 6 (3 for company)
- Inactivity period units is months
- Large items size is on
- Large item size is set to 10240 (2024 for company)
- Lock for deleted items in offline vault is set to locked
- Lock for download age limit is on
- Minimum age is 6 (3 for the company) and minimum age units is months
- Offline archives enabled state – All Users – **NOTE: Not for company/IT Standard**

- Percentage store size – 15
- ‘Prioritize Download’ option visible set to Hide Both
- ‘Refresh Archive Explorer’ View option is set to on
- Search across all indexes – turn this on
- Show download reminder – turn off
- Show setup wizard – turn off

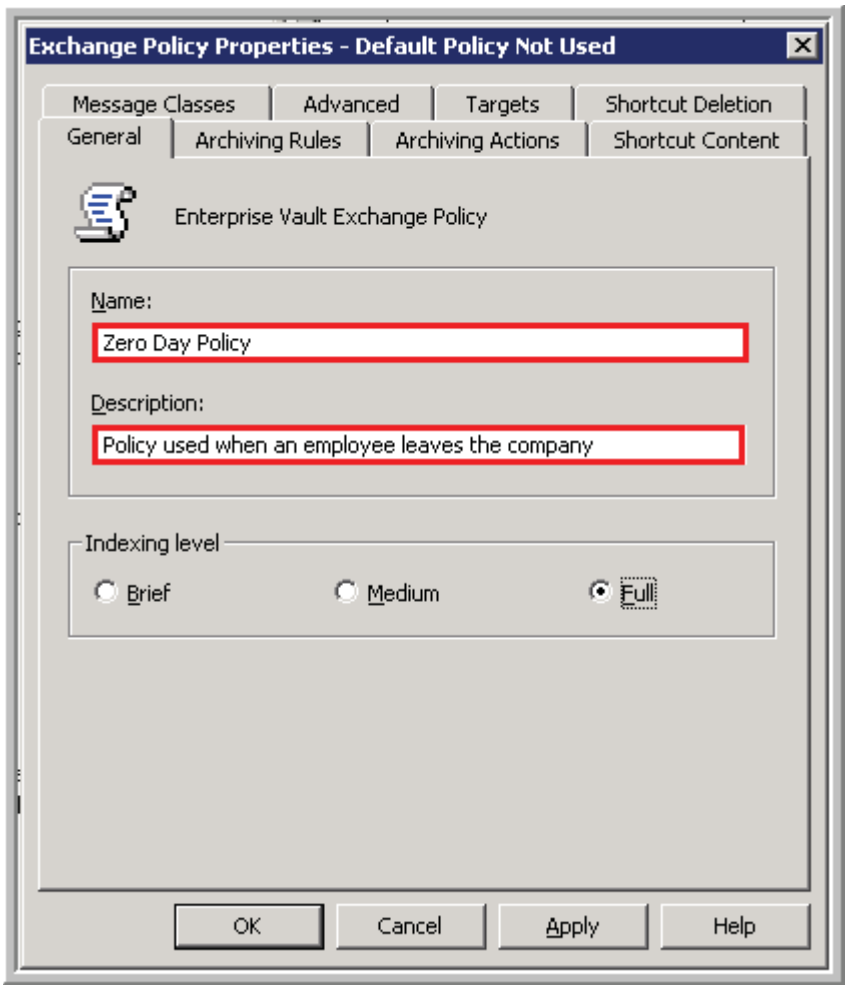
Outlook Settings

- Add server to Intranet Zone – ev;evserver01.seg.corp.root
- Allow script in public folders – Force on
- Allow script in shared folders – Force on
- ‘Delete from Vault’ button visible – Hide Both
- Fix Outlook preview pane – Apply automatically
- Launch Archive Explorer – set to Separate browser
- Public Folder operations – turn this on
- RPC over HTTP Proxy URL – set to HTTPS://webmail.com/exchange
- RPC over HTTP restrictions – set to None
- Shortcut Deletion Behavior – Both Deleted

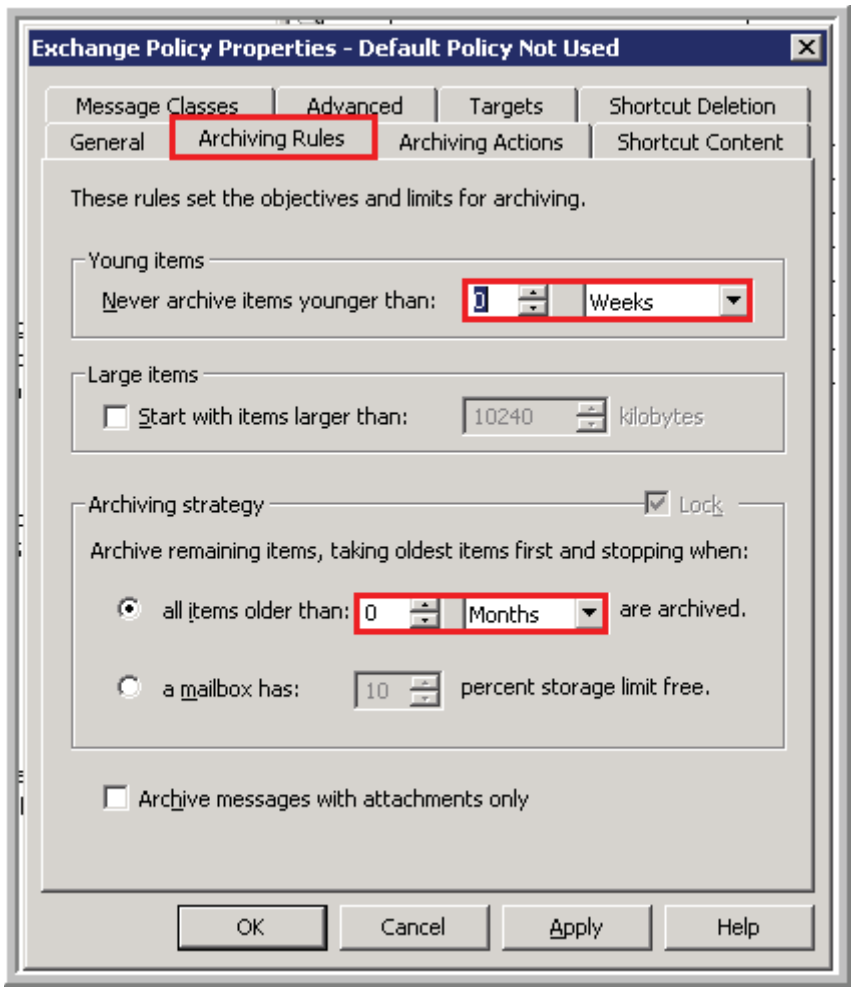
OWA settings

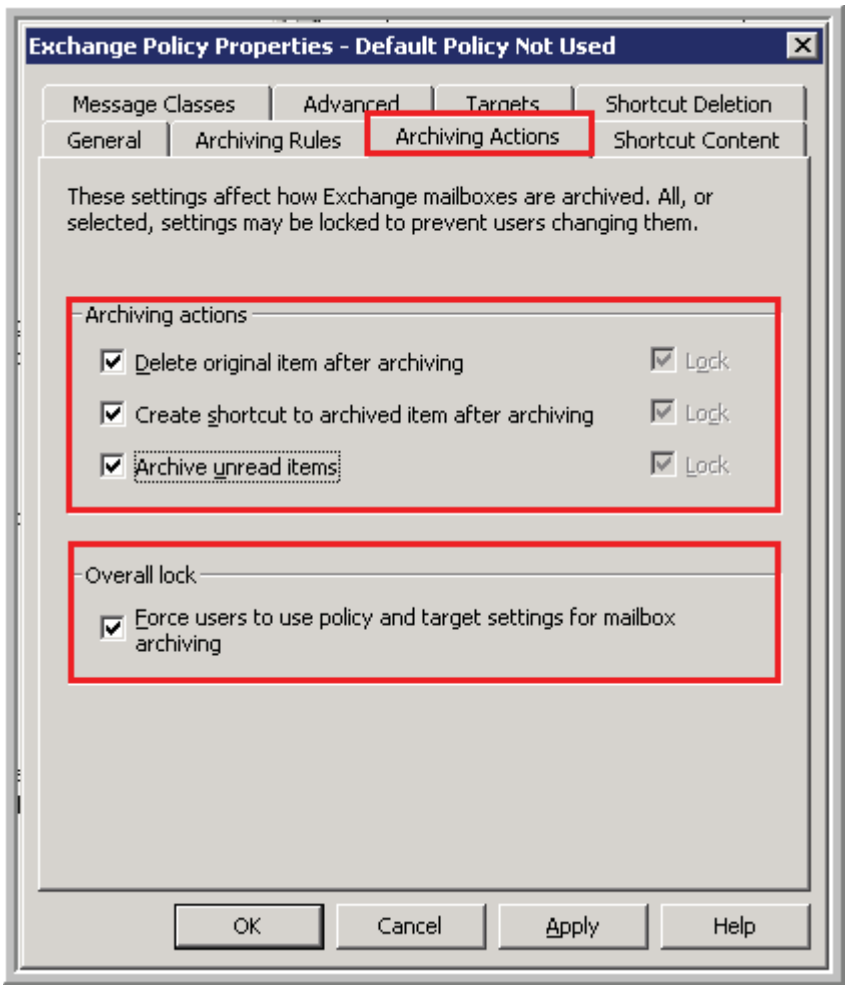
- Archive Confirmation – turn off
- ‘Cancel Operations’ on toolbar – set to off
- ‘Delete from Archive’ on context menu – Off
- ‘Delete from Archive’ on toolbar – Off
- Delete mode – Shortcut
- Premium restore function – Basic
- Premium restore function – Basic

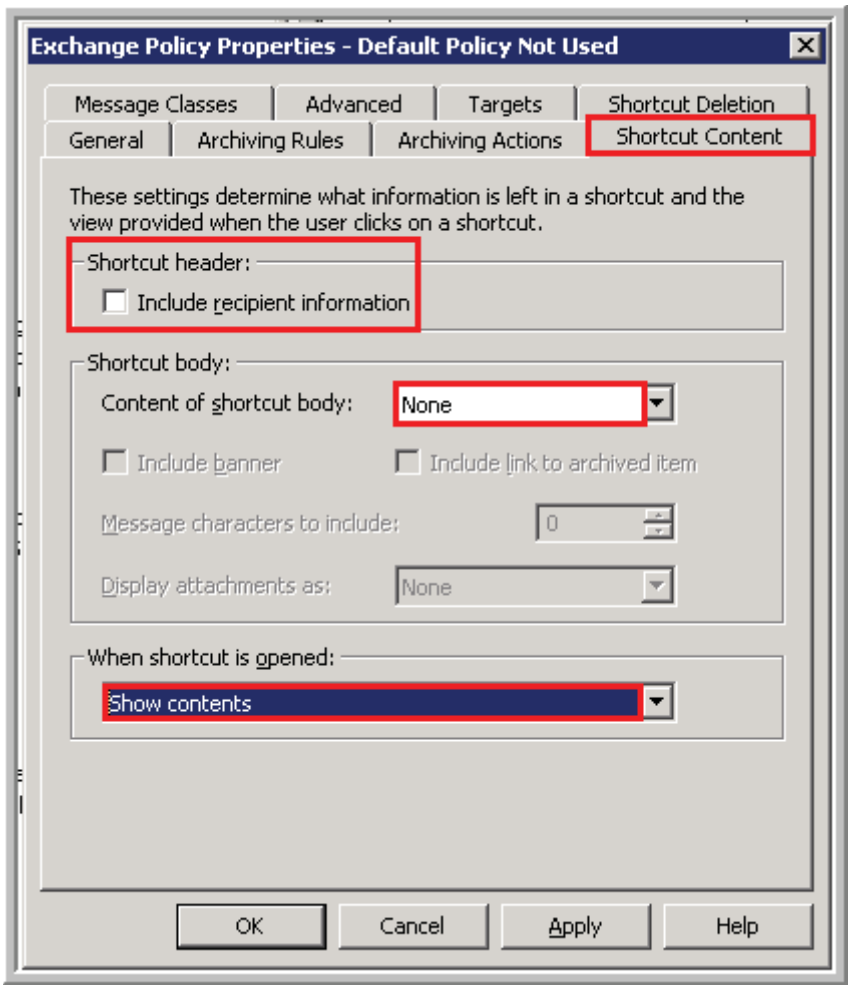
The Zero Day policy is used for employees that have left the company. They are put in this distribution list and automatically provisioned and all of their mail contents are archived from their mailbox. Follow the steps above, but with the settings pictured in the screenshots below. This mail is only retained for 90 days.

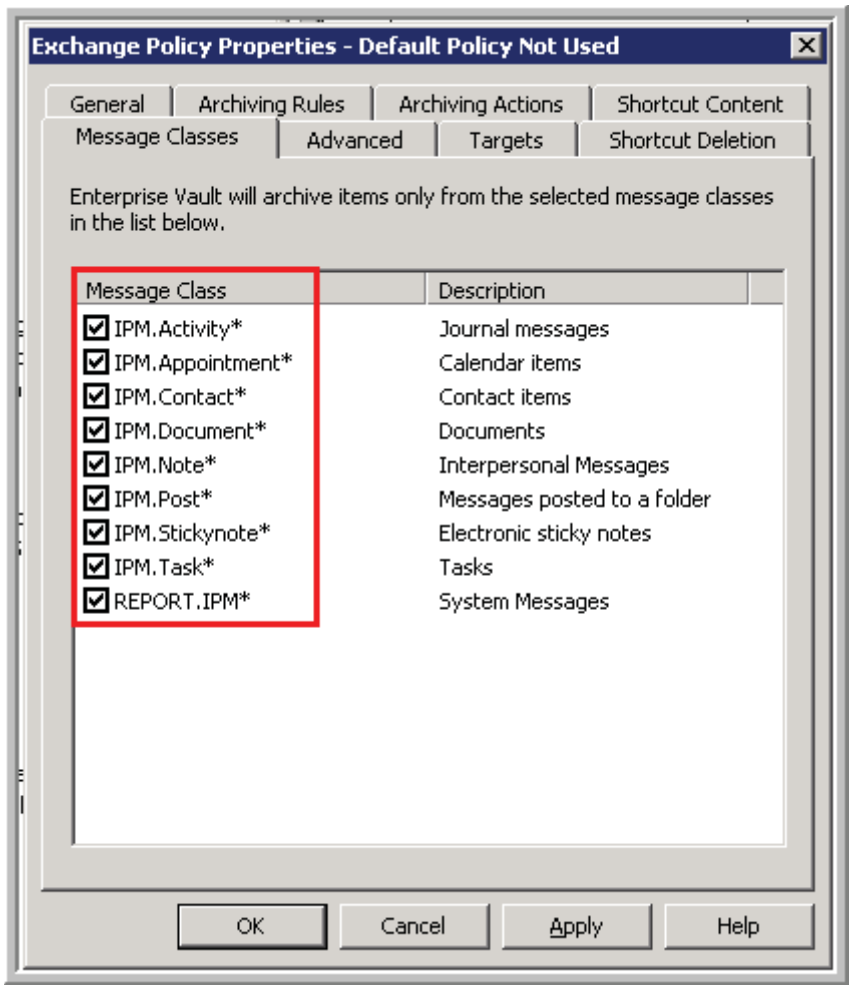


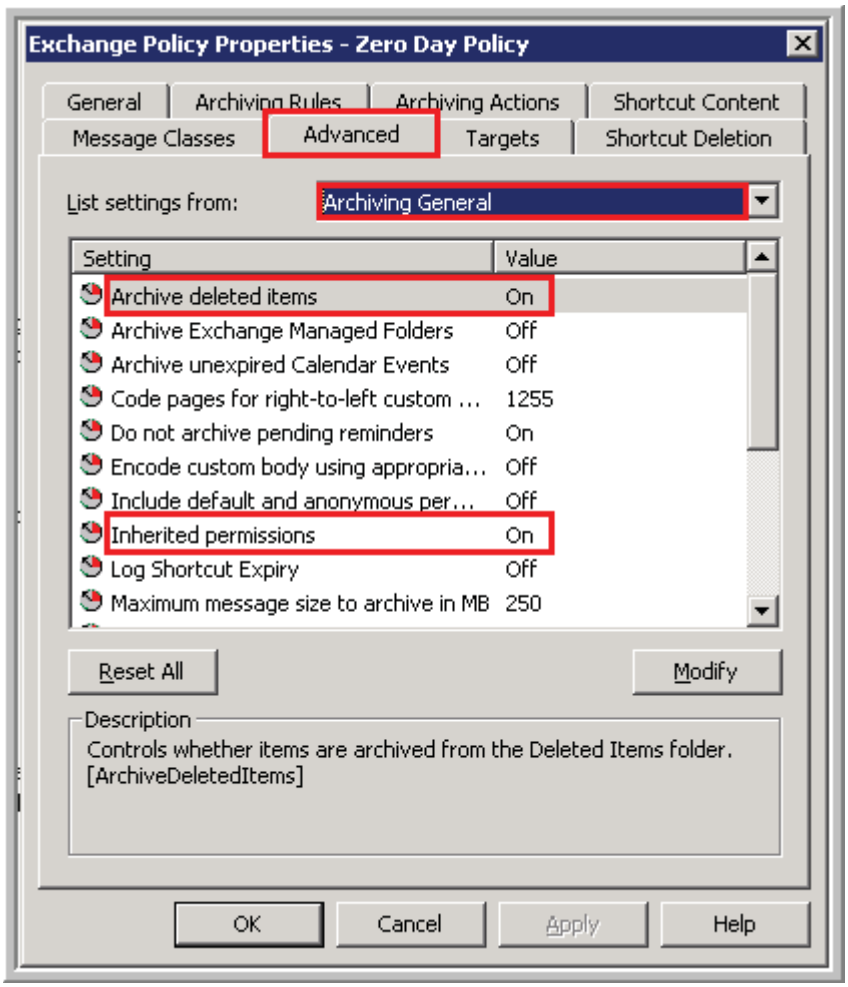
Below put in 0 Days, not months or weeks.


Exchange Policy Properties - Default Policy Not Used
Message Classes
Advanced
Targets
Shortcut Deletion
General
Archiving Rules
Archiving Actions
Shortcut Content
These rules set the objectives and limits for archiving.
Young items
Never archive items younger than:
0
Weeks
Large items
Start with items larger than:
10240
kilobytes
Archiving strategy
Lock
Archive remaining items, taking oldest items first and stopping when:
all items older than:
0
Months
are archived.
a mailbox has:
10
percent storage limit free.
Archive messages with attachments only
OK
Cancel
Apply
Help


Exchange Policy Properties - Default Policy Not Used
Message Classes
Advanced
Targets
Shortcut Deletion
General
Archiving Rules
Archiving Actions
Shortcut Content
These settings affect how Exchange mailboxes are archived. All, or selected, settings may be locked to prevent users changing them.
Archiving actions
Delete original item after archiving
Lock
Create shortcut to archived item after archiving
Lock
Archive unread items
Lock
Overall lock
Force users to use policy and target settings for mailbox archiving
OK
Cancel
Apply
Help

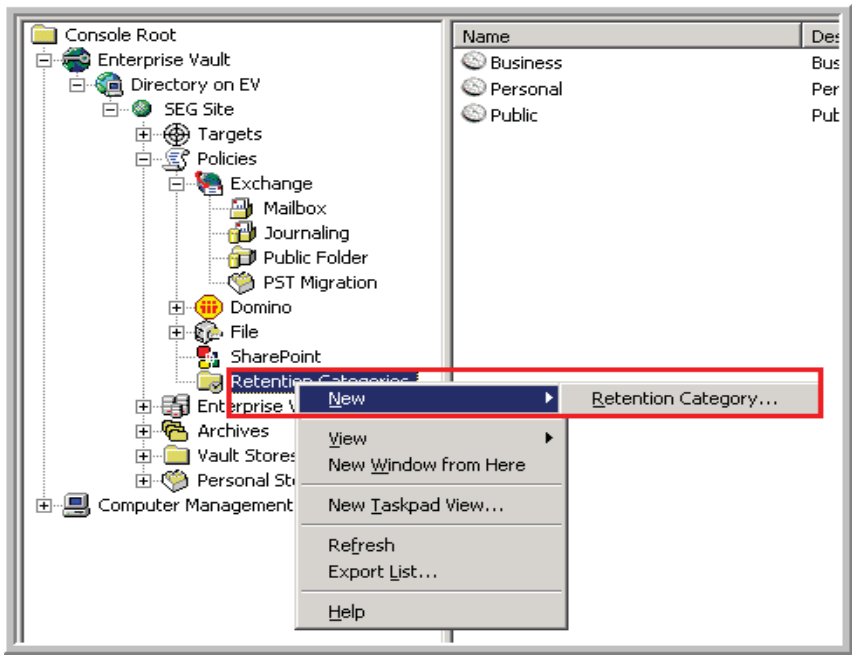

Exchange Policy Properties - Default Policy Not Used
Message Classes
Advanced
Targets
Shortcut Deletion
General
Archiving Rules
Archiving Actions
Shortcut Content
These settings determine what information is left in a shortcut and the view provided when the user clicks on a shortcut.
Shortcut header:
Include recipient information
Shortcut body:
Content of shortcut body:
None
Include banner
Include link to archived item
Message characters to include:
0
Display attachments as:
None
When shortcut is opened:
Show contents
OK
Cancel
Apply
Help


Exchange Policy Properties - Default Policy Not Used
General
Archiving Rules
Archiving Actions
Shortcut Content
Message Classes
Advanced
Targets
Shortcut Deletion
Enterprise Vault will archive items only from the selected message classes in the list below.
Message Class
Description
IPM.Activity*
Journal messages
IPM.Appointment*
Calendar items
IPM.Contact*
Contact items
IPM.Document*
Documents
IPM.Note*
Interpersonal Messages
IPM.Post*
Messages posted to a folder
IPM.Stickynote*
Electronic sticky notes
IPM.Task*
Tasks
REPORT.IPM*
System Messages
OK
Cancel
Apply
Help

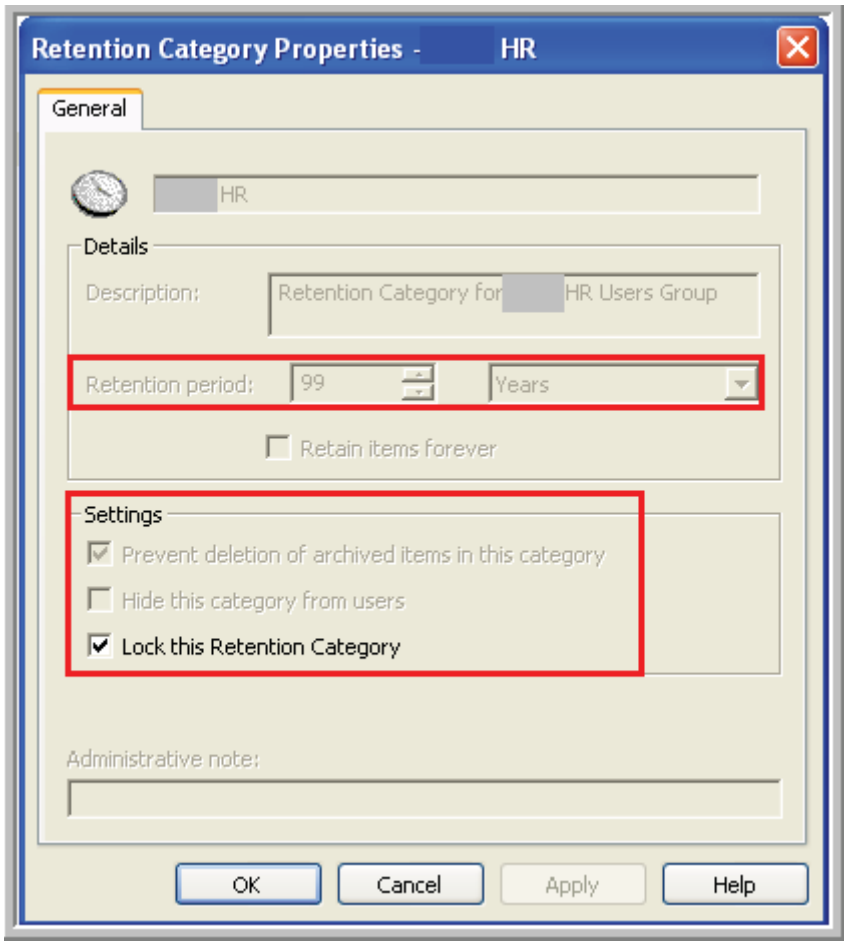


Configure Retention Category Details

Browse to Policies and right click on Retention Categories and select New – Retention Category. Currently all retention categories are configured the same.



Set the Retention Period to 99 years except for the Zero Day retention, which is set to 90 days. Confirm that Prevent deletion of archived items in this category and Lock this retention category are checked and then click on OK.

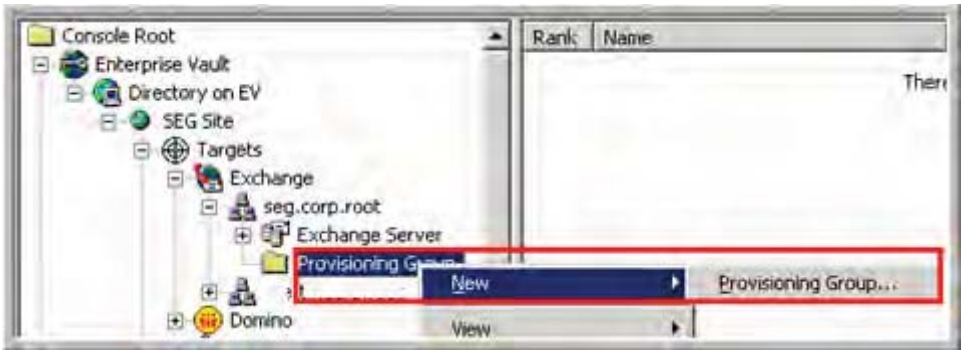


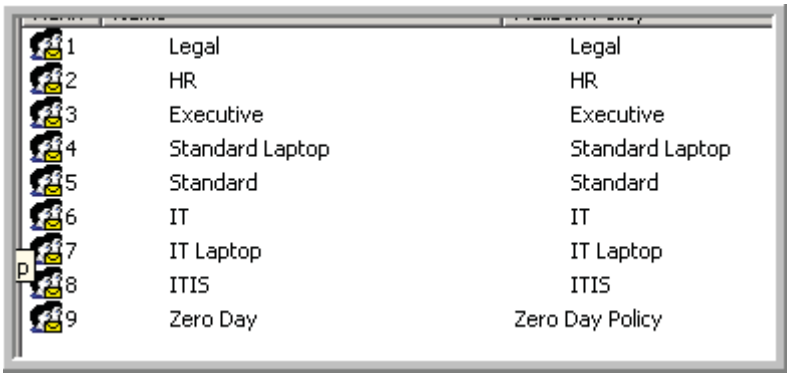
Create all the retention categories listed below and in the table in the Policy Configuration section.

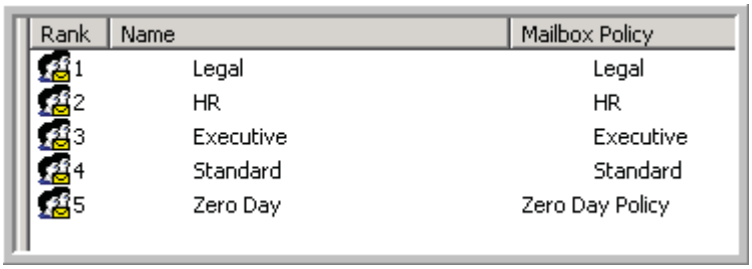
Default Retention - No...	Default retention category for	SEG Site	98 years
Executive	Retention Category for	Executive Users Group	99 years
HR	Retention Category for	HR Users Group	99 years
Legal	Retention Category for	Legal Users Group	99 years
Standard	Retention Category for	Standard Users Group	99 years
Not Used	Retention Category for	Journaling	99 years
Executive	Retention Category for	Executive Users Group	99 years
HR	Retention Category for	HR Users Group	99 years
IT	Retention Category for	IT Users Group	99 years
Legal	Retention Category for	Legal Users Group	99 years
Standard	Retention Category for	Standard Users Group	99 years
Zero Day	Retention Category for	Users that left the company	3 months

Configure the Provisioning Groups

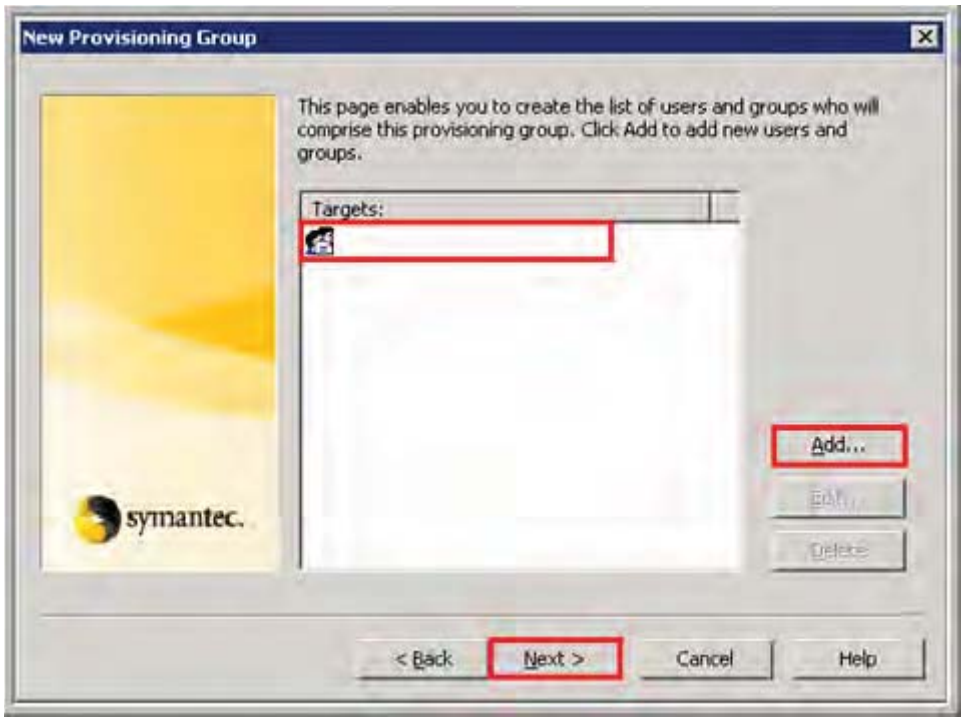
Refer to Policy Configuration for the table regarding the provisioning groups that need to be created. Browse to the Site –> Targets –> Exchange –> Domain and then right click on Provisioning Group –> New –> Provisioning Group. NOTE: The parent company Provisioning Groups need to be created under the parent company domain directory. See screenshots below for how the completed provisioning groups should appear.



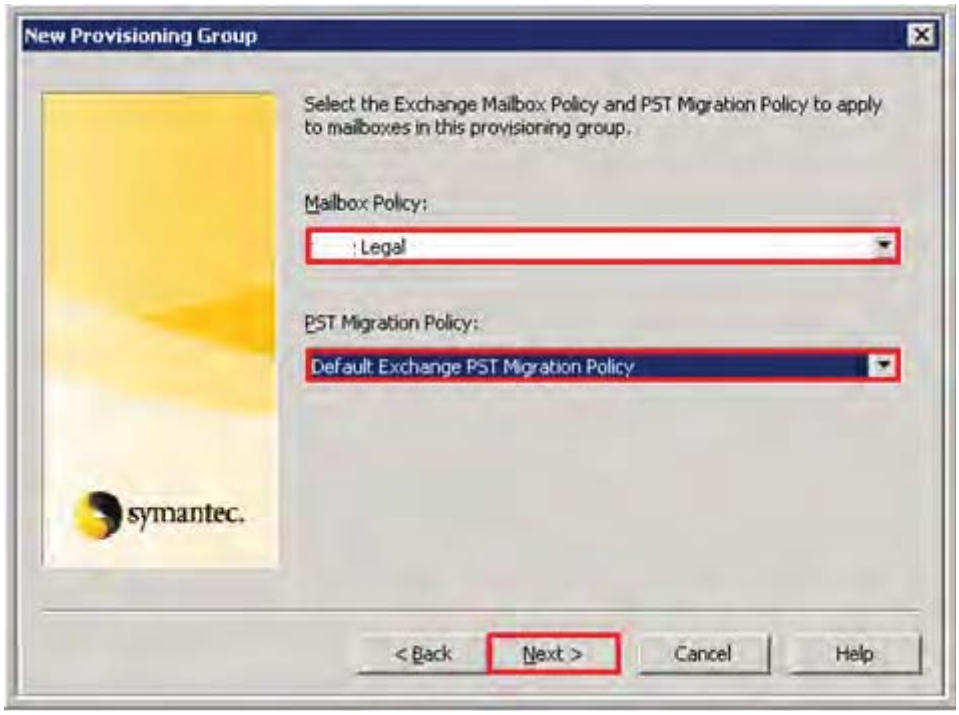




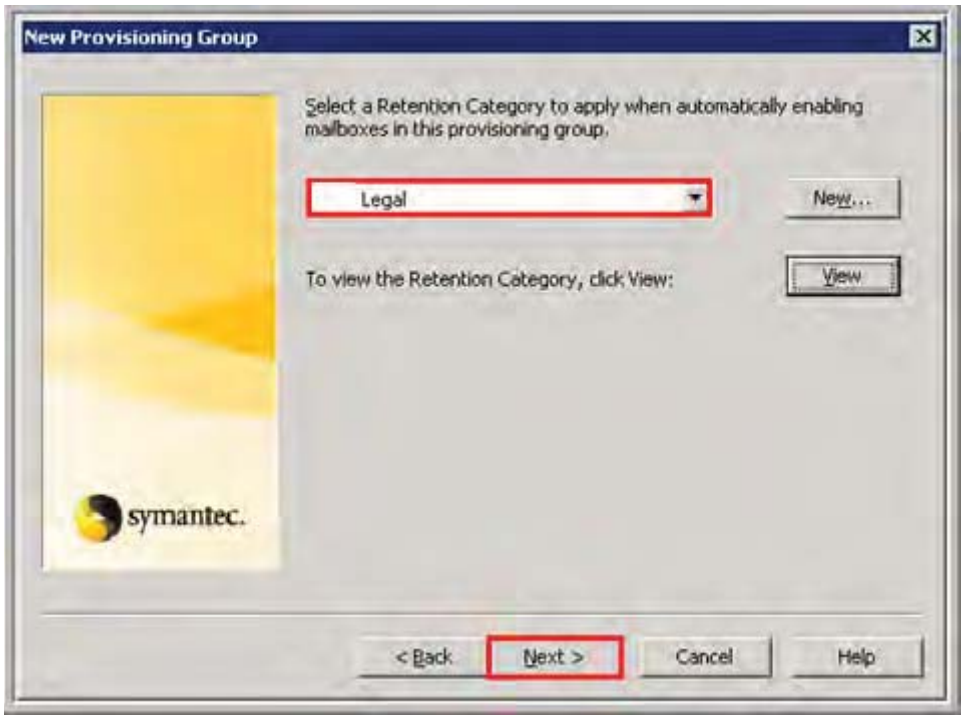
Click on Add and add the associated distribution list referenced in the table and then click on Next.



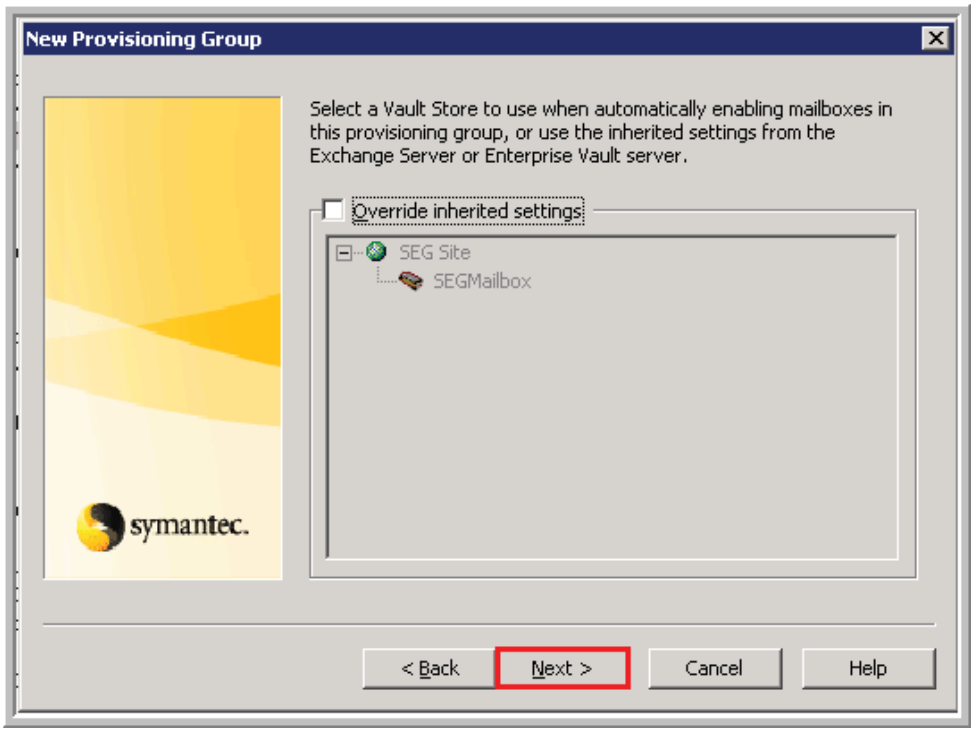
Select the associated Mailbox Policy and the Default PST Migration policy and click on Next.



Select the associated Retention Category and click on Next.

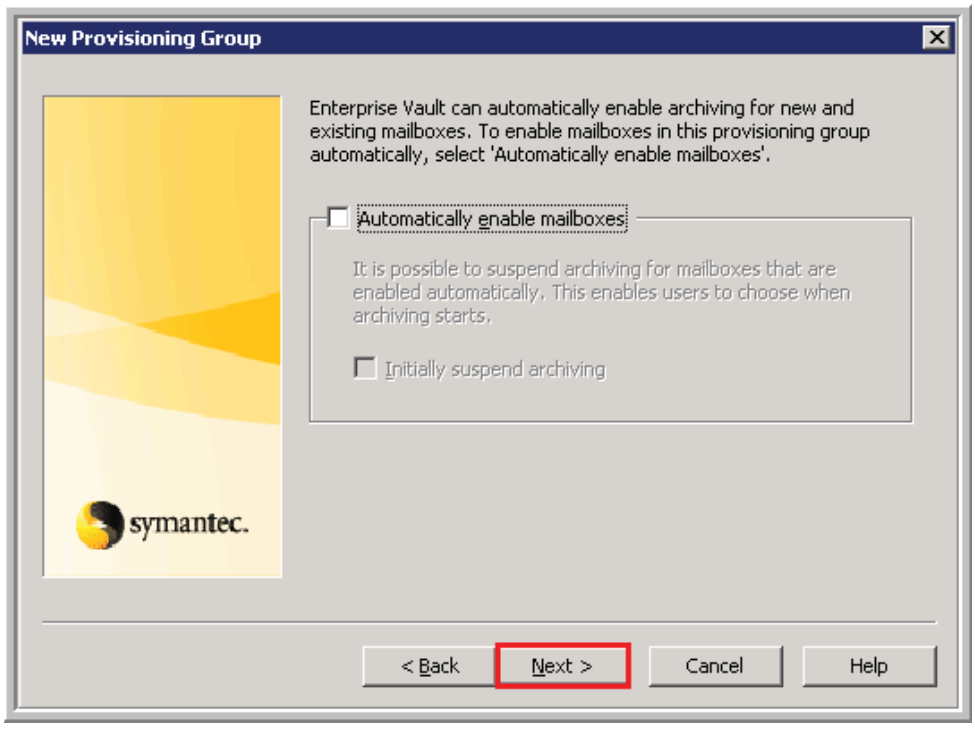


Do not override settings on the next two screens and click on Next.





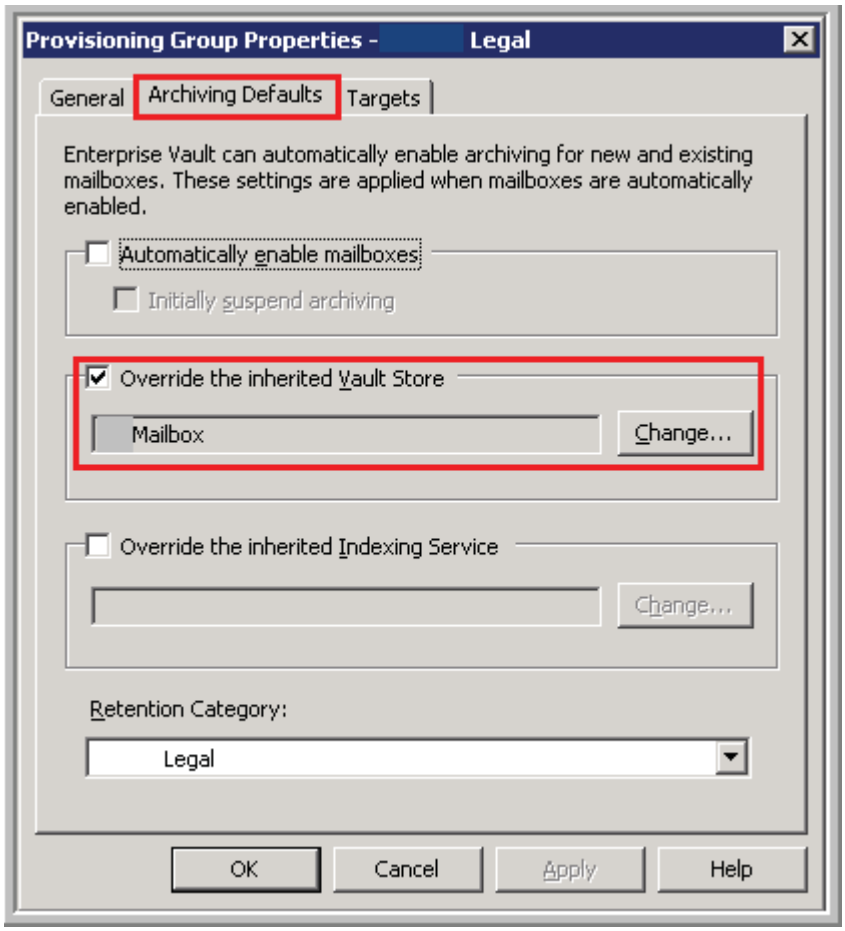
Do not automatically enable mailboxes and click on Next.



Confirm the settings and click on Finish.

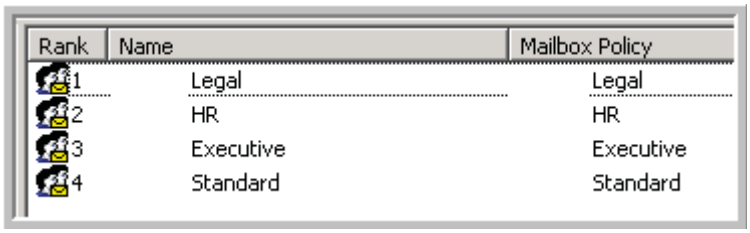


When completed with all the Provisioning Groups go into the properties of all the parent company Provisioning Groups and click on the Archiving Defaults tab and check the Override the inherited Vault Store and change it to PARMailbox. This needs to be done so all new users will archive to the correct vault store.



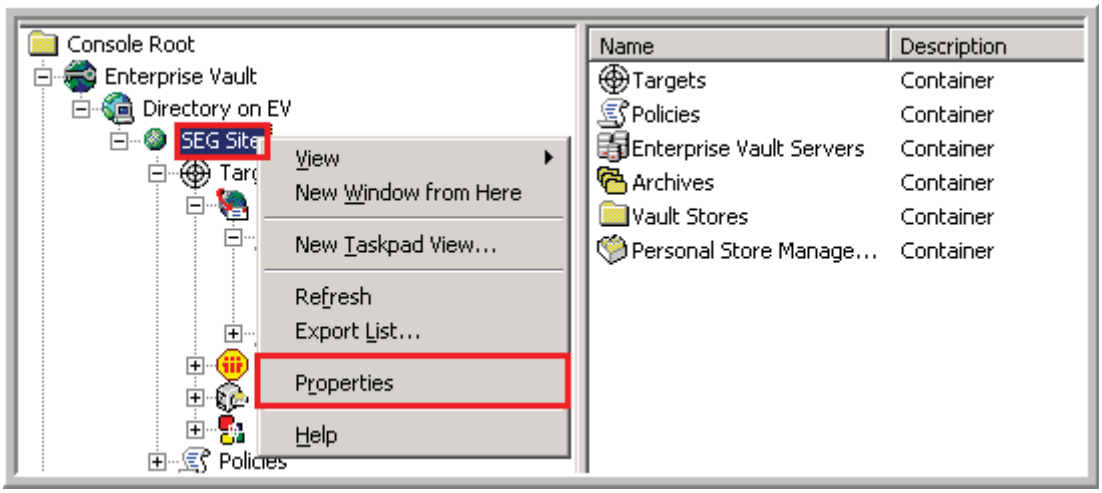
Right click on the Provisioning Group folder for each site and set the priorities in the screenshots below – HR > Legal > Executive > Standard. Note that if a user is in multiple groups they will be provisioned based on the first group they are a member of.



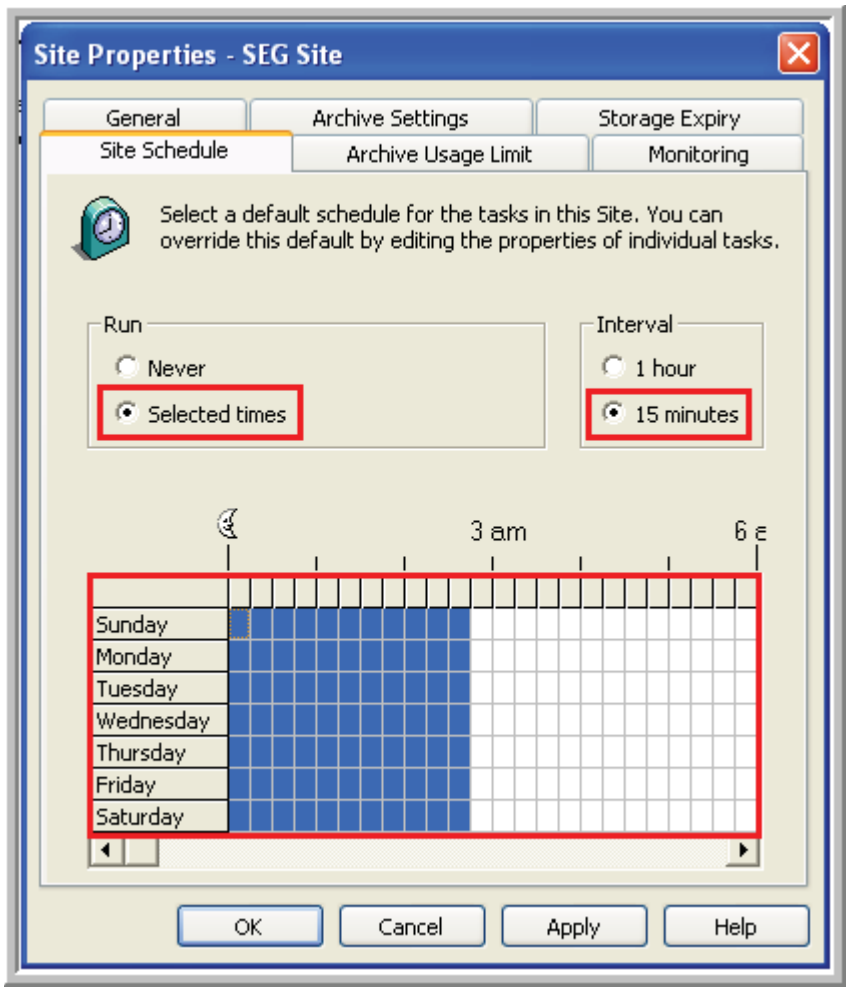


Complete the Archive Configuration

Right click on the SEG site and click on properties.



Configure it to run from 11:00 PM to 2:45 AM and click on OK.



Configure the Enable Mailbox Notification

Copy the .msg EnableMailboxMessage.msg to \\stevault01\c$\Program Files\Enterprise Vault and then edit it with the documents in the following location – the Overview document is just attached to the email.

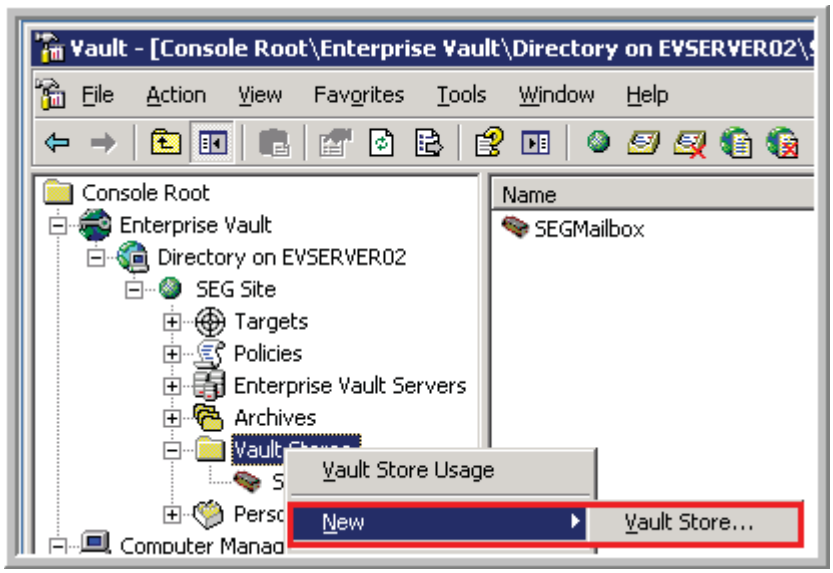
Test by disabling and re-enabling an account to verify the message looks correct.

Appendix E

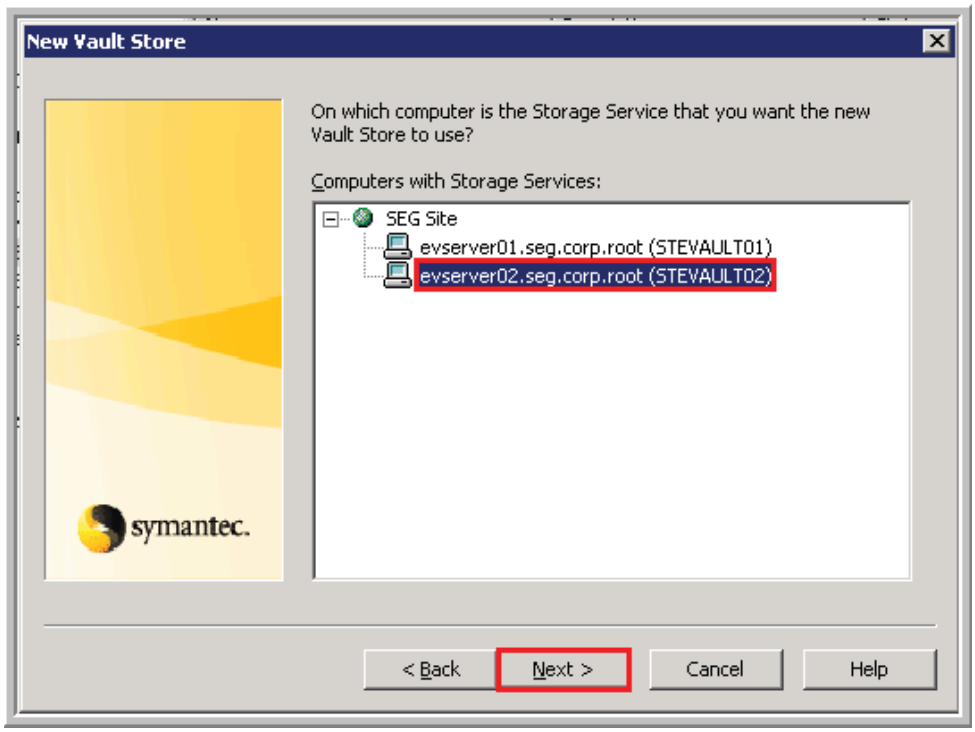
Enterprise Journal Installation and Configuration

For journaling see below regarding the mailboxes, distribution lists, journal name and mailbox locations for the company and parent company. There are 4 journals for the company and parent company to account for 4 potentially different retention categories – Standard, HR, Legal and Executive. Journaling configuration needs to be completed on STEVAULT02. First right click on the Vault Store > New > Vault Store. This only works if all the users are placed in the appropriate mailbox stores based on their position in the company since journaling is only as granular as the store level.

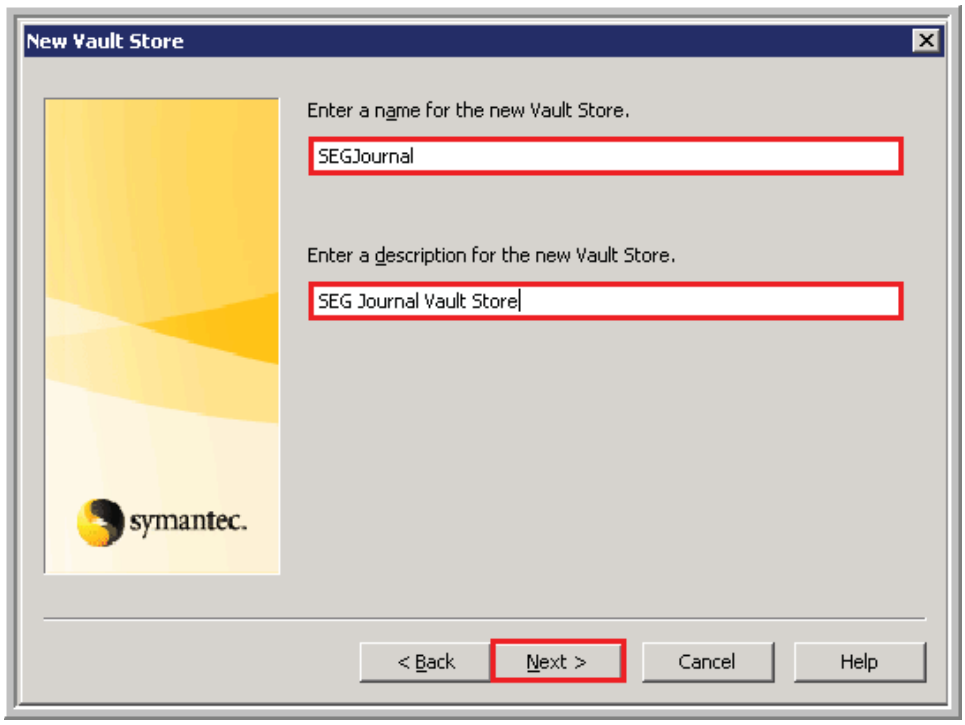
Distribution List	**Mailbox**	**Location**	**Journal – Vault Store**
DL – LMC – Journal – Standard	EV-LMC-STD-Journal	EAGLE1 > Second Storage Group > Journal Store	PARstandardJournal
DL – LMC – Journal – Executive	EV-LMC-EXEC-Journal	EAGLE1 > Second Storage Group > Journal Store	PARexecutiveJournal
DL – LMC – Journal – Legal	EV-LMC-LEG-Journal	EAGLE1 > Second Storage Group > Journal Store	PARlegalJournal
DL – LMC – Journal – HR	EV-LMC-HR-Journal	EAGLE1 > Second Storage Group > Journal Store	PARhrJournal
DL-SEG-Journal-Standard	EV-SEG-STD-Journal	STEXCHANGE03 > Storage Group 1 > Mailbox Store 1	SEGstandardJournal
DL-SEG-Journal-Executive	EV-SEG-EXEC-Journal	STEXCHANGE03 > Storage Group 1 > Mailbox Store 1	SEGexecutiveJournal
DL-SEG-Journal-Legal	EV-SEG-LEG-Journal	STEXCHANGE03 > Storage Group 1 > Mailbox Store 1	SEGlegalJournal
DL-SEG-Journal-HR	EV-SEG-HR-Journal	STEXCHANGE03 > Storage Group 1 > Mailbox Store 1	SEGhrJournal



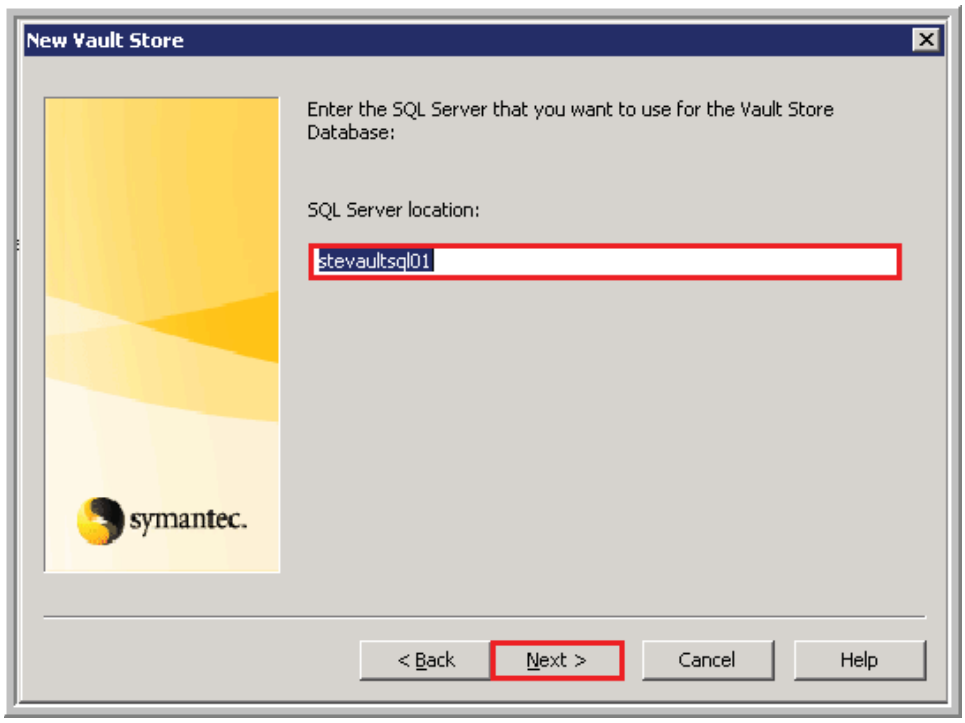
Select evserver02 and then click on Next.



Enter the name for the store (see table above) and a description and click on Next.

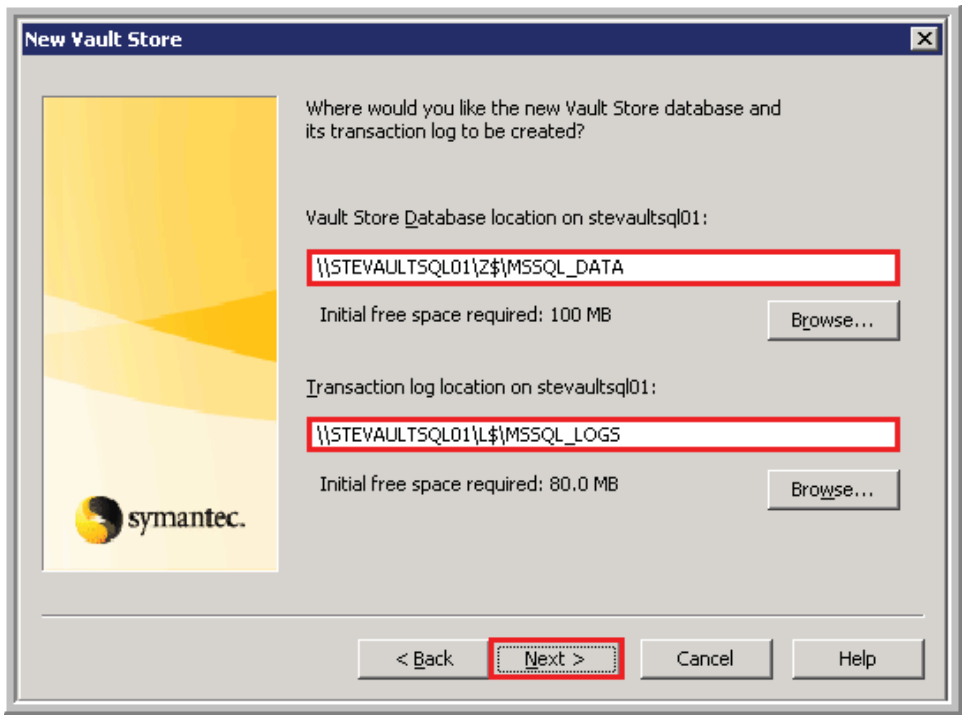


Enter the SQL Server location, STEVAULTSQL01, and click Next.

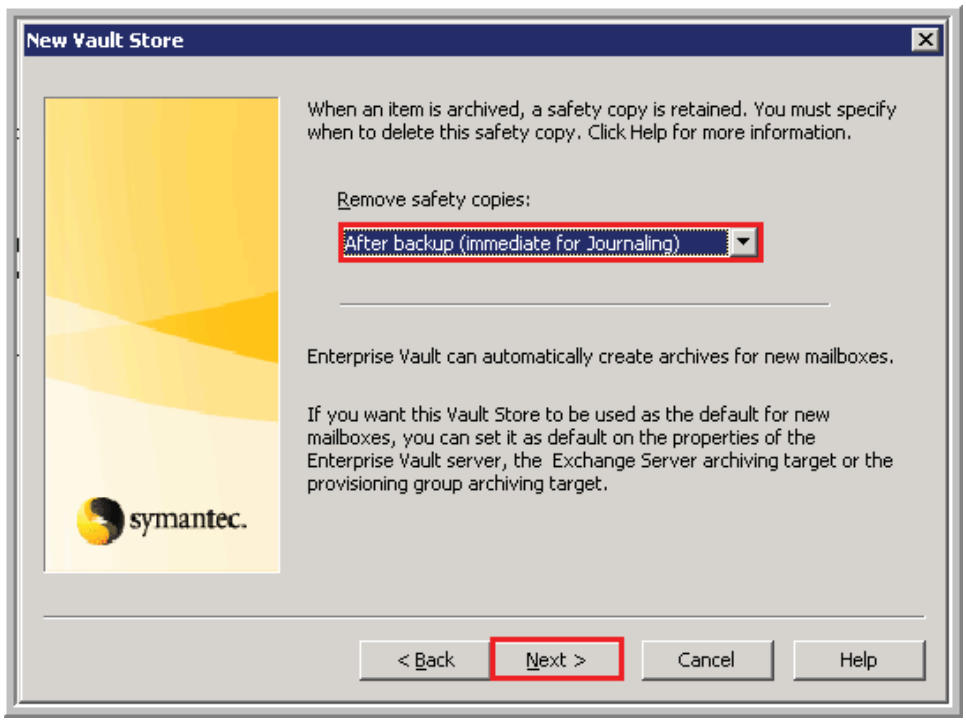


Enter the Vault Store Database and Transaction Log locations,

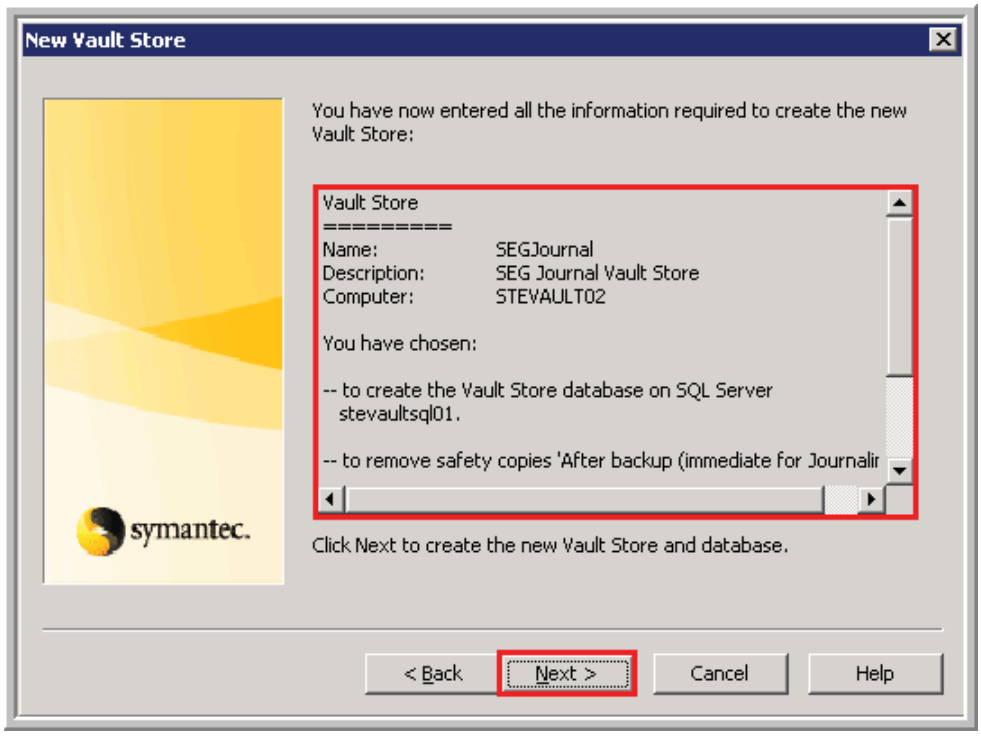
Z:\MSSQL_DATA and L:\MSSQL_LOGS and click on Next.

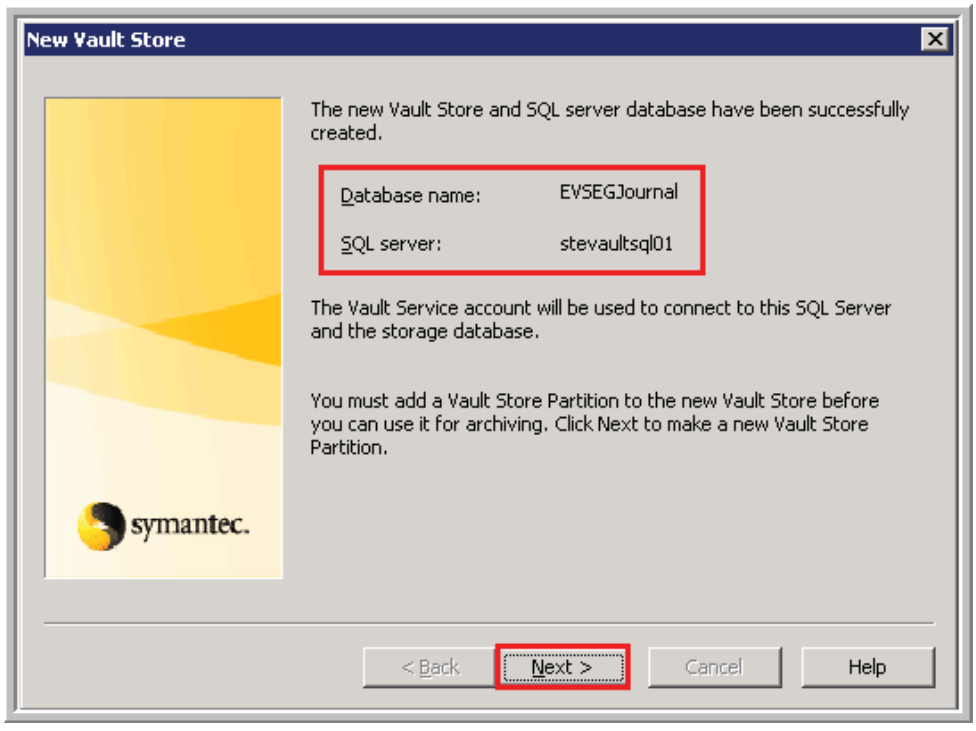


Configure for "After Backup (immediate for Journaling)" and click on Next.

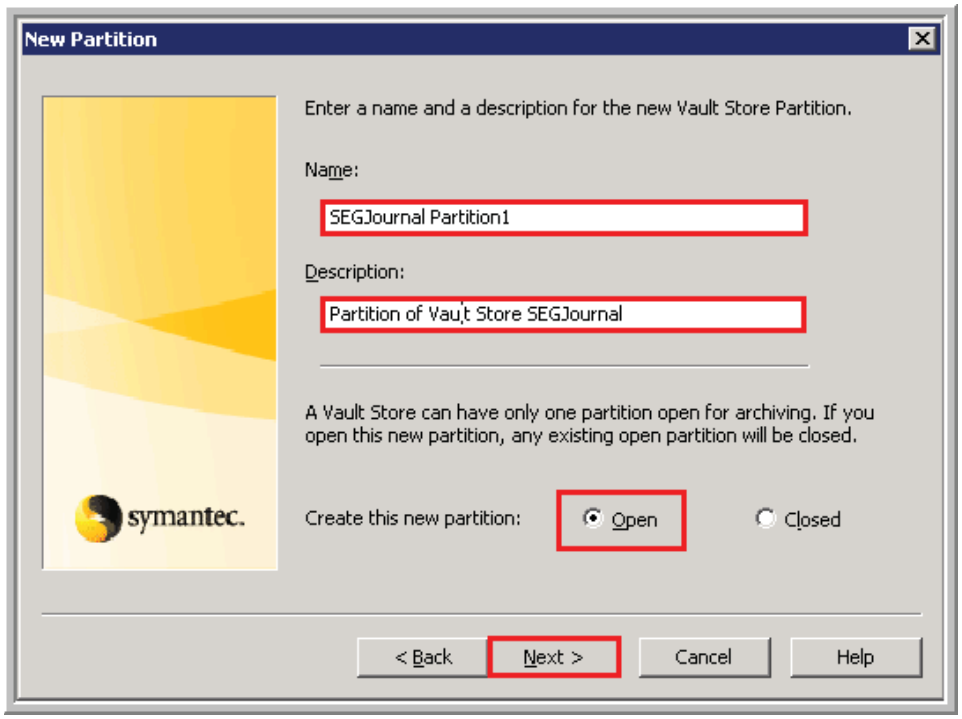


Confirm all the settings and click on Next for the following three screens.

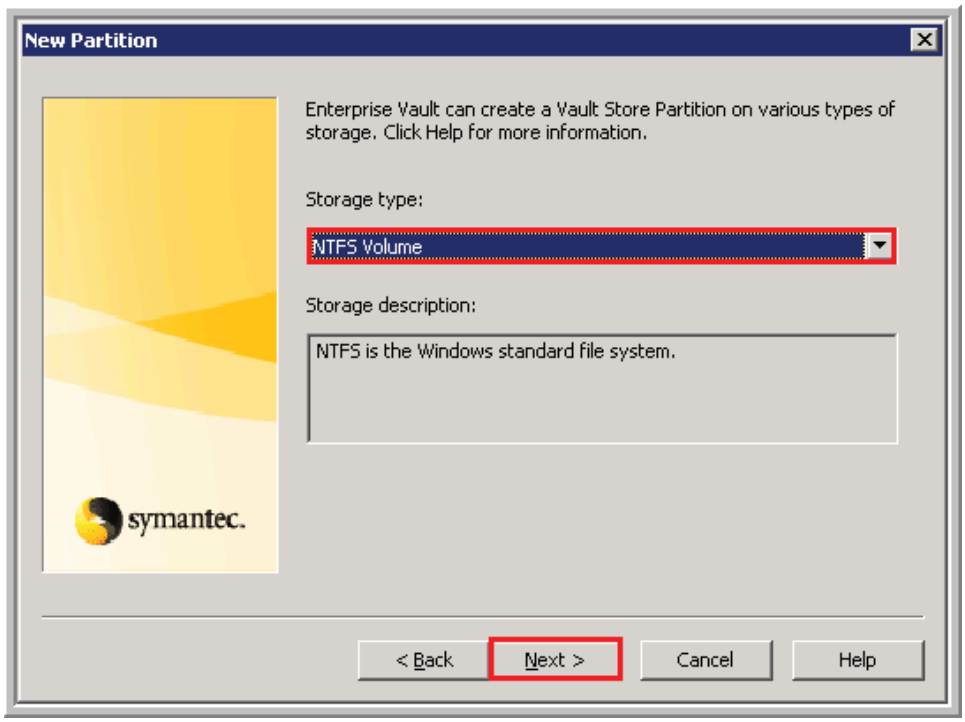




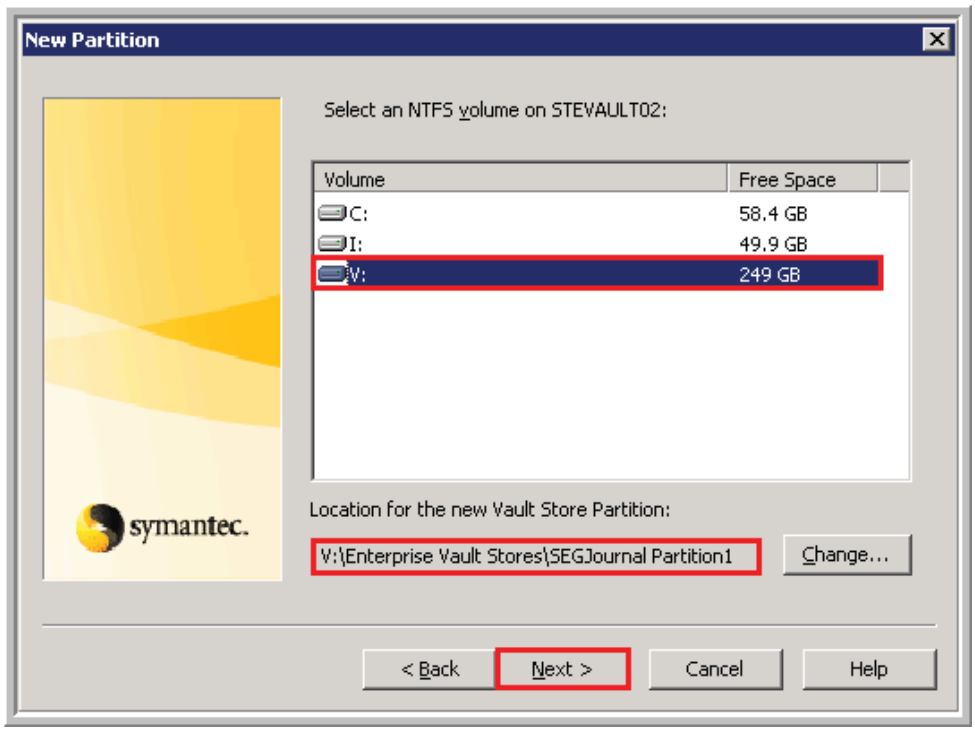
Enter the name for the Vault Store Partition, SEGJournal Partition1, and the description and confirm it is Open and click on Next.



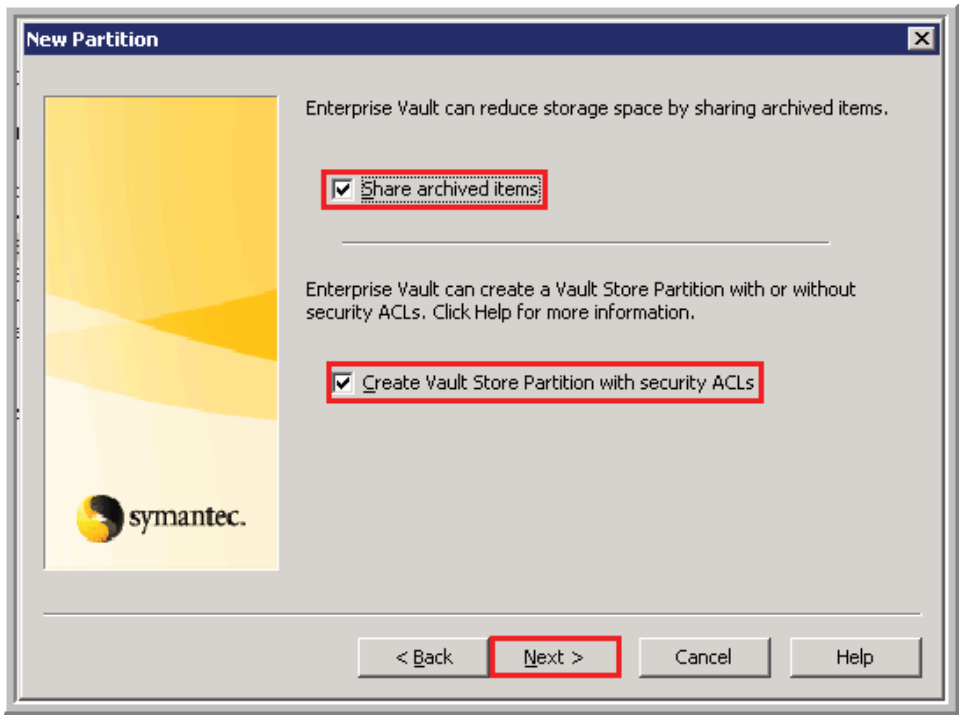
Select NTFS for the Storage type and click on Next.



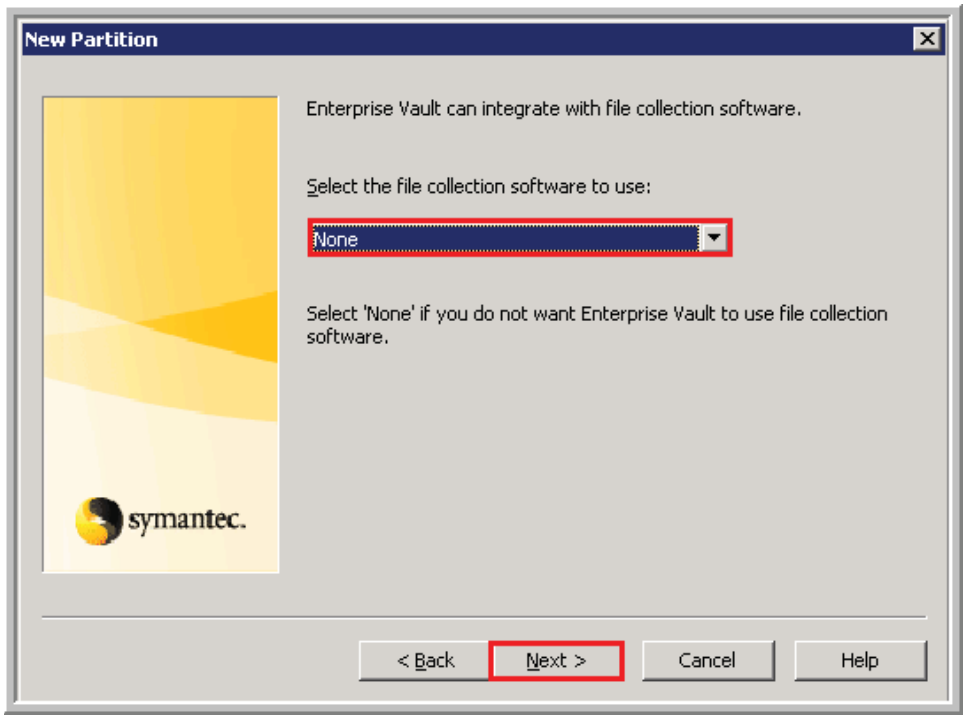
Select the V drive for the Vault with the default partition location and click on Next.



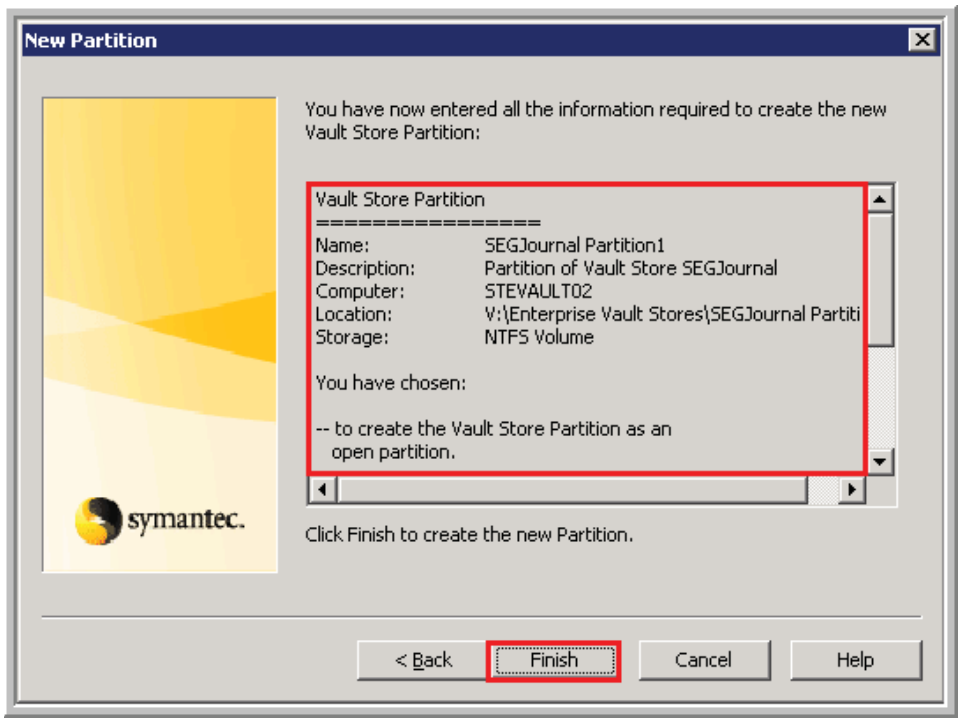
Confirm Share archived items and Create Vault Store Partition are checked and click on Next.



Do not select any file collection software and click on Next.

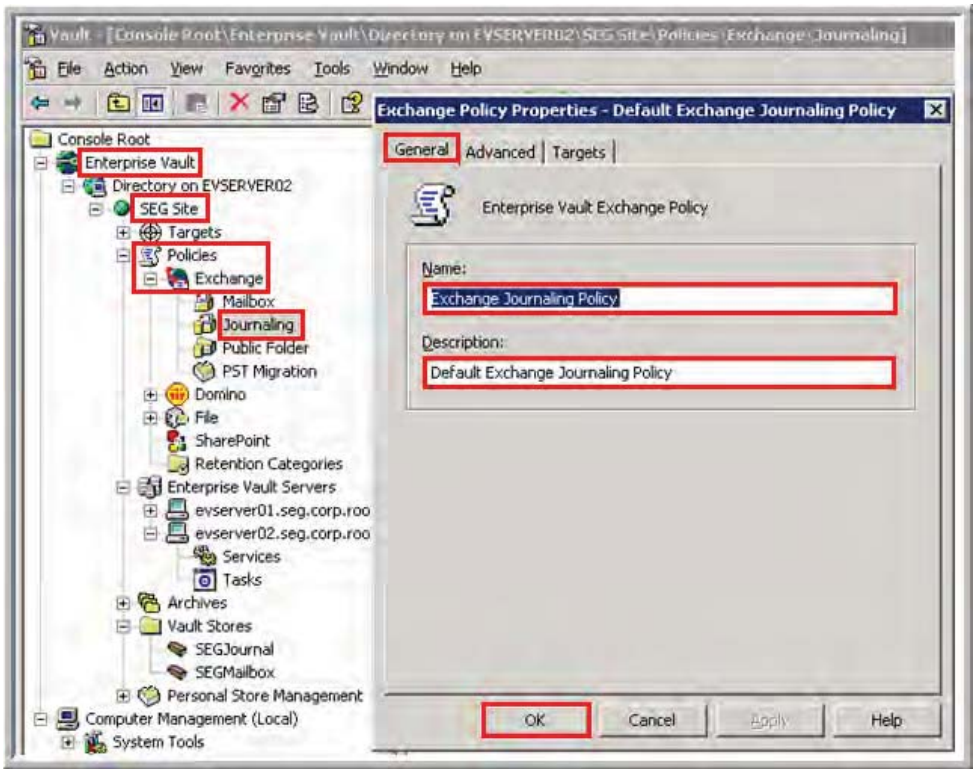


Confirm settings and click on Finish and then Close on the next window.

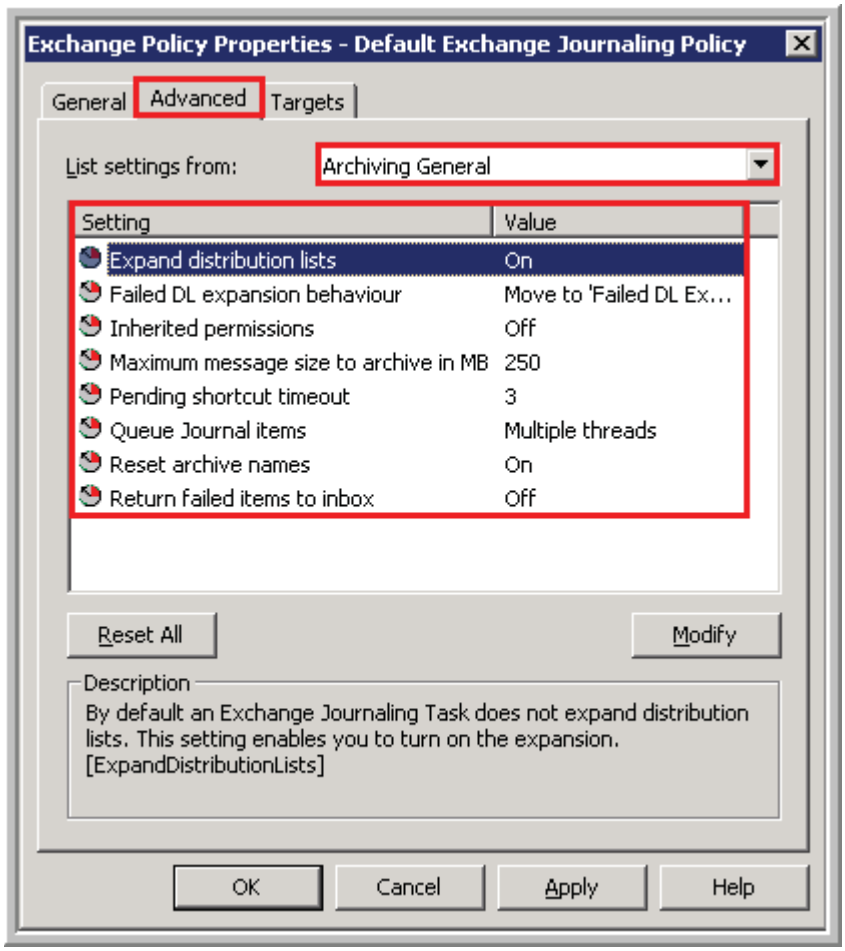


Configure the Journaling Policy

Configure the Exchange Journaling Policy by going to Policies –> Exchange –> Journaling with the name Exchange Journaling Policy. This same policy will apply to the company and parent companies journals.

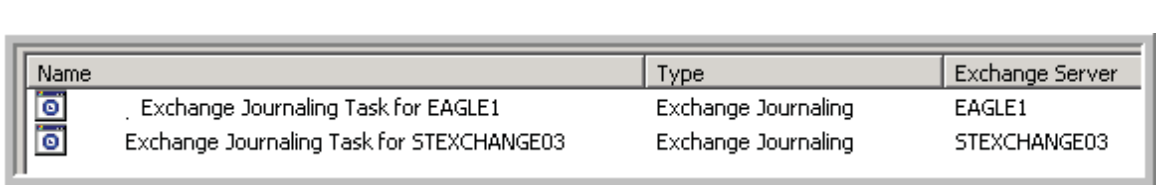


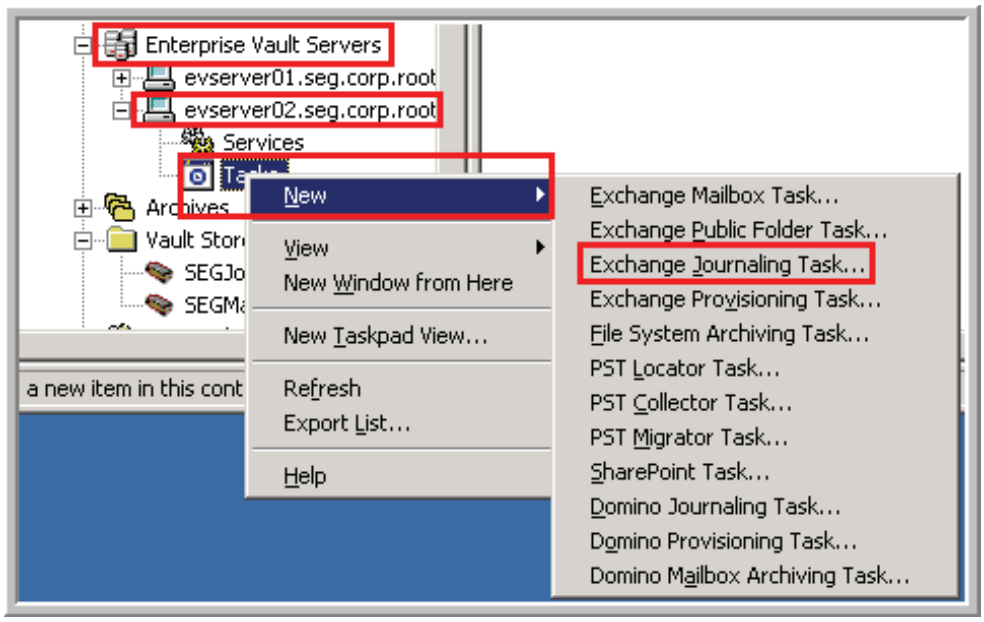
Click on the Advanced Tab and confirm the settings match what is displayed below other than the Return Failed Items to Inbox – this setting should be turned “On”.



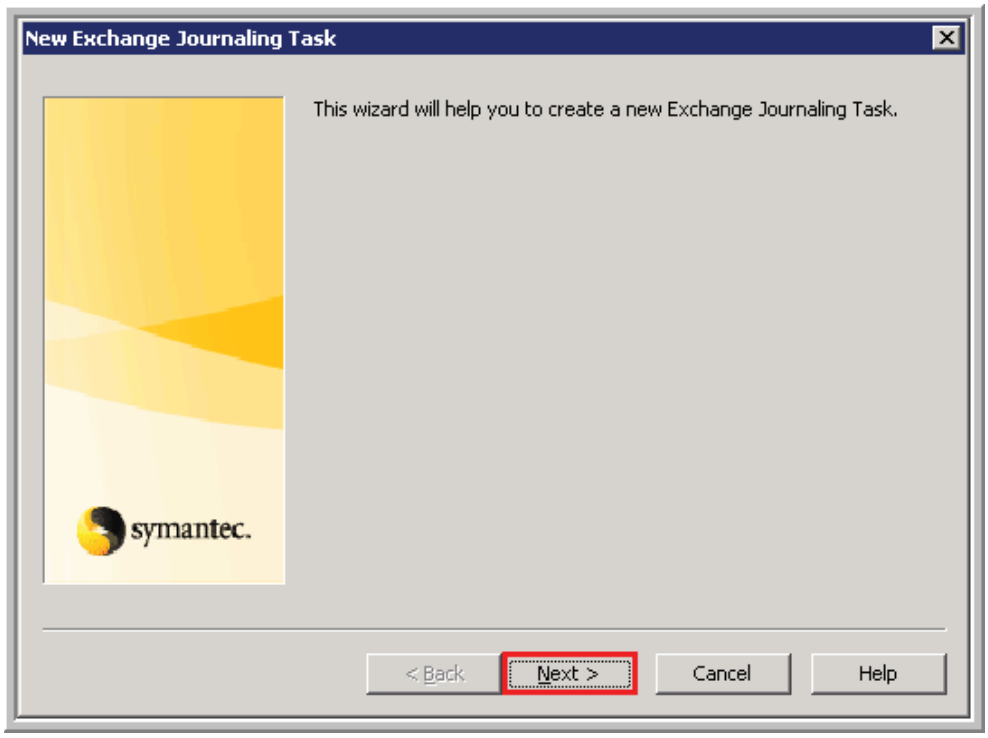
Configure the Journaling Task

Browse to Enterprise Vault Servers > evserver02.seg.corp.root and then right click on New > Exchange Journaling Task. Create a journaling task like pictured below for EAGLE1 and STEXCHANGE03 since these are where the 8 journal mailboxes are located.

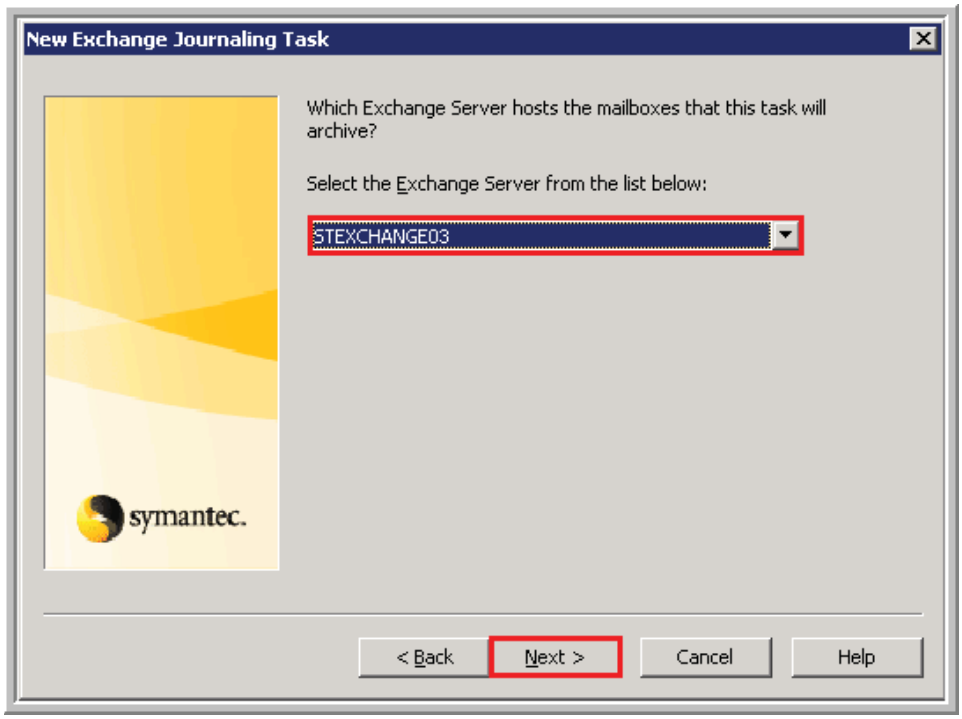




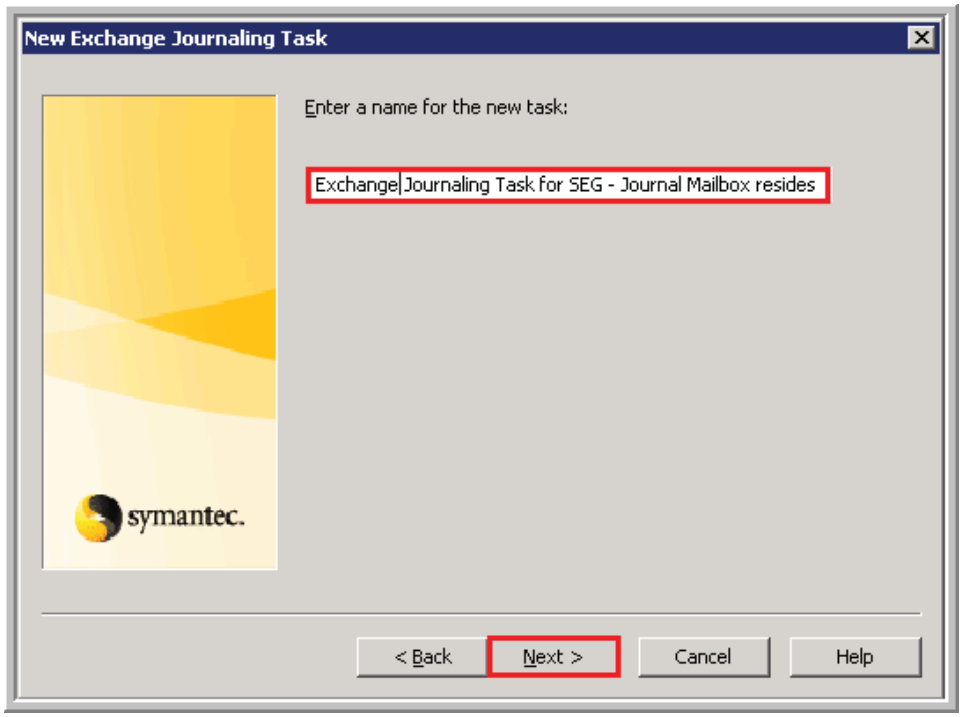
Click on Next.



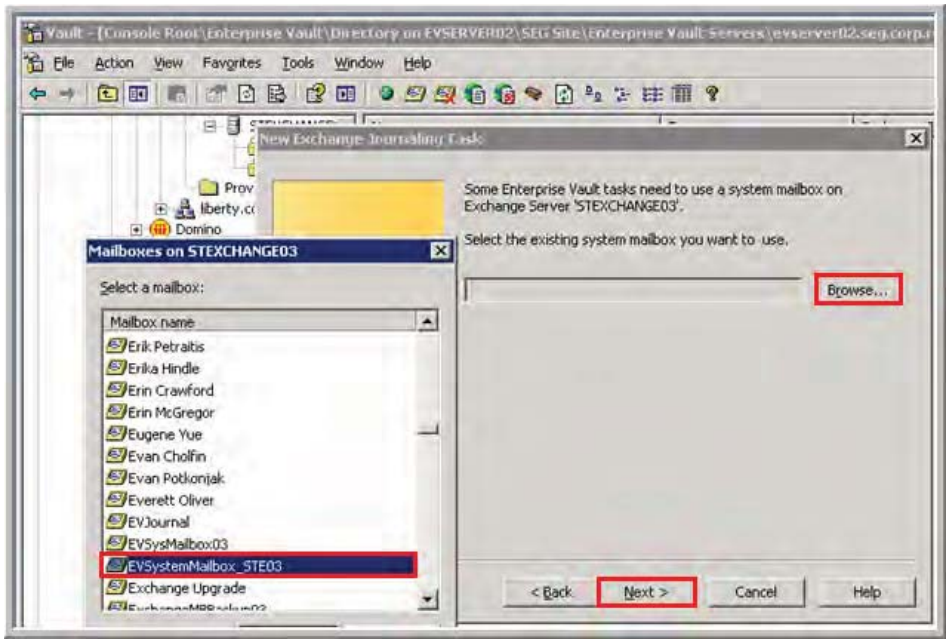
Select the Exchange Server – Note you must create a task for every server you are journaling, but in this case all mail is sent to the EVJournal mailbox located on STEXCHANGE03.



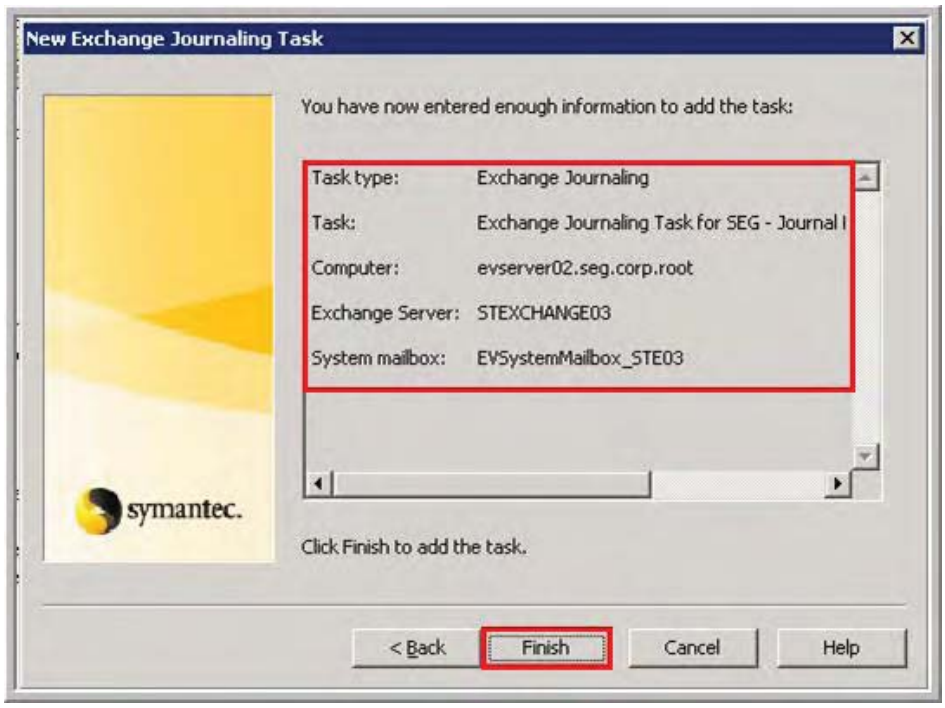
Enter the name for the task, Exchange Journaling Task for SEG – Journal Mailbox resides on STEXCHANGE03.

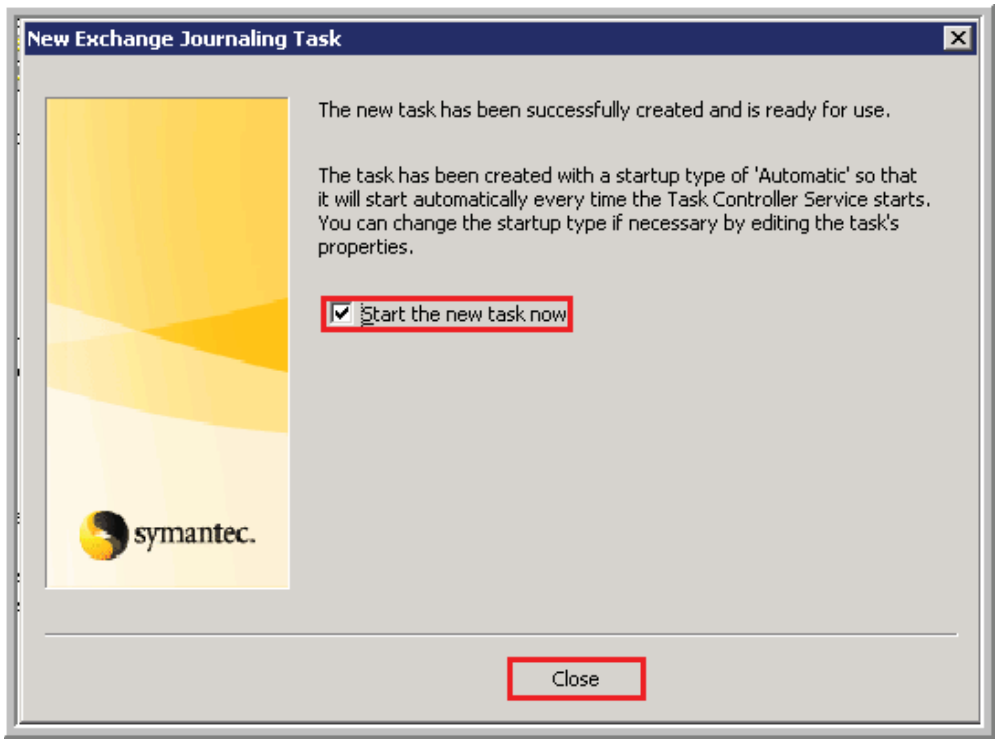


Select the System Mailbox – EVSystemMailbox_STE03 (Enterprise Vault Notification) and then click on Next. Note this is not the same mailbox that journaled mail is sent to.



Confirm the settings and click on Finish and then ensure that Start the new task now is checked and click on Close.

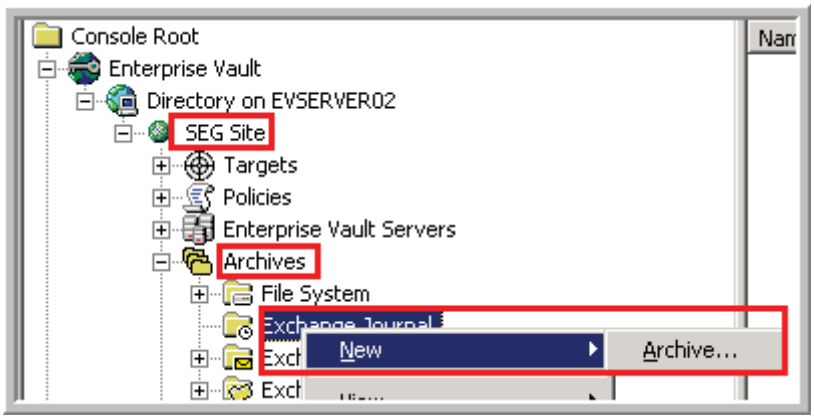




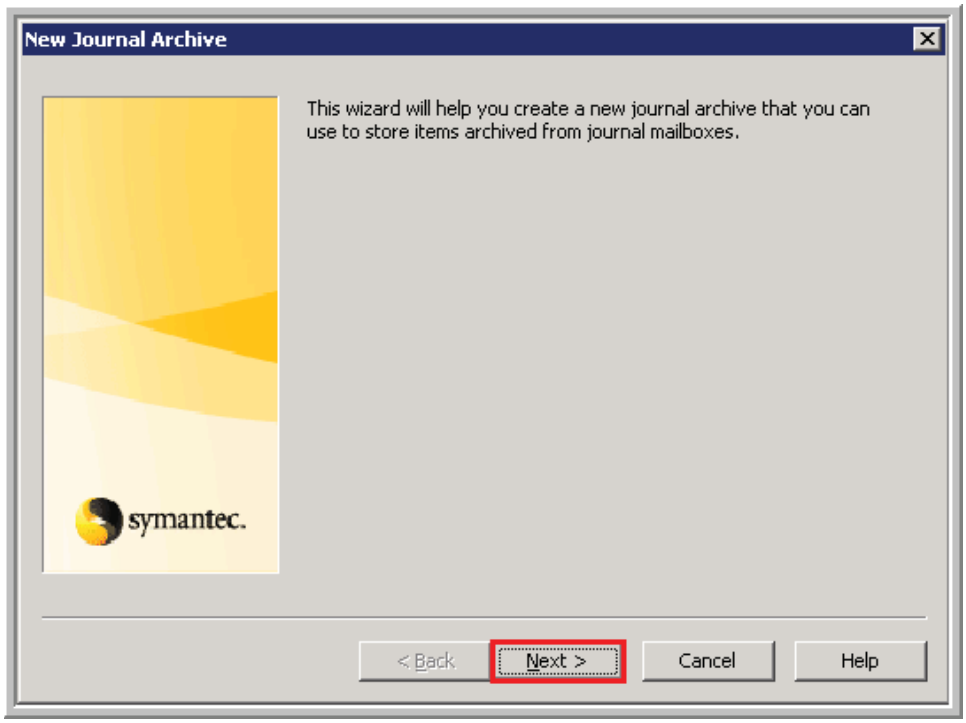
Create a Journal Archive

Browse to Archives and right click on Exchange Journal and click on New > Archive. See table in Step 1 regarding the Journal Archives that need created (see screenshot below for final list) and the mailboxes that will be used.

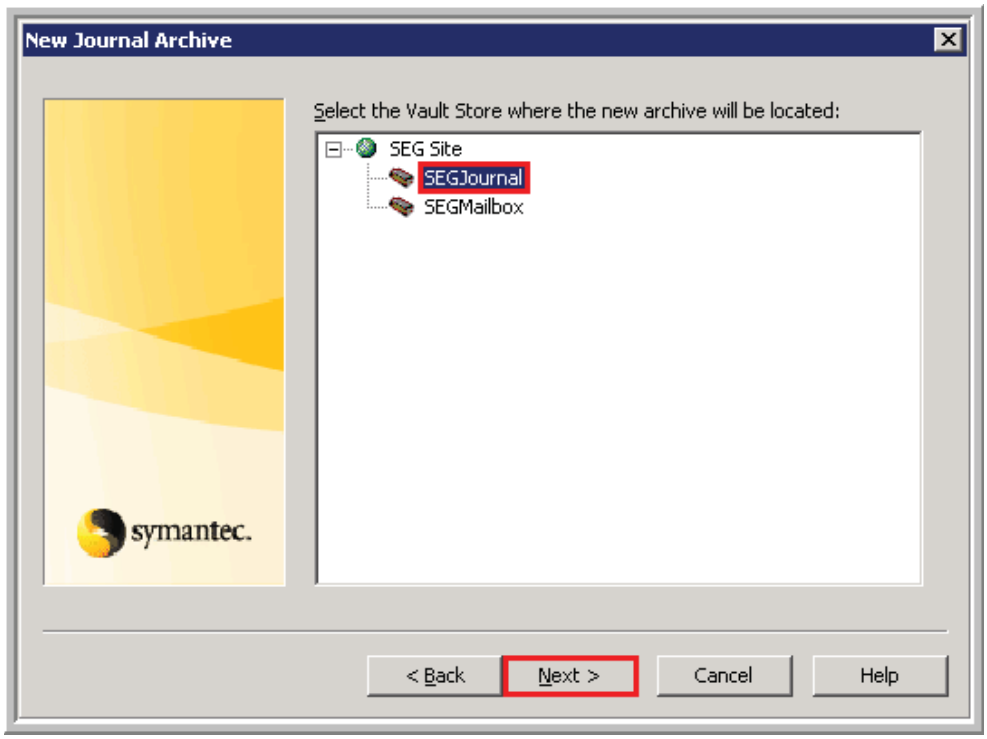




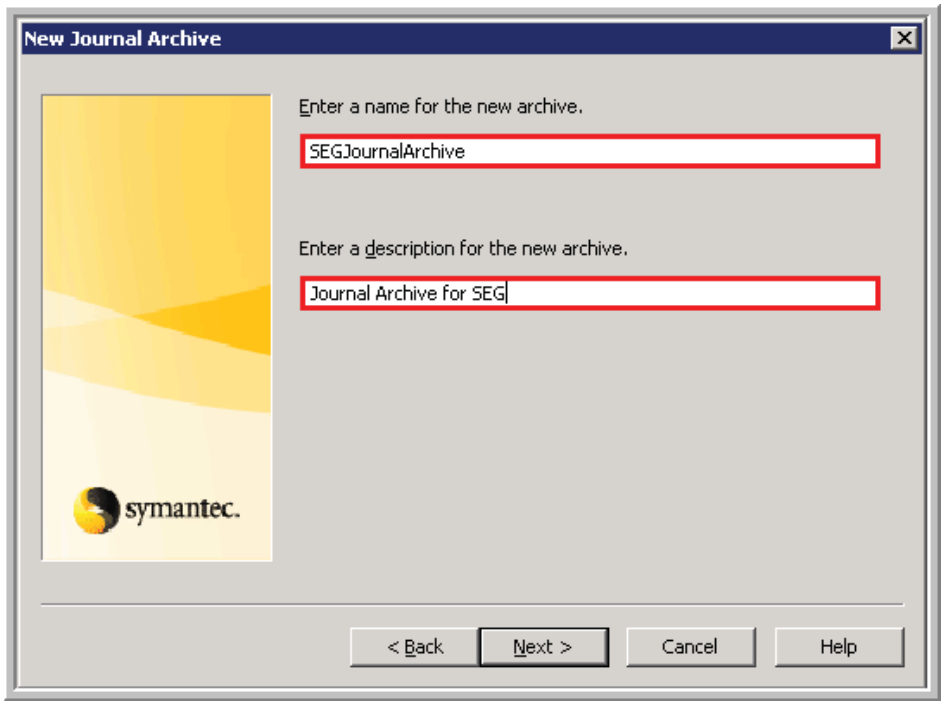
Click on Next.



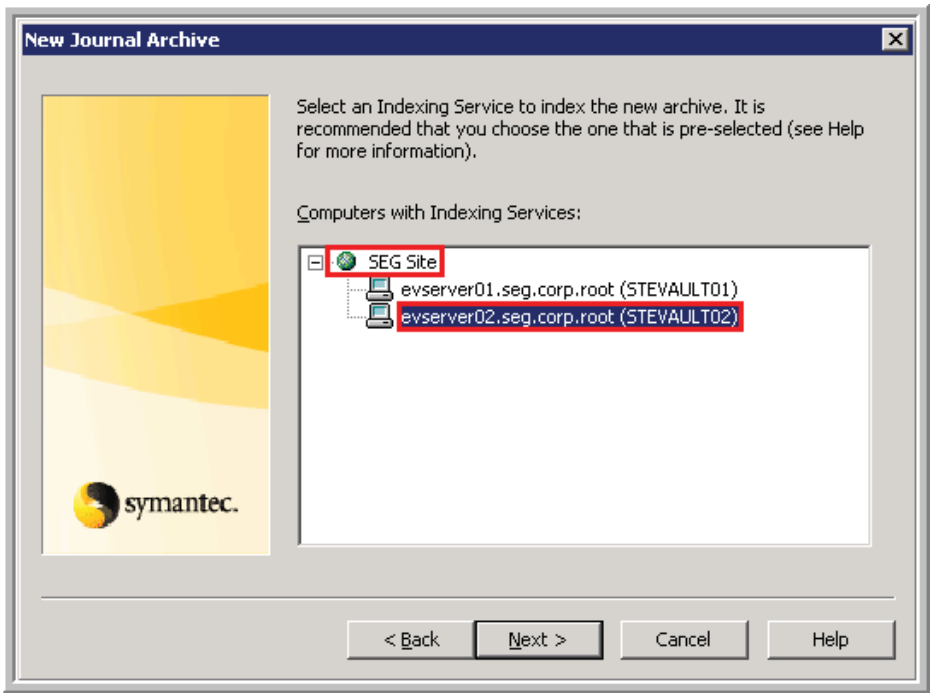
Select the Vault Store SEGJournal and click on Next.



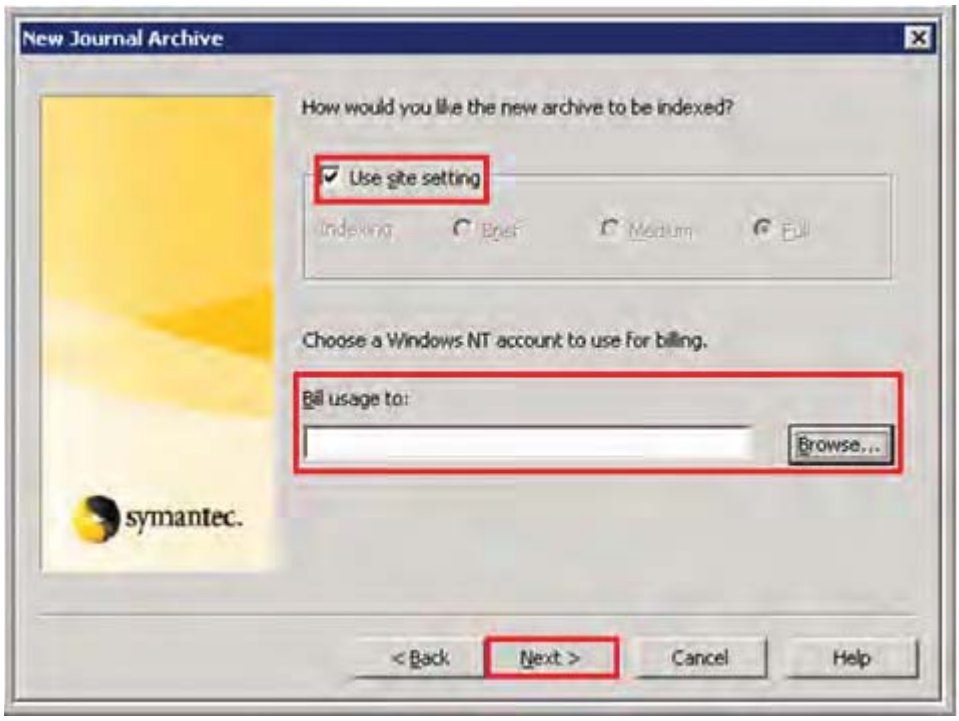
Enter the name SEGJournalArchive for the archive name and Journal Archive for SEG for the description.



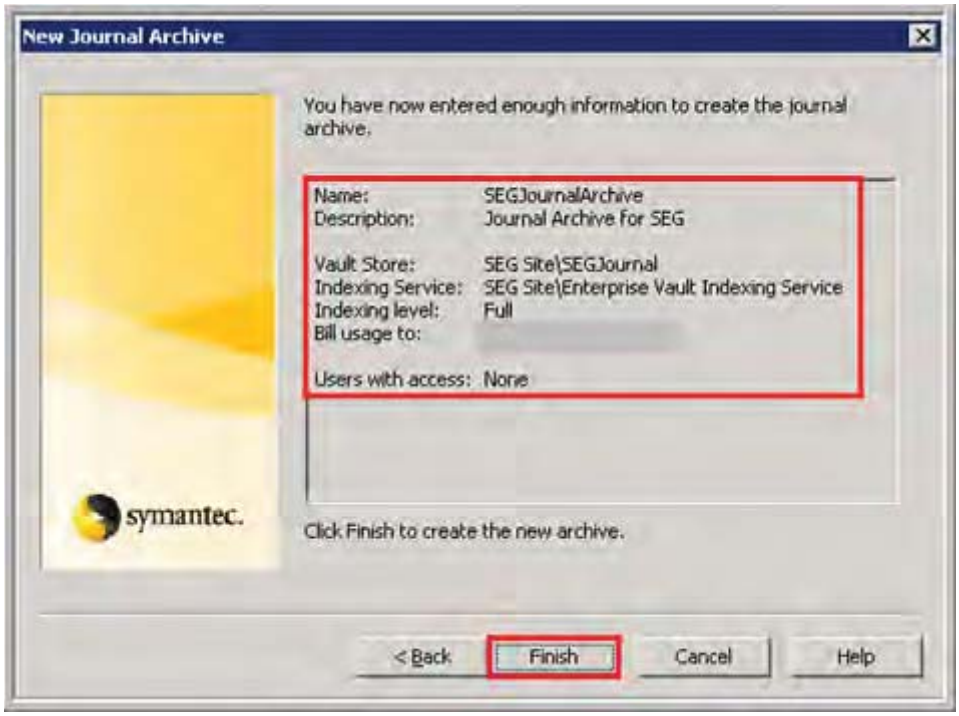
Select evserver02.seg.corp.root and click on Next.

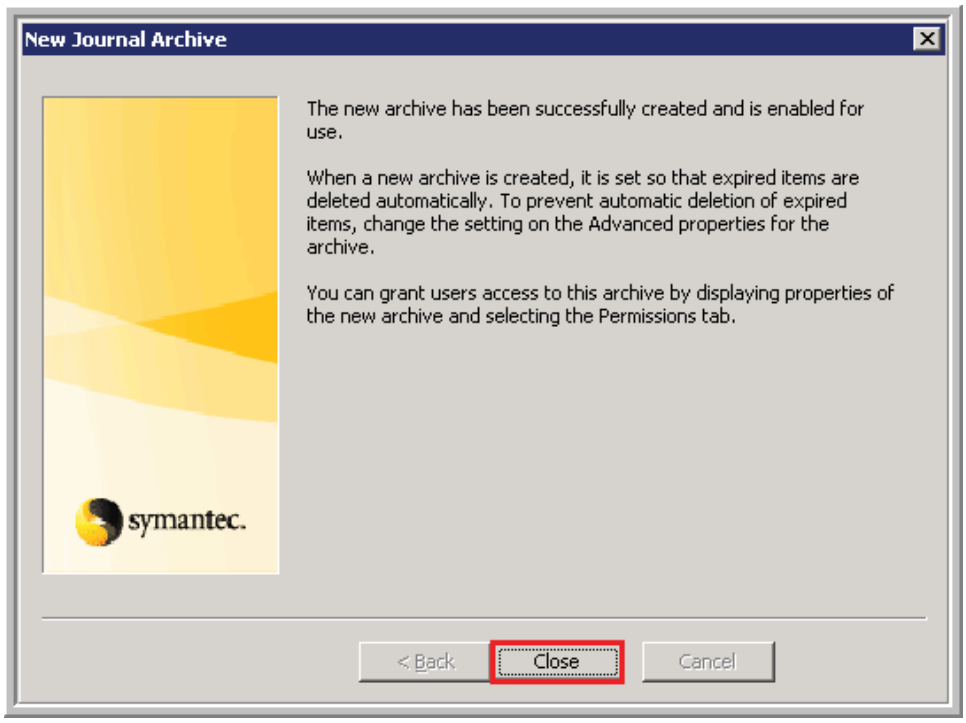


Check the box for Use site setting and then Bill usage to Encore\EVJournal.



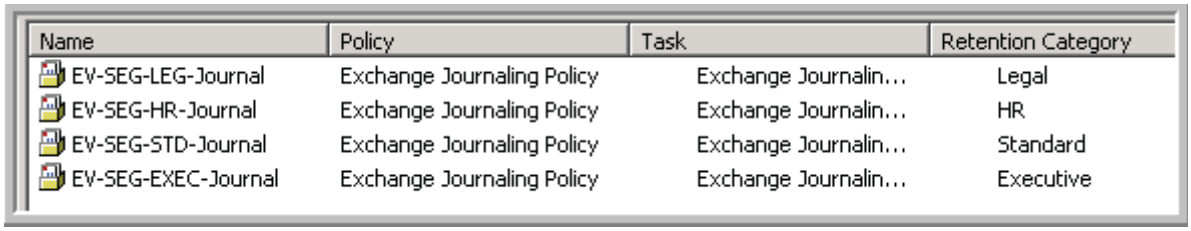
Confirm settings and click on Finish and then Close.



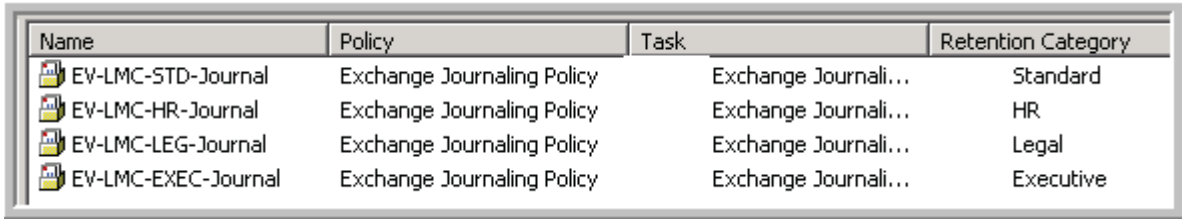


Create a Journal Mailbox Target

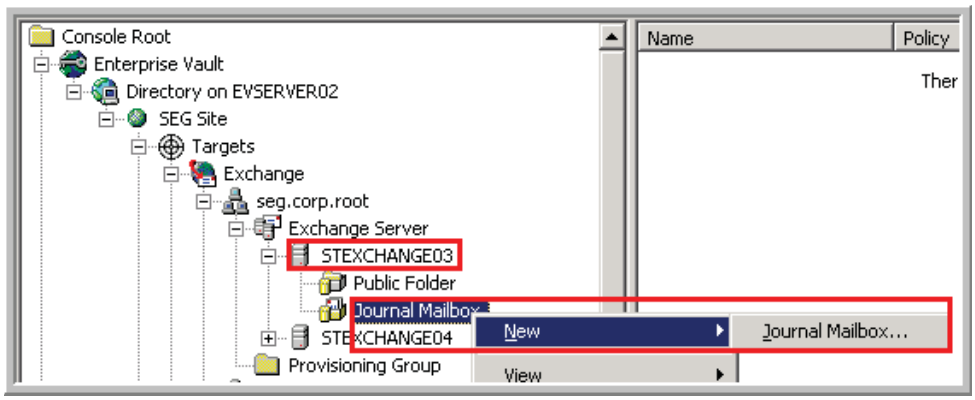
Browse to the SEG Site > Targets > Exchange > seg.corp.root (and parent.corp.root for the parent company) > Exchange Server > STEXCHANGE03 (and EAGLE1 for the parent company) and right click on Journal Mailbox and click New > Journal Mailbox. See screenshots below for Journal Mailboxes.



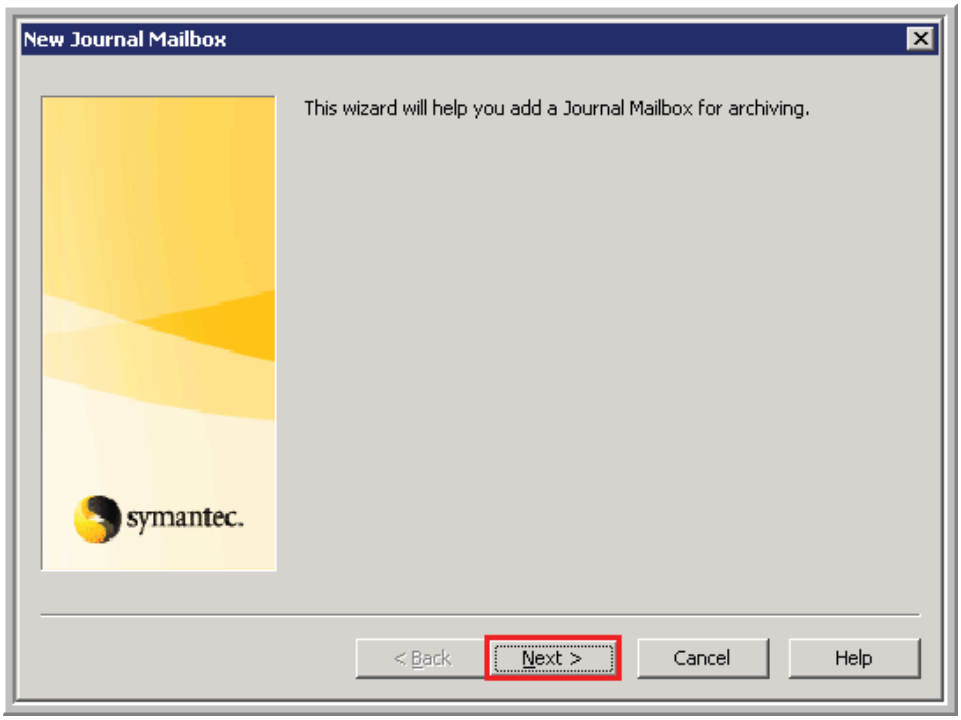
Name	Policy	Task	Retention Category
EV-SEG-LEG-Journal	Exchange Journaling Policy	Exchange Journalin...	Legal
EV-SEG-HR-Journal	Exchange Journaling Policy	Exchange Journalin...	HR
EV-SEG-STD-Journal	Exchange Journaling Policy	Exchange Journalin...	Standard
EV-SEG-EXEC-Journal	Exchange Journaling Policy	Exchange Journalin...	Executive



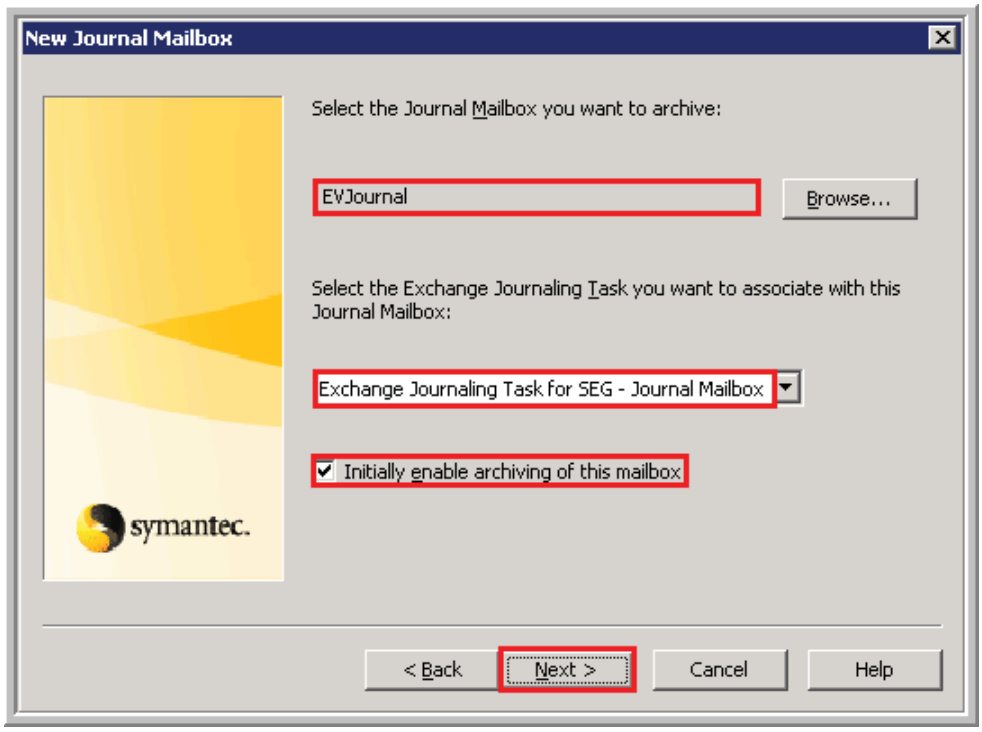
Name	Policy	Task	Retention Category
EV-LMC-STD-Journal	Exchange Journaling Policy	Exchange Journali...	Standard
EV-LMC-HR-Journal	Exchange Journaling Policy	Exchange Journali...	HR
EV-LMC-LEG-Journal	Exchange Journaling Policy	Exchange Journali...	Legal
EV-LMC-EXEC-Journal	Exchange Journaling Policy	Exchange Journali...	Executive



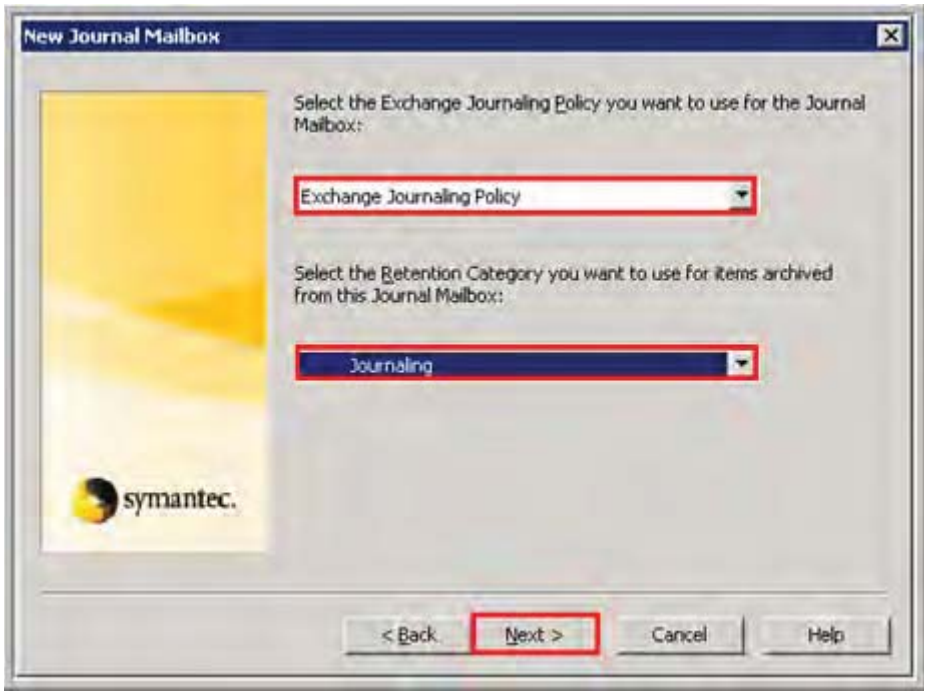
Click on Next.



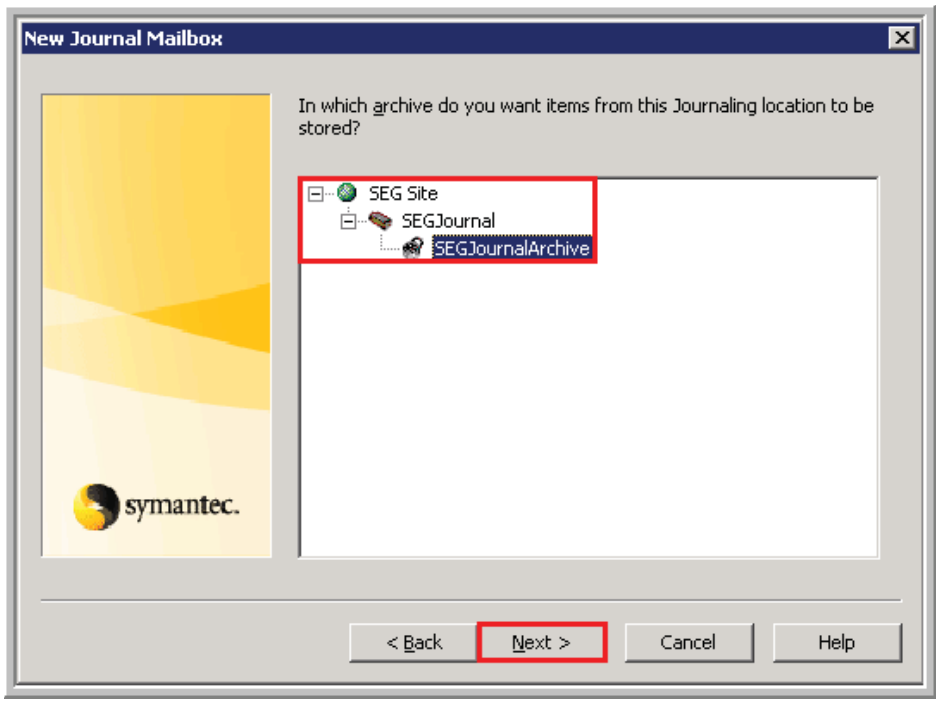
Browse to select the mailbox and then select the Exchange Journaling task, i.e. EV-SEG-EXEC-Journal and the company Exchange Journaling Task for STEXCHANGE03 and check the box to enable it and click on Next.



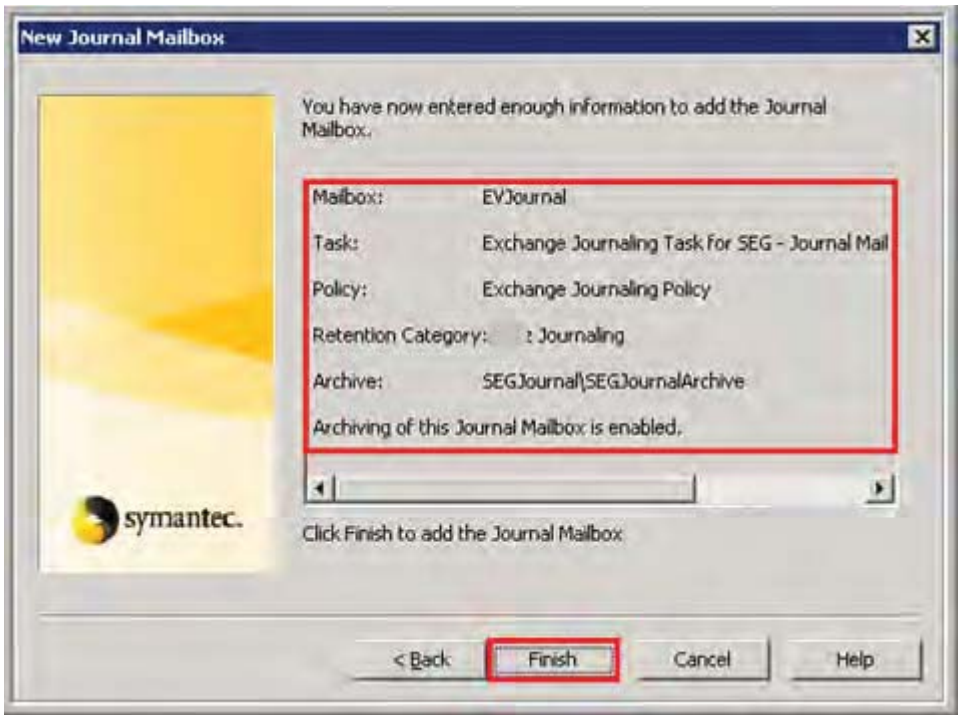
Select the Exchange Journaling Policy and the matching retention category and click on Next.



Select the SEGJournalArchive and click on Next.



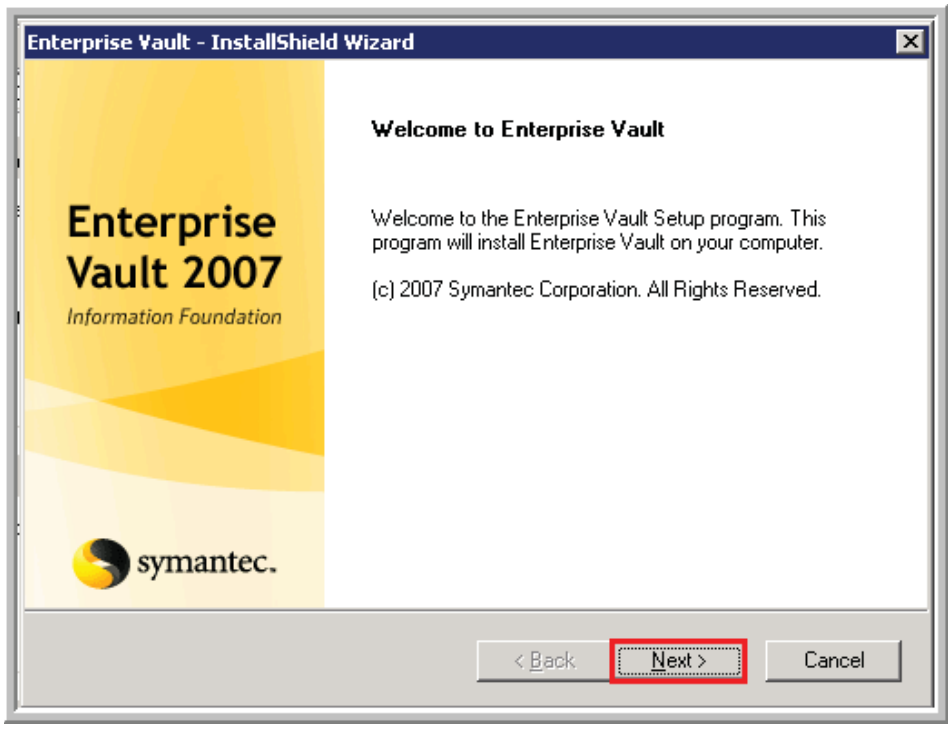
Confirm the settings and click on Finish and click on Close in the next window.



Appendix F

Reporting and Operations Manager

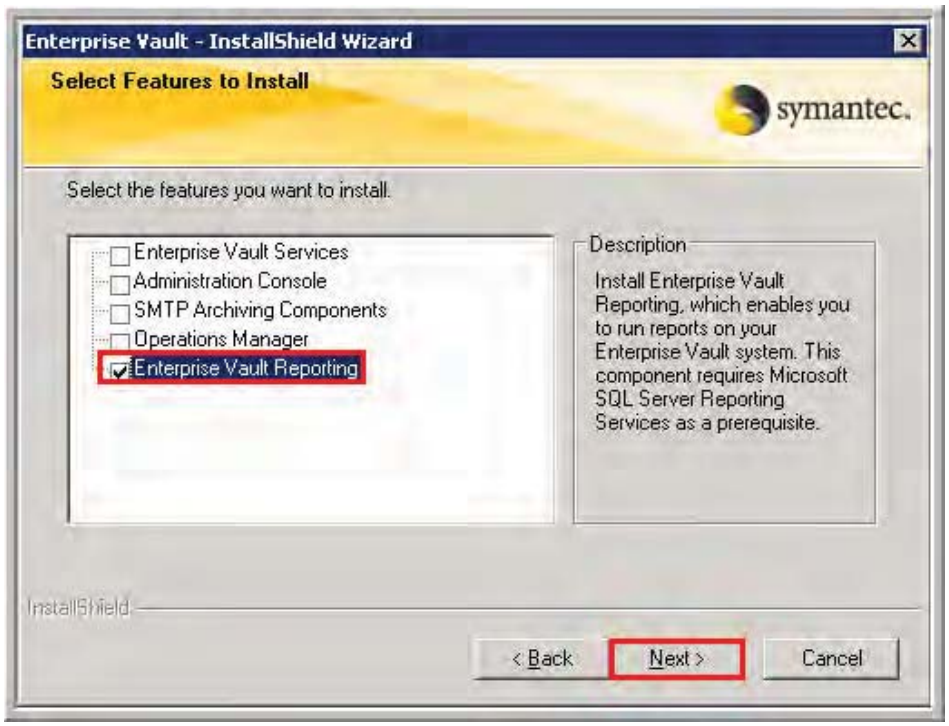
Logon to the SQL server with the VaultAdmin account and run setup.exe from the Enterprise Vault 2007 installation files and click on Next and Yes for the license.



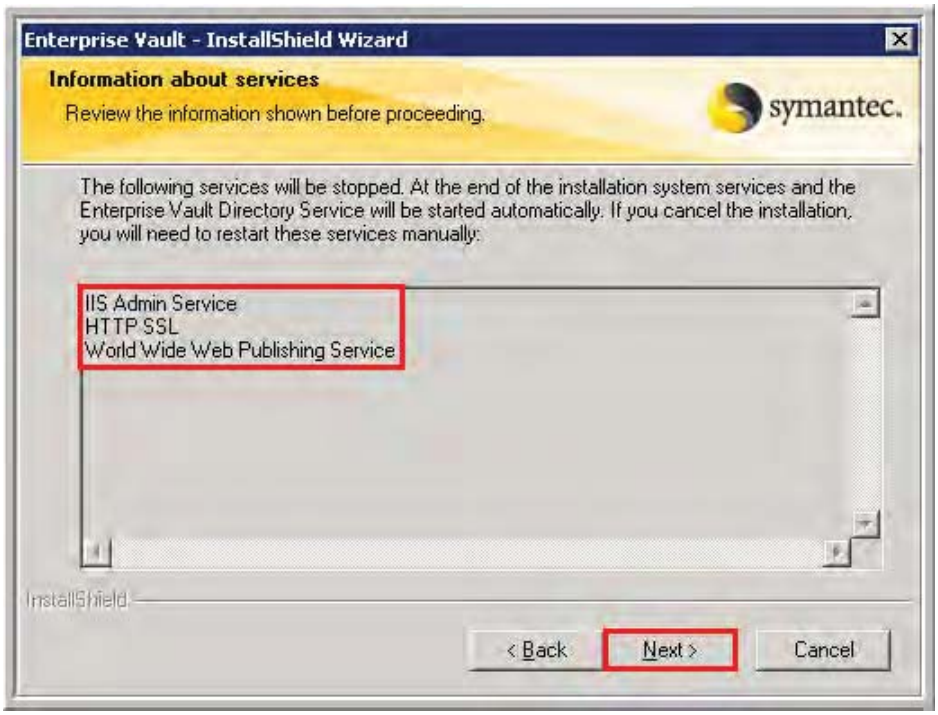
Confirm the default install location and click on Next.



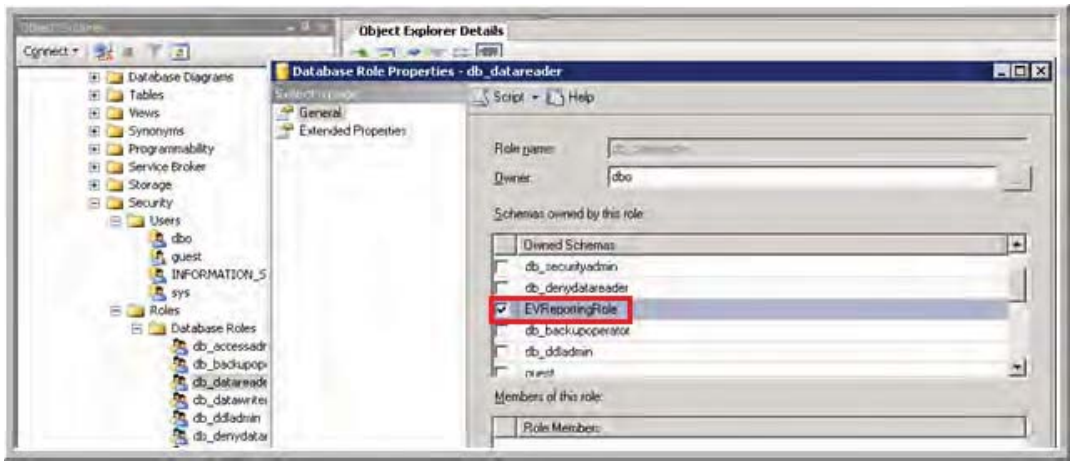
Select only the Enterprise Vault Reporting to be installed and click on Next.



Click on Next and Finish.

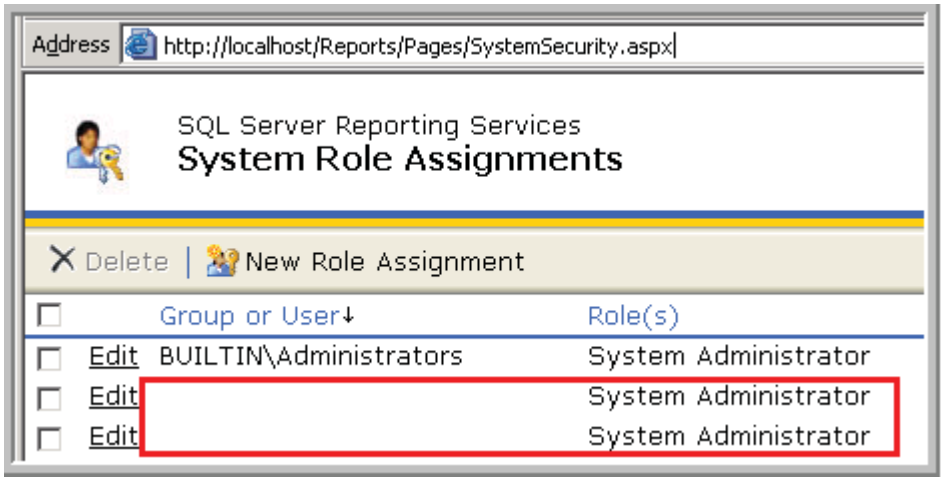


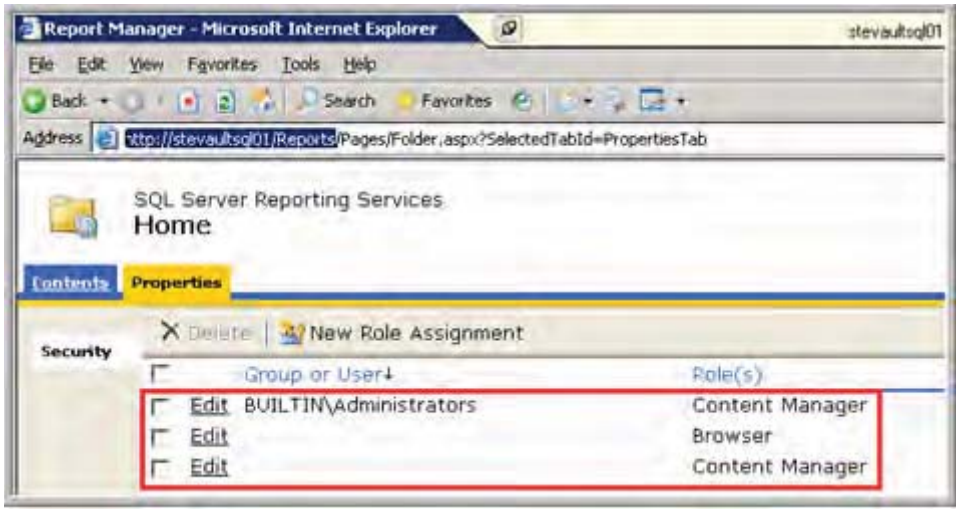
Go into the DB roles and grant ev_reporting the dbdatareader role to all of the Enterprise Vault databases.



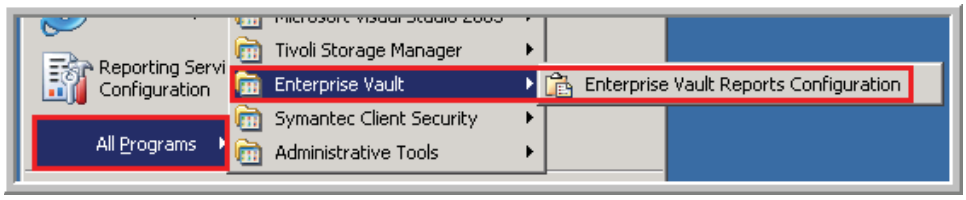
Grant ev_reporting local administrator rights on STEVAULTSQL01 and then launch the following web page and grant svcreporting and VaultAdmin the system administrator and content manager roles.

http://localhost/Reports/Pages/SystemSecurity.aspx

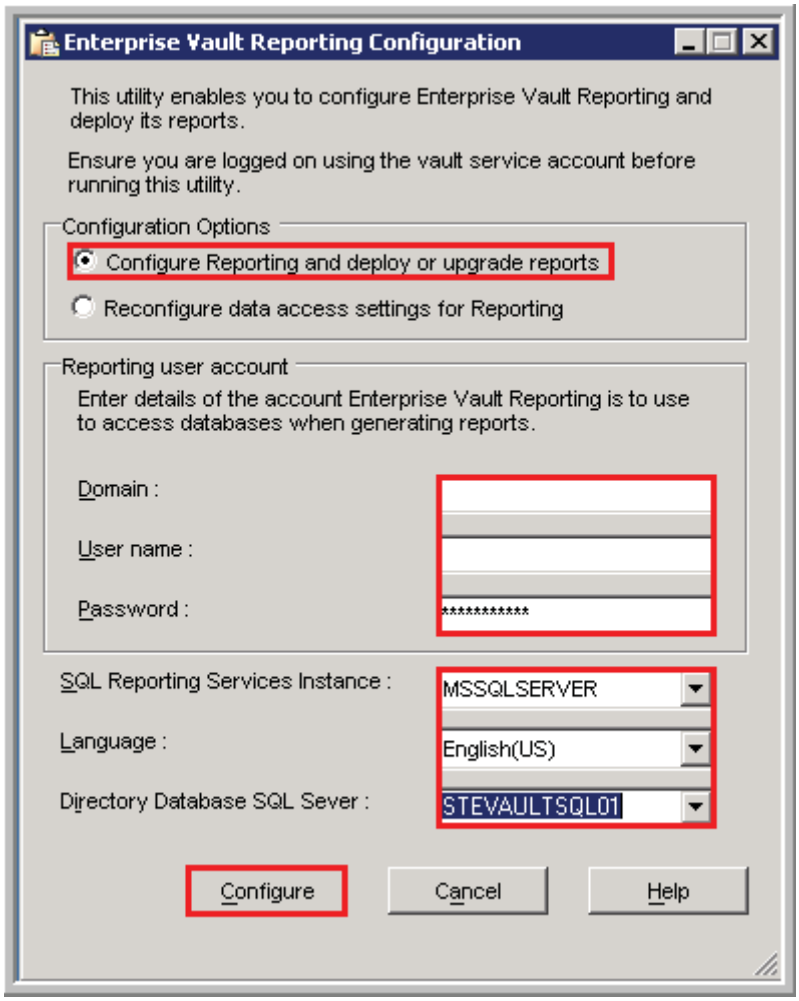




Go to All Progams > Enterprise Vault > Enterprise Vault Reports Configuration.

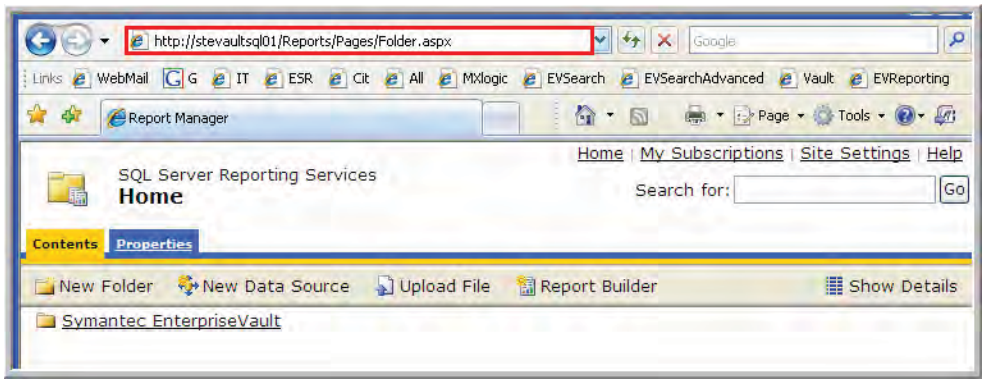


Enter the username svc_reporting and the fully qualified domain and run the configuration.



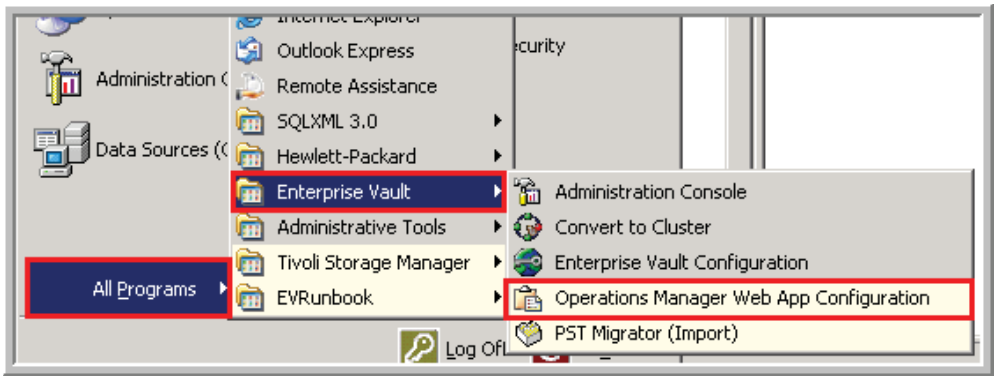
Once it completes test by launching the report monitoring website -

http://stevaultsql01/Reports/Pages/Folder.aspx

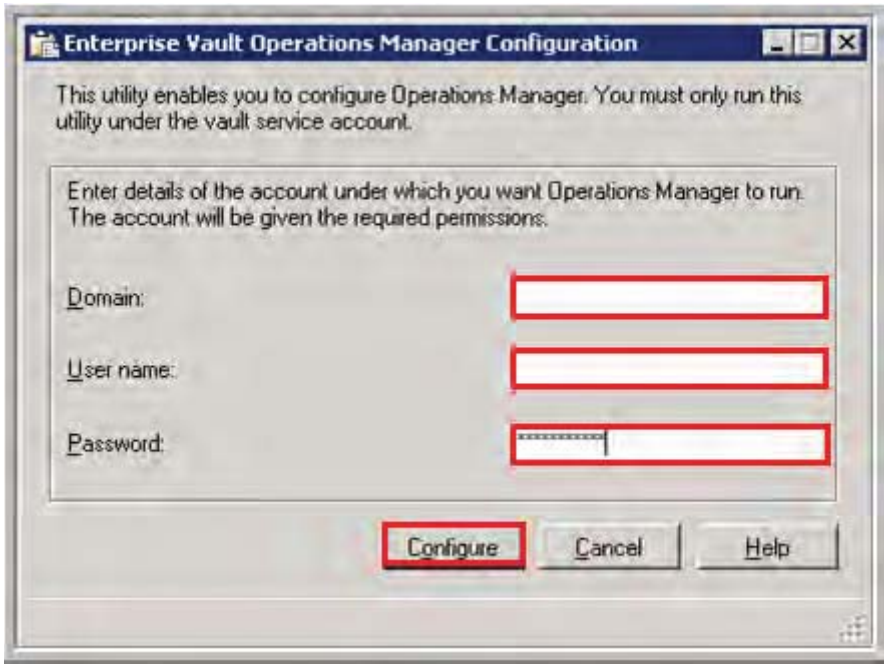


Install Operations Manager

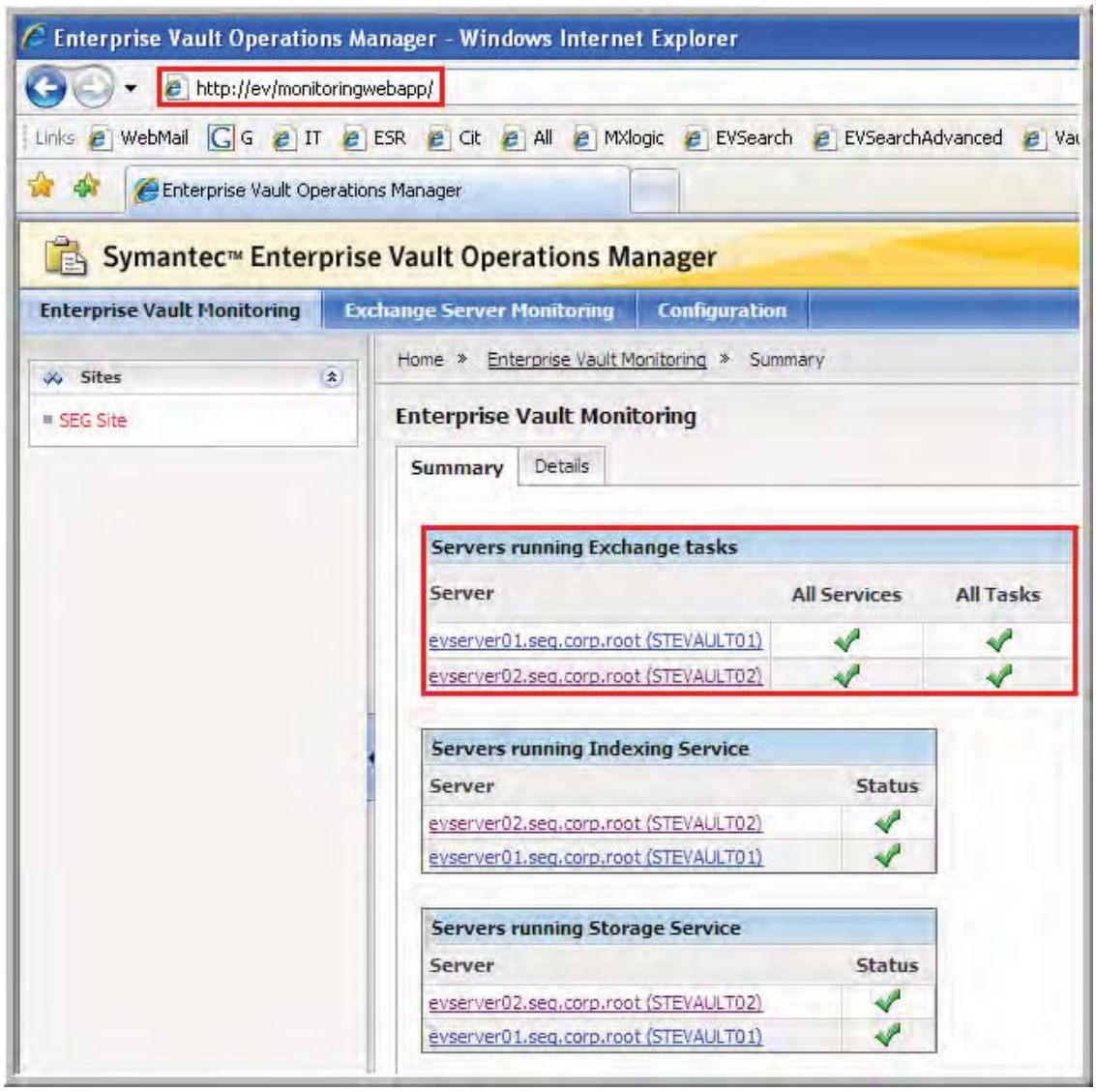
Install Enterprise Vault Operations Manager (OVOM) on STEVAULT01. Go to All Programs > Enterprise Vault > Operations Manager Web App Configuration.



Enter the domain and user account VaultAdmin.



Confirm that you can get to the website and see the Enterprise Vault servers and their status. http://ev/monitoringwebapp/



Appendix G

Discovery Accelerator

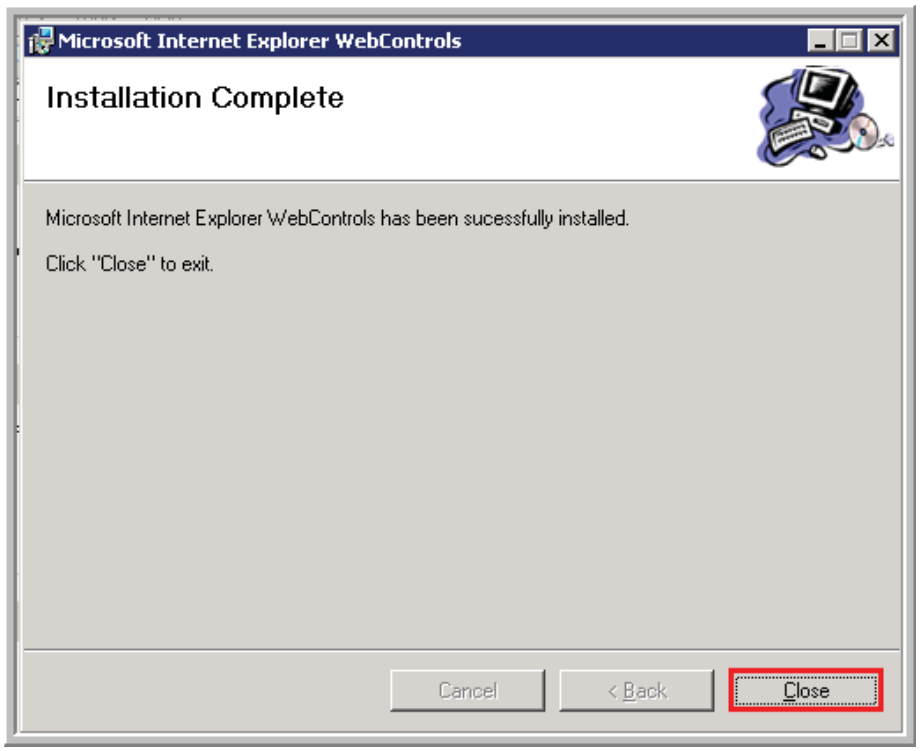
Discovery Accelerator is tightly integrated with Enterprise Vault and cannot be installed and configured until Enterprise Vault is operational.

First install the Internet Web Controls.



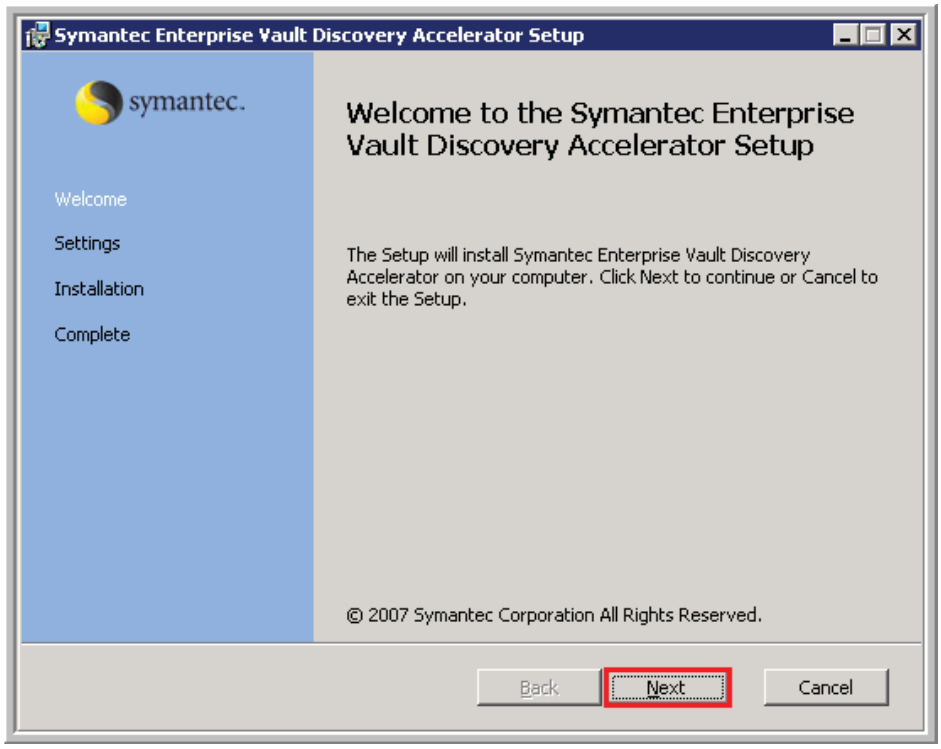
Accept the license agreement and click on Next and then Next on the following screen.

Click on Close after the install is confirmed.

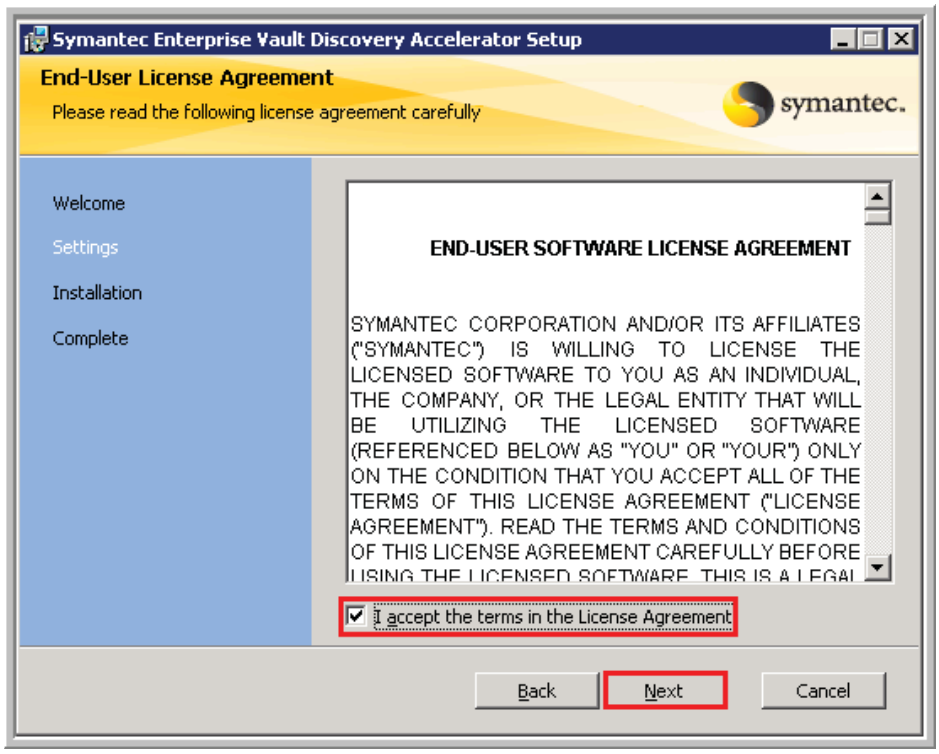


Run daccel_en.msi.

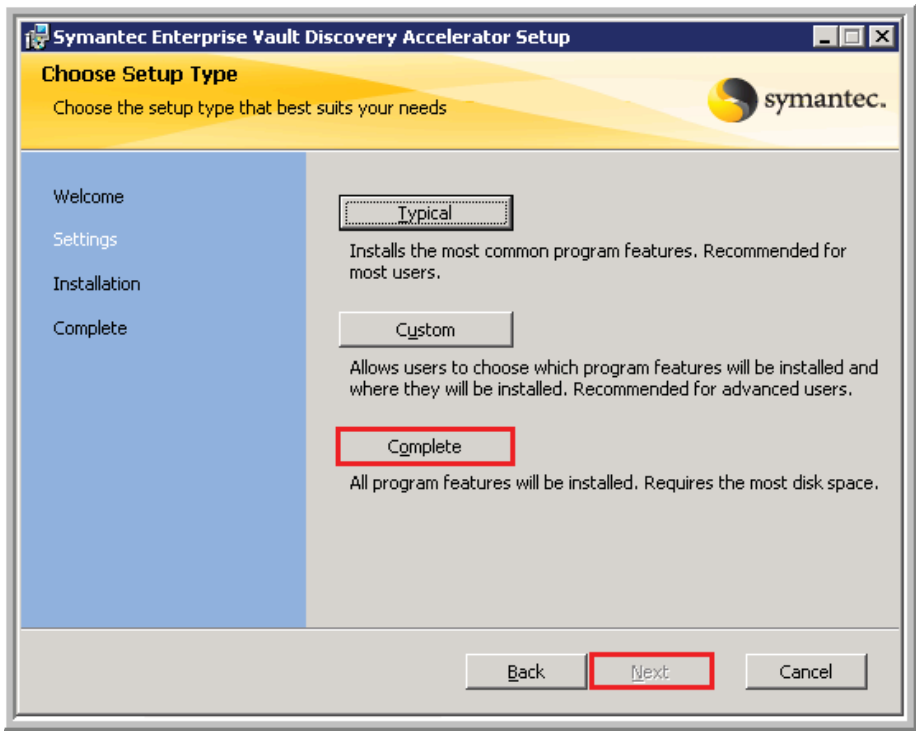
Click on Next for the Enterprise Vault Discovery Accelerator Setup.



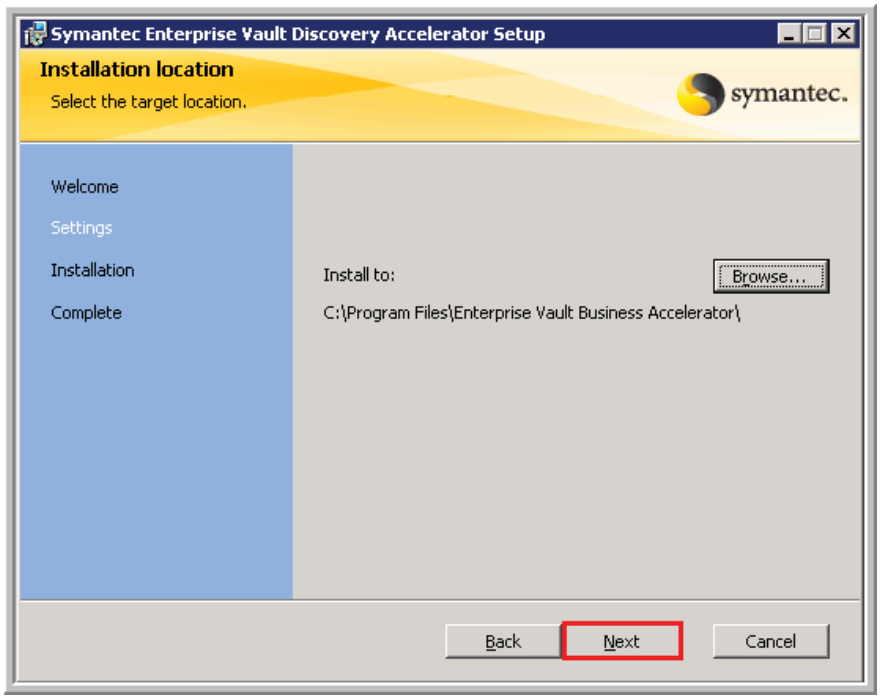
Check the box to accept the license agreement and click on Next.



Click on Complete and Next.



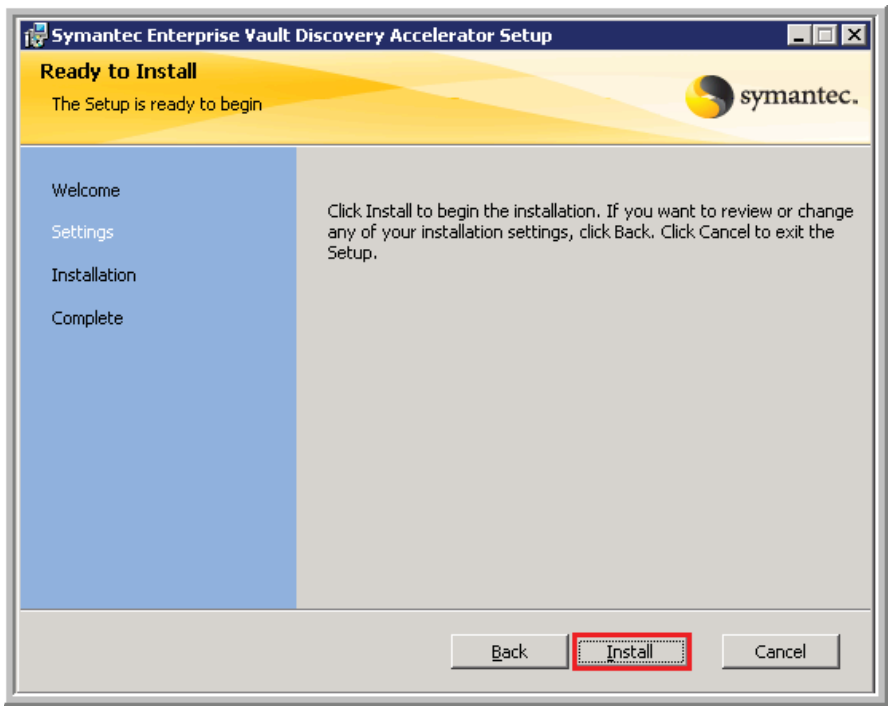
Confirm the installation location and click on Next. If there is an application partition install it to that location.



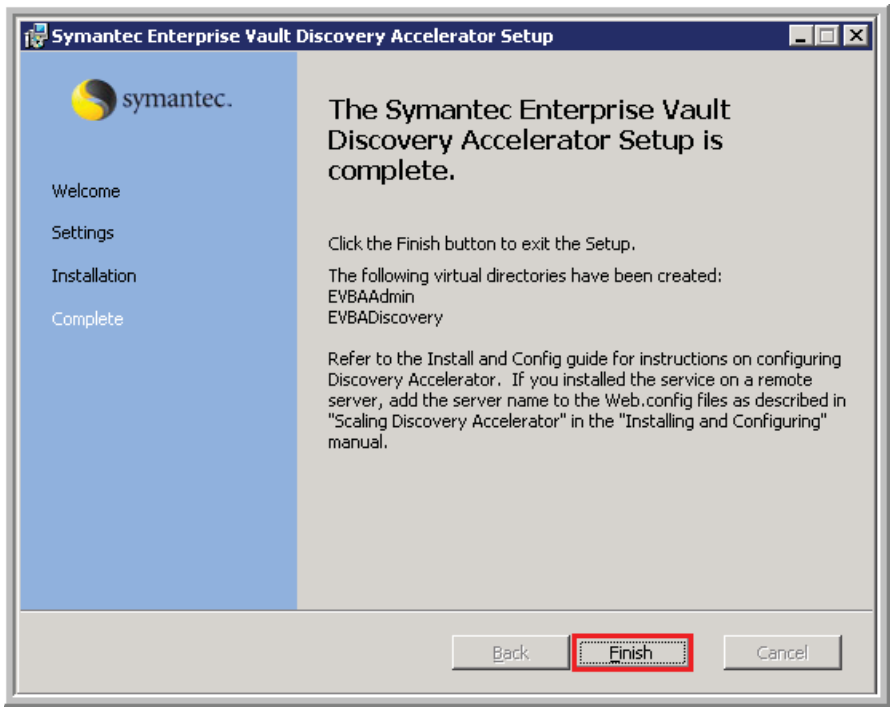
Enter the Vault Admin domain, username (VaultAdmin) and password.



Click on Install.



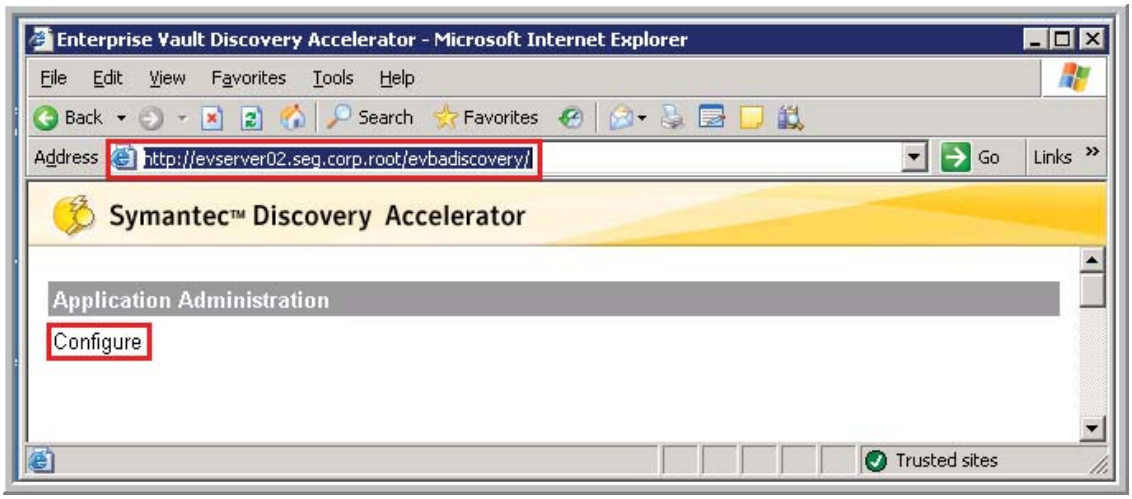
Click on Finish and reboot the system.



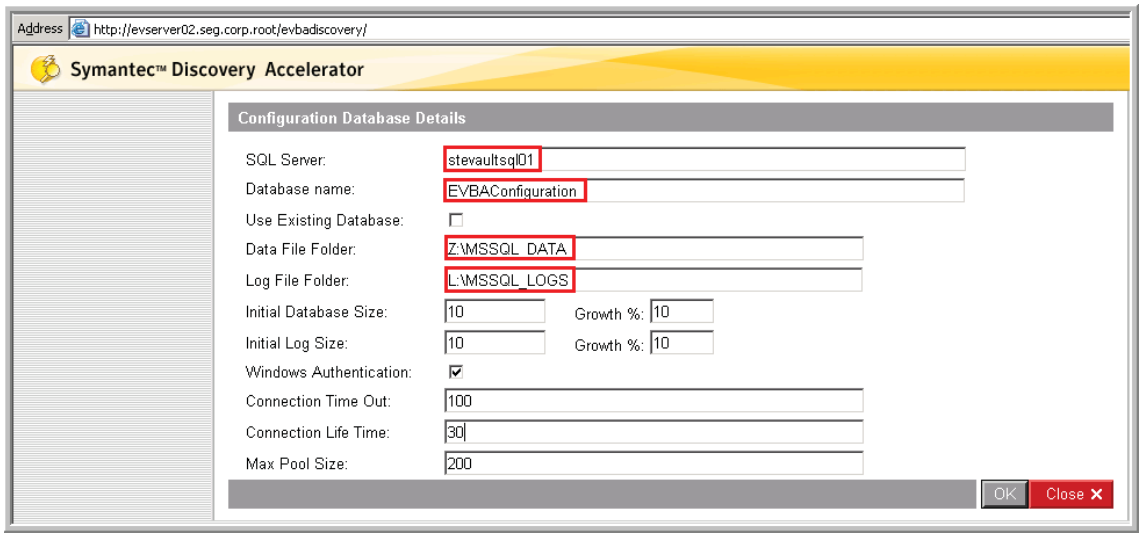
Copy the licenses from the Program Files\Enterprise Vault\Installed Licenses folder to Program Files\Enterprise Vault Business Accelerator and then restart the Enterprise Vault Accelerator Manager Service.

Configure Discovery Accelerator

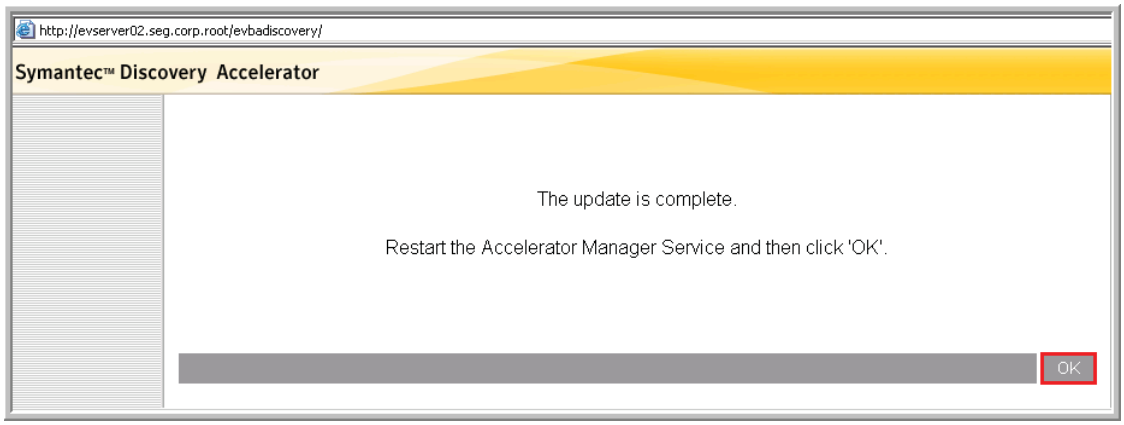
Go to http://evserver02.seg.corp.root/evbadiscovery/ and click on Configure.



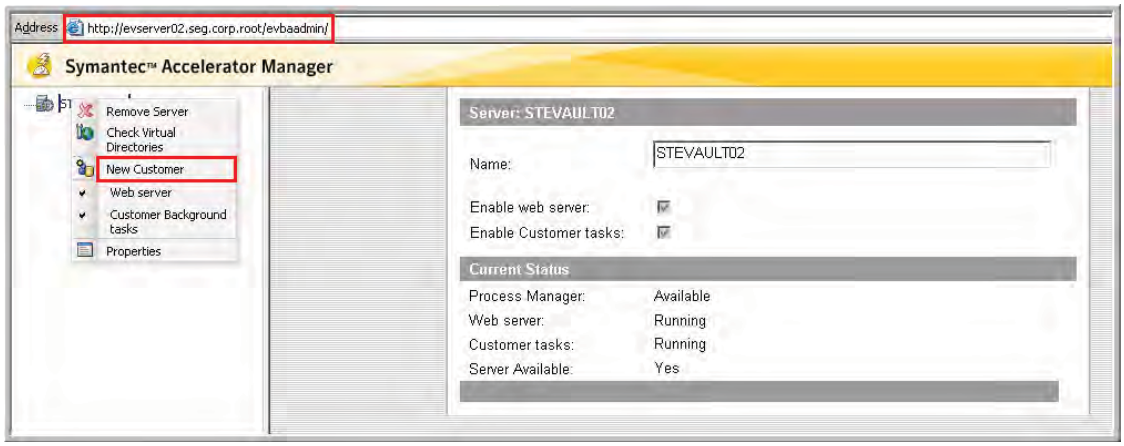
Enter the SQL server “stevaultsql01” and the database name “EVBAConfiguration” and the data and log locations, “Z:\MSSQL_DATA” and “L:MSSQL_LOGS” and click OK.



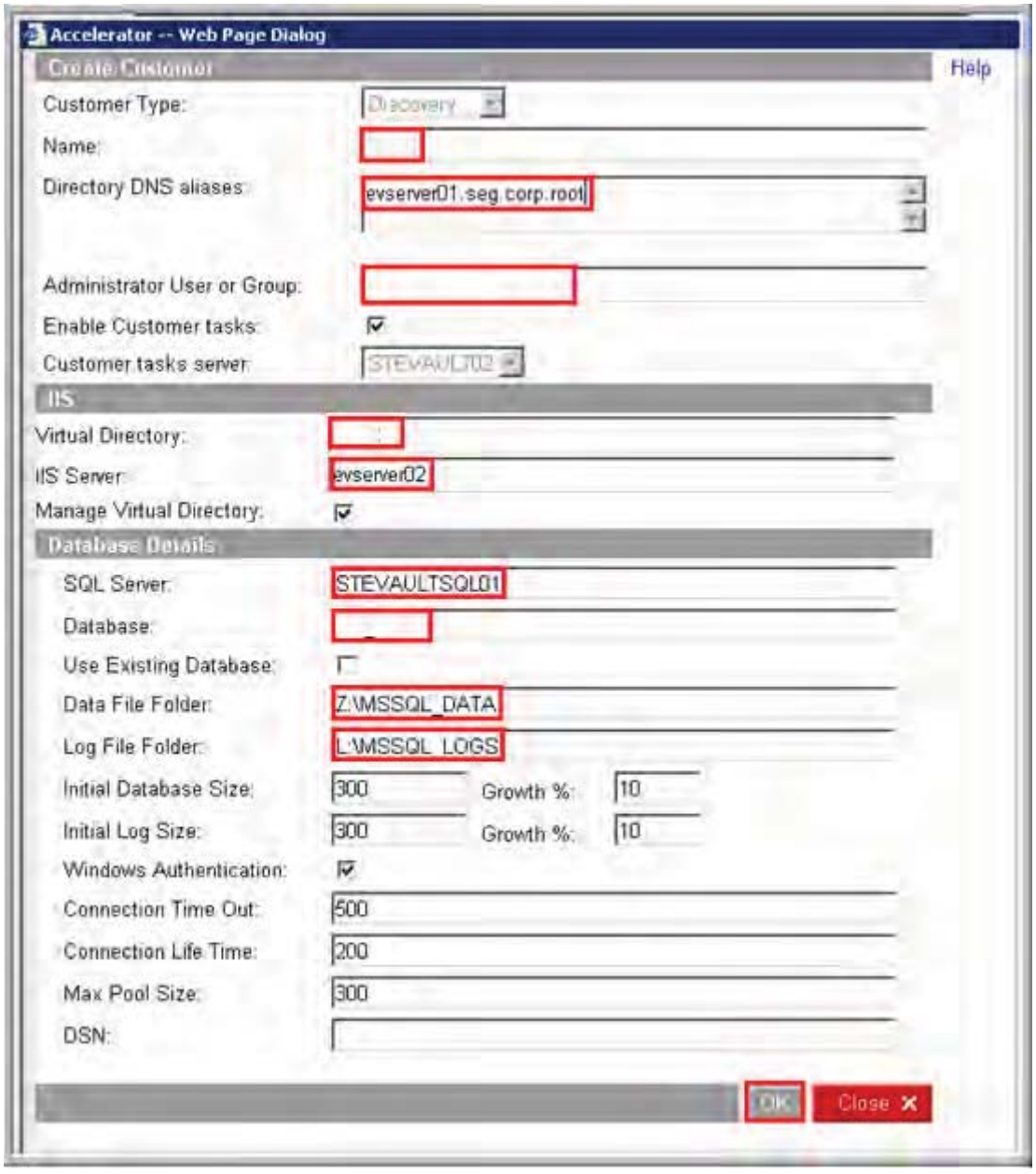
Manually restart Accelerator Manager Service and click on Next.



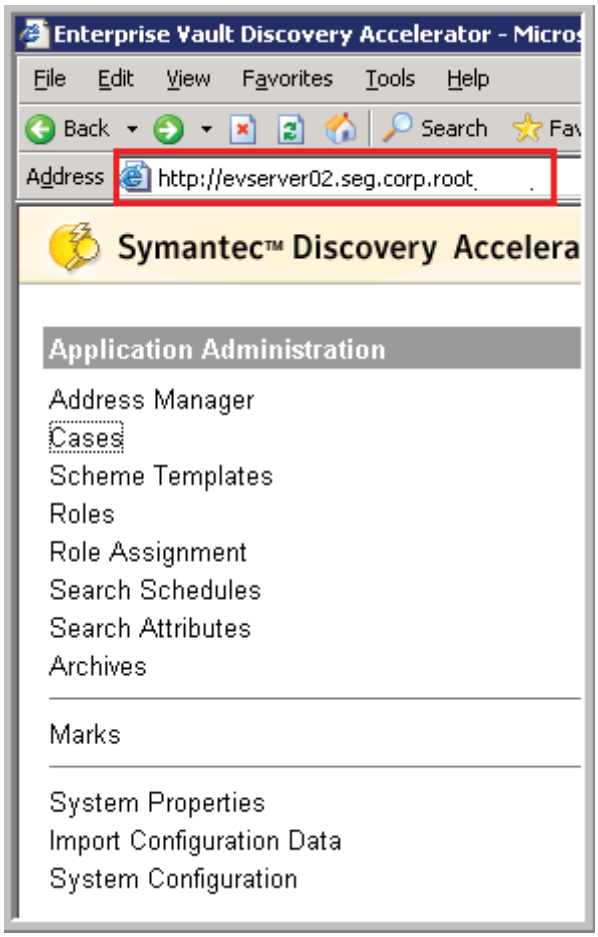
Go to the URL http://evserver02.seg.corp.root/evbaadmin. Then click on New Customer.



Enter the information below. Be sure to enter the company for the name and the name of the Virtual Directory and then repeat these two steps to create the parent company.



Test the sites configured and make sure they are in the IE Local Intranet Zones.



Click on Role Assignments and then Discovery System Admin and add VaultAdmin to this role.



Appendix H

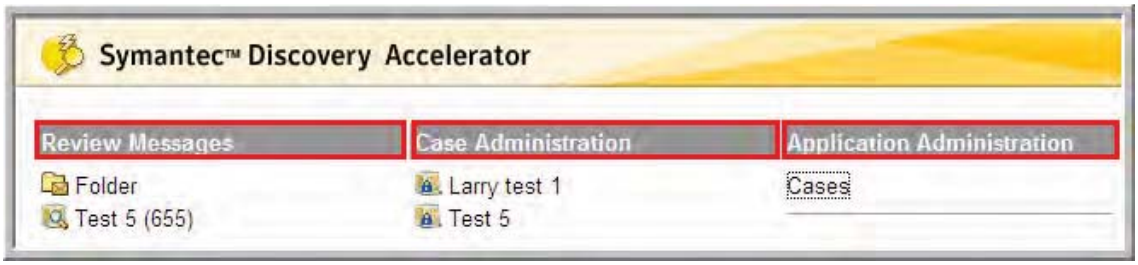
Discovery Accelerator End User Configuration and Training

For individuals in IT that need access to complete searches for legal add them to the Case Manager role by clicking on Role Assignments and adding the users domain account. Grant the user Full Control to the C:\Discovery Accelerator Export. This is the location where exported discoveries are downloaded to. These following steps would be completed by the individual in IT completing the search for legal.

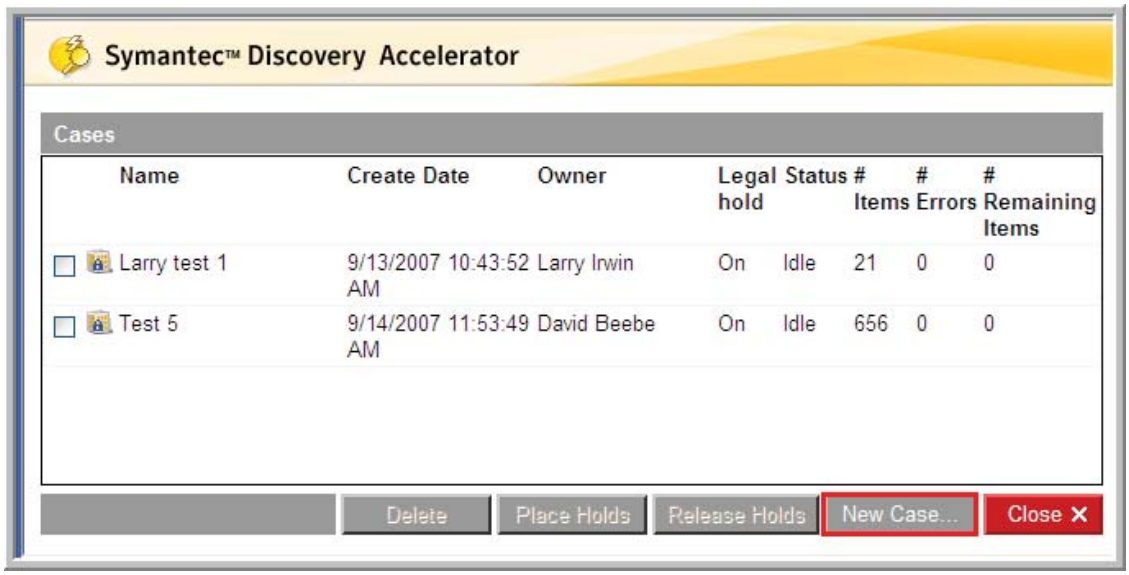
Logon to the site that you are performing the search for. The steps after this assume that the user logging on has only the Case Manager role.

- Company: http://evserver02.seg.corp.root/company/
- Parent Company: http://evserver02.seg.corp.root/parentcompany/

There are three areas that will show – Review Messages, used for reviewing messages returned in searches, Case Administration, used to view previous case searches setup and then Application Administration, used to view and create new Cases.



Click on Cases and then New Cases.

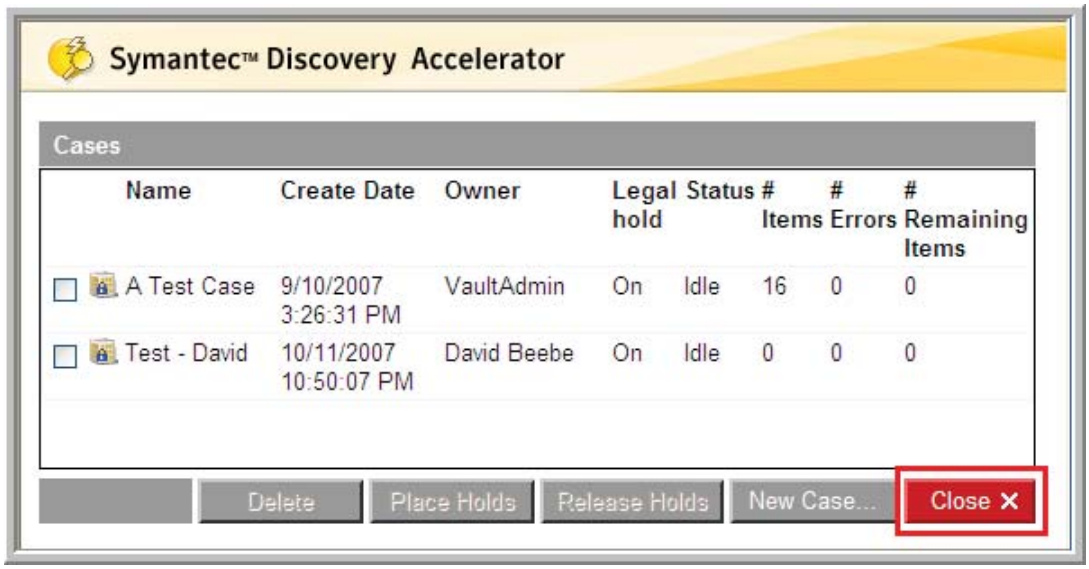


Type in a name for the case and select the required archives – see table below. Note that the output folder is "C:\Discovery Accelerator Export\ParentCompany" or "C:\Discovery Accelerator Export\Company". Fill in the Reason field for why the search is being done and then click OK.

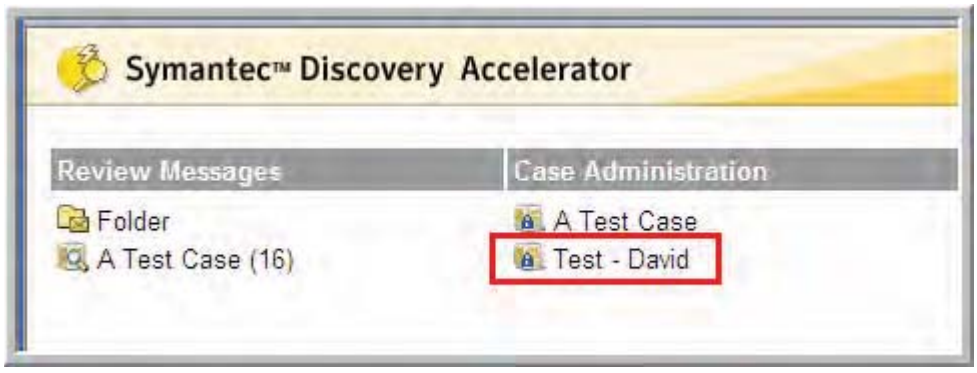
Enterprise Vault Archive Name	**Archive Journal Details**
PARexecutiveJournal	Journal Archive for Parent Executive Users
PARhrJournal	Journal Archive for Parent HR Users
PARlegalJournal	Journal Archive for Parent Legal Users
PARMailbox	Mailbox Archive for Parent Users
PARstandardJournal	Journal Archive for Parent Standard Users
SEGexecutiveJournal	Journal Archive for Company Executive Users
SEGhrJournal	Journal Archive for Company HR Users
SEGlegalJournal	Journal Archive for Company Legal Users

SEGMailbox	Mailbox Archive for Company Users
SEGstandardJournal	Journal Archive for Company Standard Users

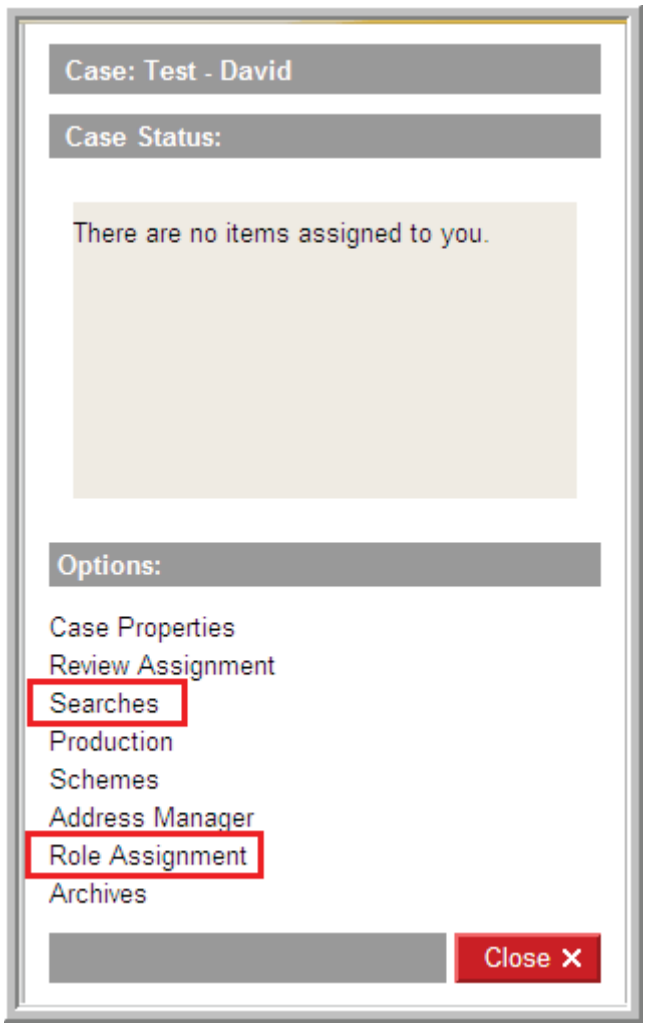
Click on close.



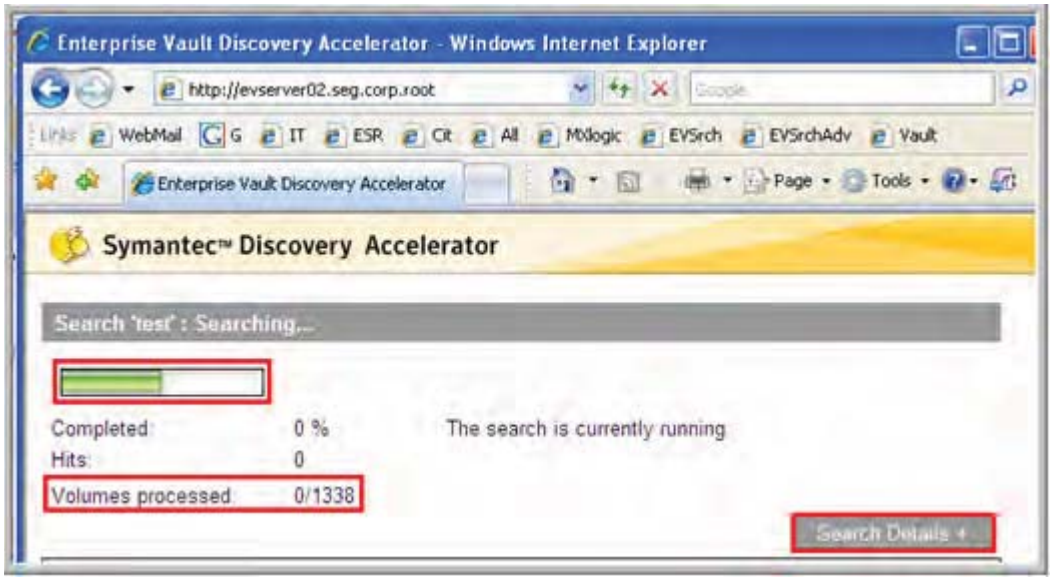
Then click on the newly created case in the main window.



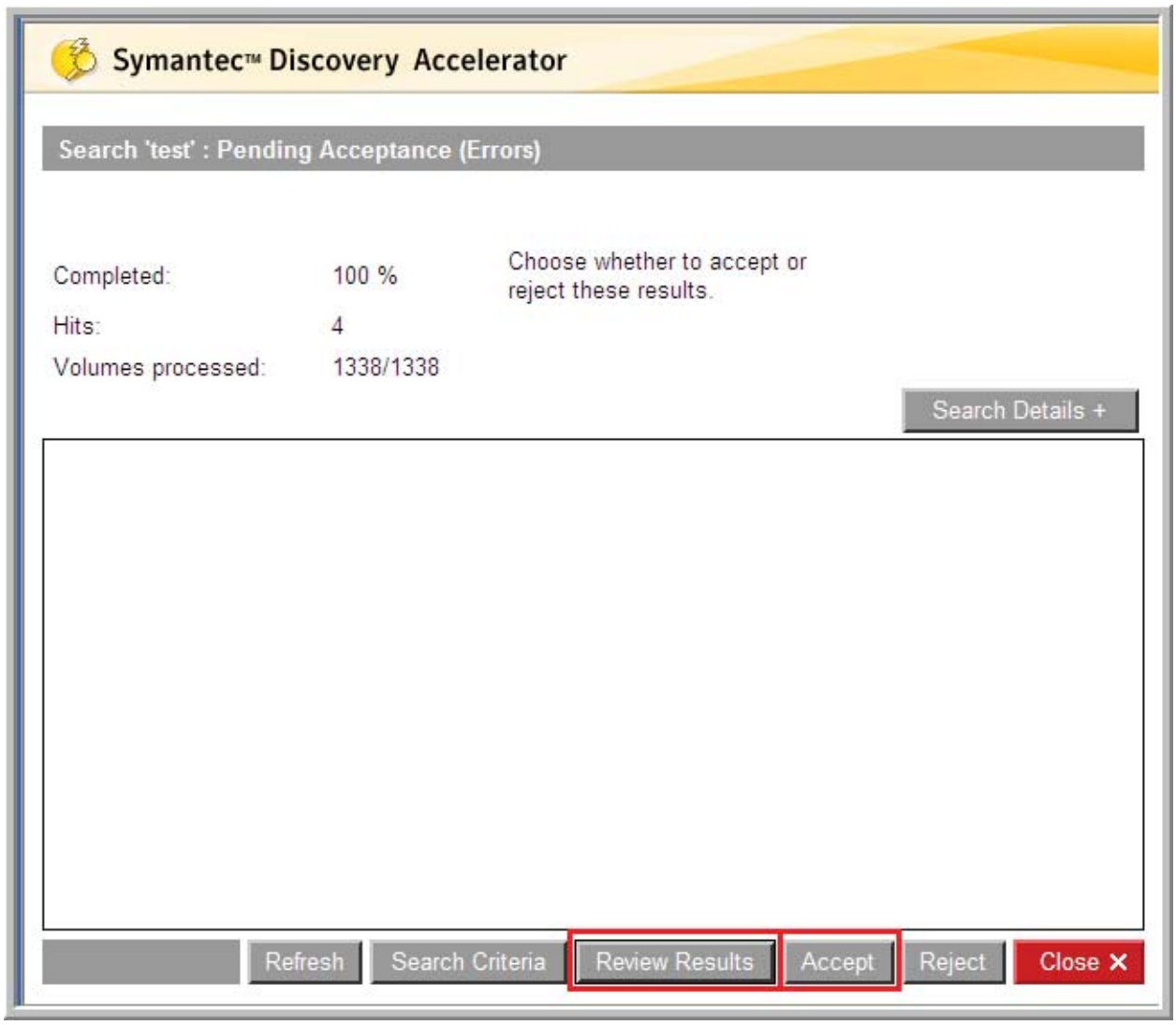
There are two main areas from this section that will be managed - Searches and Role Assignment. In Role Assignment you can assign reviewers to the case and in searches you can define what search you want to run. Click on the Searches link and then on the New Search link at the bottom right.



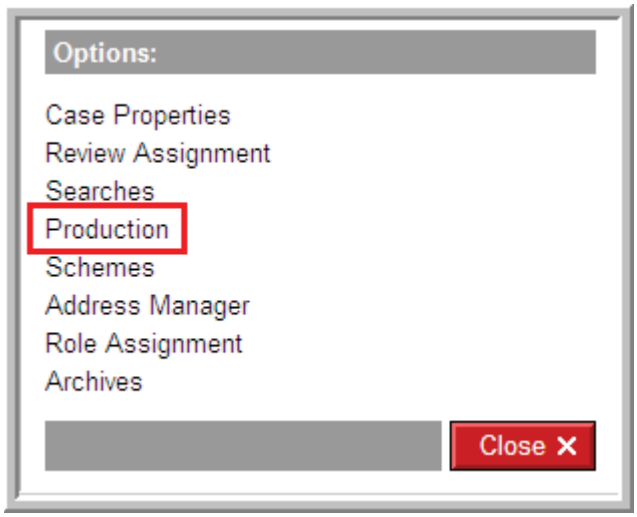
In the next page there are a variety of options to search for, be sure to use the pull down options to select the criteria that you want to search for. In this section the help button in the upper right can be very helpful in customizing the search to meet the legal search requirements. Click OK after criteria have been entered. The screen below will show the status of the search, you can keep hitting Search Details to refresh.



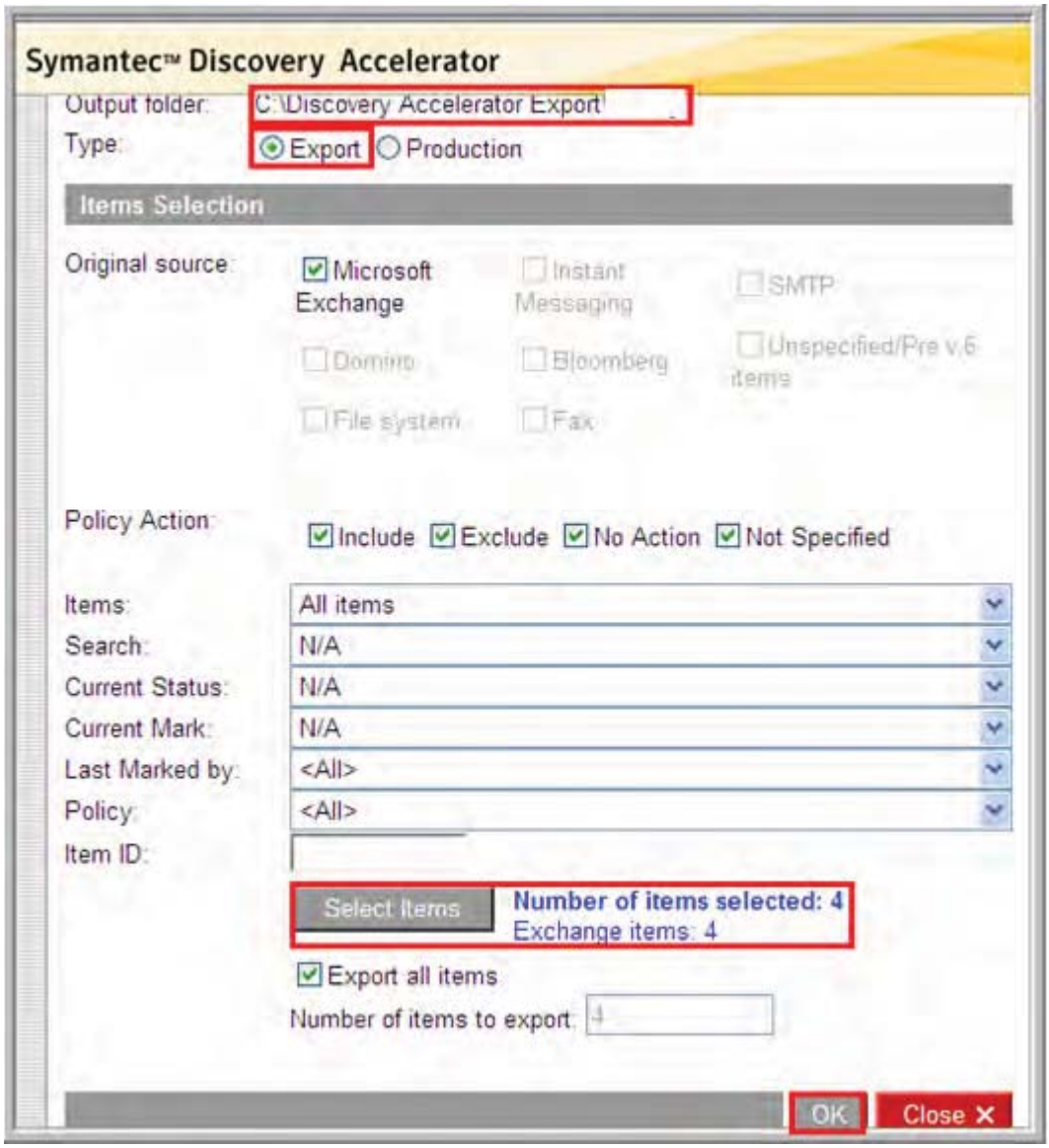
After the search has reached 100% you can accept the results. Another option is to Review the results in which case you can view and mark the results for review. Click on the Accept button. Then click on Close to go back to the main case screen.



Click on the production link and then the New Run button.

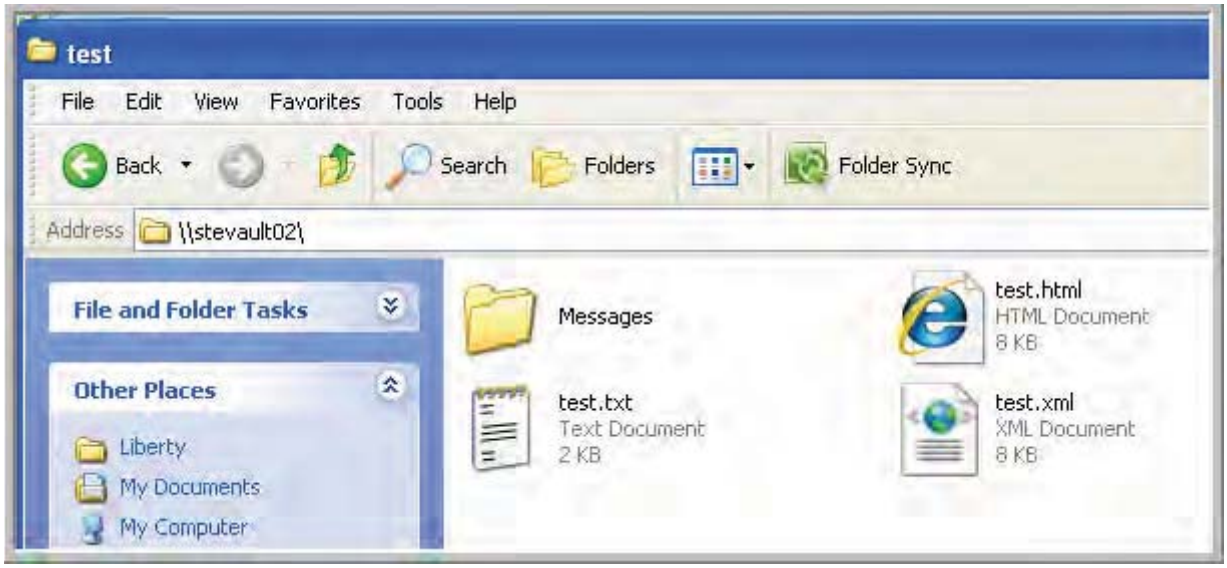


Put in a name for the run and then confirm that Export is selected. Then assuming you want all items selected click on the Select Items button and confirm the number next to it lists the items to be exported, then click on OK and then OK on the next screen. The processing screen will be displayed. Wait until it is finished and click on Close.


Symantec™ Discovery Accelerator
Output folder: C:\Discovery Accelerator Export
Type: Export Production
Items Selection
Original source: Microsoft Exchange Instant Messaging SMTP Domino Bloomberg Unspecified/Pre v.6 items File system Fax
Policy Action: Include Exclude No Action Not Specified
Items: All items
Search: N/A
Current Status: N/A
Current Mark: N/A
Last Marked by: <All>
Policy: <All>
Item ID:
Select items
Number of items selected: 4
Exchange items: 4
Export all items
Number of items to export: 4
OK
Close


Symantec™ Discovery Accelerator
Production: Test - David
Name
Created
Status
Items
test
10/11/2007 11:28:26 PM
Finished
4
New Run...
Close

Open up the share \\stevault02\test. Click on the site the search was run from and then find the folder with the name of the search that was run. The Messages folder contains the messages in the search and the test.html file at the root of the folder is a summary of the messages found, containing links to the emails in the messages folder. All of this data can be copied to a DVD/CD to be researched further.



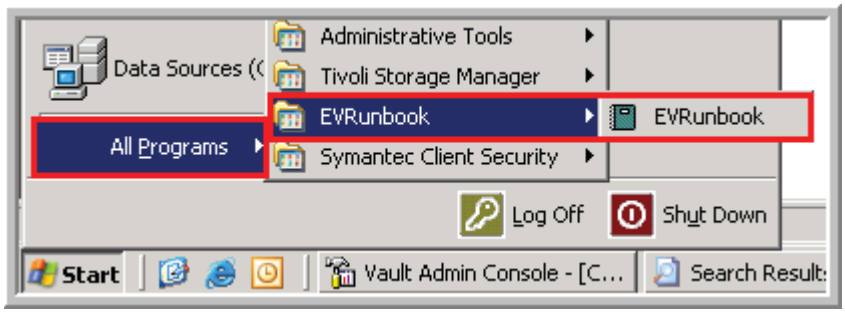
Appendix I

Day to Day Administration and Troubleshooting

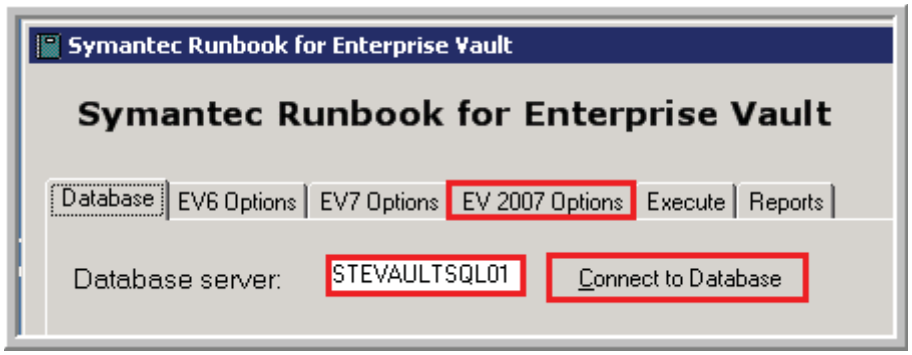
Site Settings Report Generation

EVRuntime is an application installed on STEVAULT01. This application automatically gathers all configuration information of the site and puts it in an HTML file. This report may be requested by Symantec when calling for support and is an excellent way to quickly see all the configuration settings within the environment. You can gather as much or as little information as you want by selecting the necessary options.

To generate a new report go to STEVAULT01 and log on as VaultAdmin – Program Files – EVRunbook – EVRunbook.



Enter the database, STEVAULTSQL01, and click on Connect. Then click on the EV 2007 tab and click on all the settings that you want, which will probably be all but File, Sharepoint and Domino settings, unless you are running the report for specific settings.



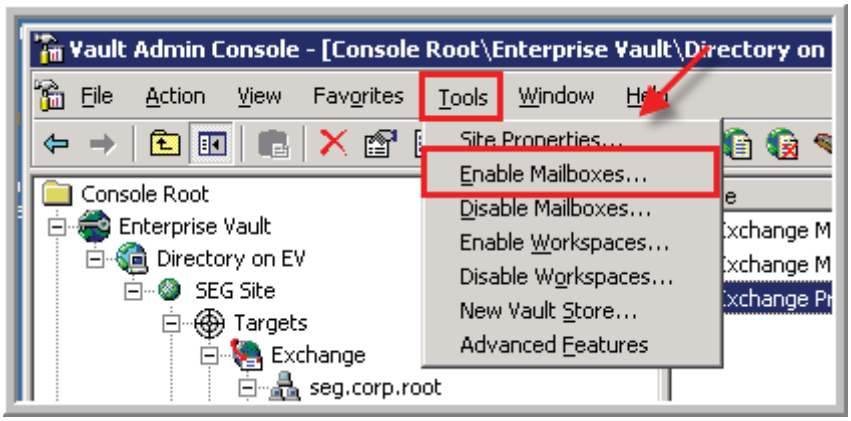
Review the results.html file generated in the Program Files\EVRuntime folder.

Common Enterprise Vault Tasks

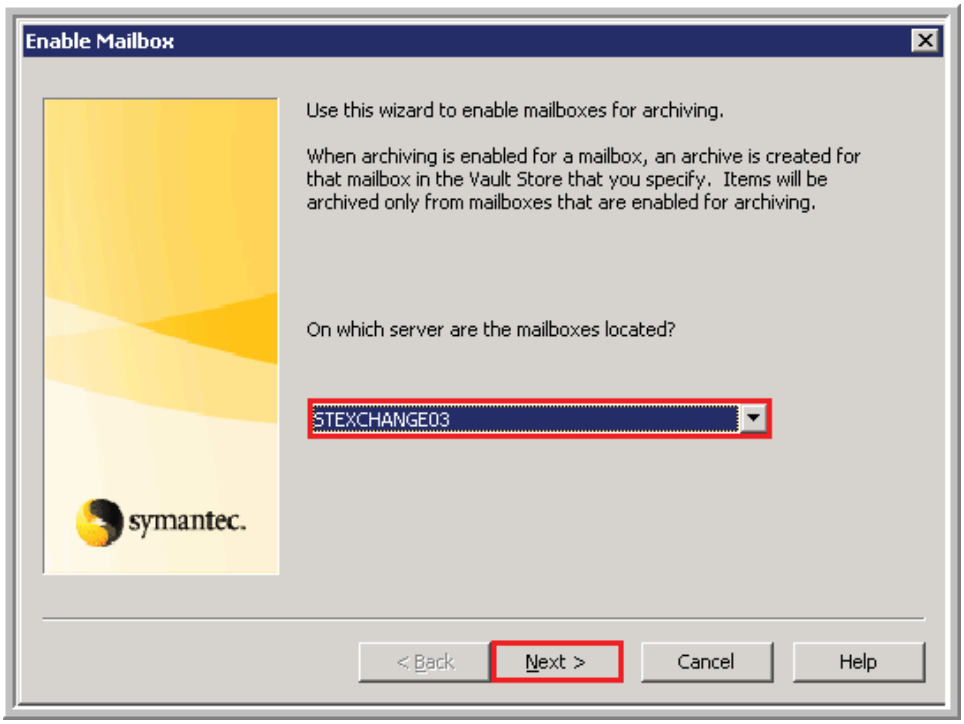
There are many tasks that are required for the overall administration of Enterprise Vault which are required for the health and functionality of the solution.

Enabling Mailboxes

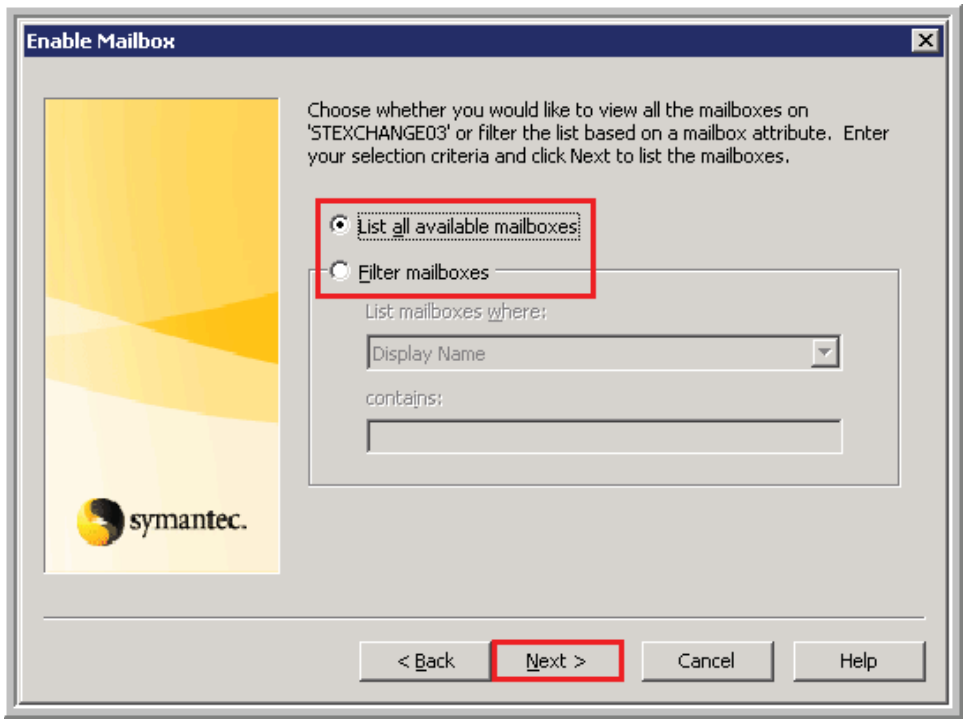
To enable a new mailbox you can either click on Tools – Enable Mailbox or click on the icon below the help menu option (see arrow below). Note that before you enable a new user you will want to confirm they have the Enterprise Vault client installed, otherwise they will not be able to retrieve email. After the production release the client should be installed on a new desktop.



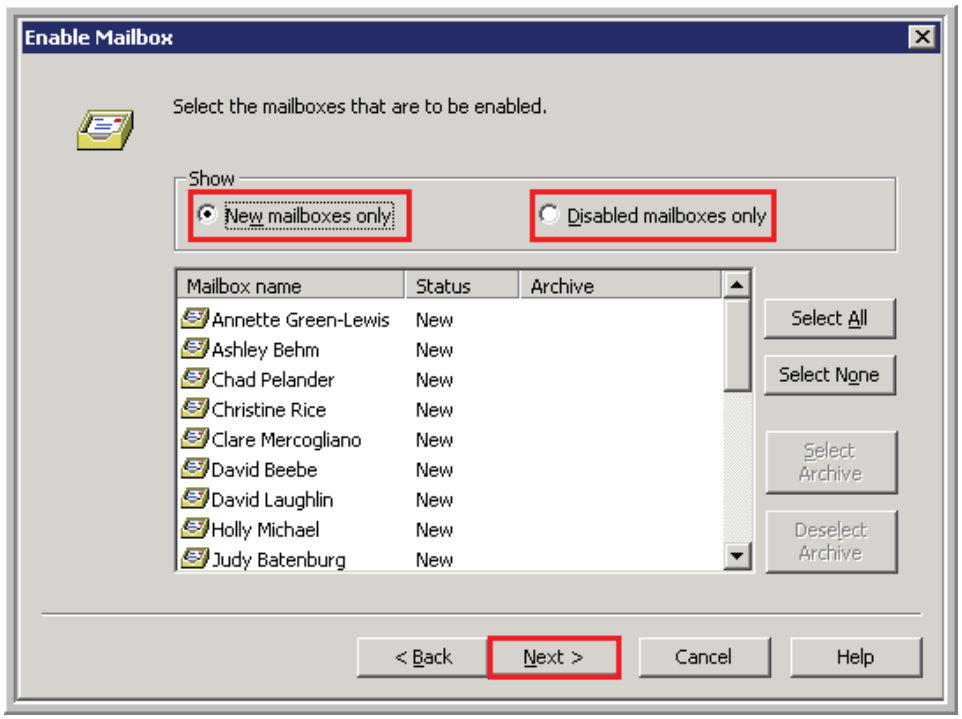
Then select the mail server that the mailbox resides on and click on Next. Note that the account will not show up unless it has been provisioned.



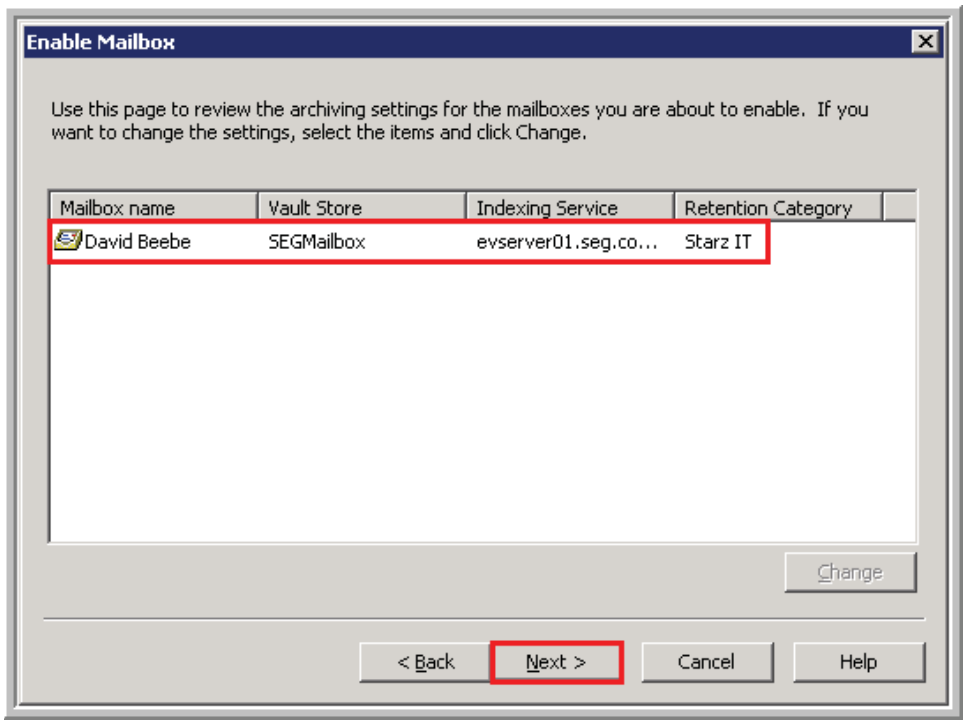
You can filter mailboxes or just select to list all available like pictured below and then click on Next.



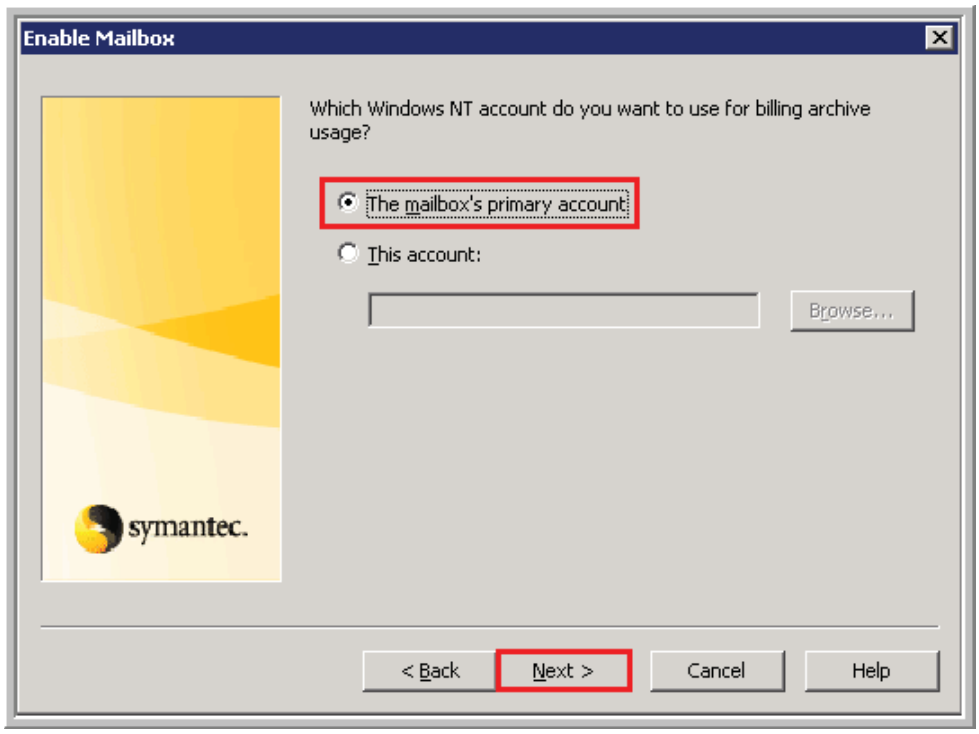
Click on the mailbox(es) that you want enabled and then click on Next. Note that if you previously disabled a mailbox you would need to select that radio button to see it to enable it. Once you enable a mailbox the newly enabled user will get a welcome email.



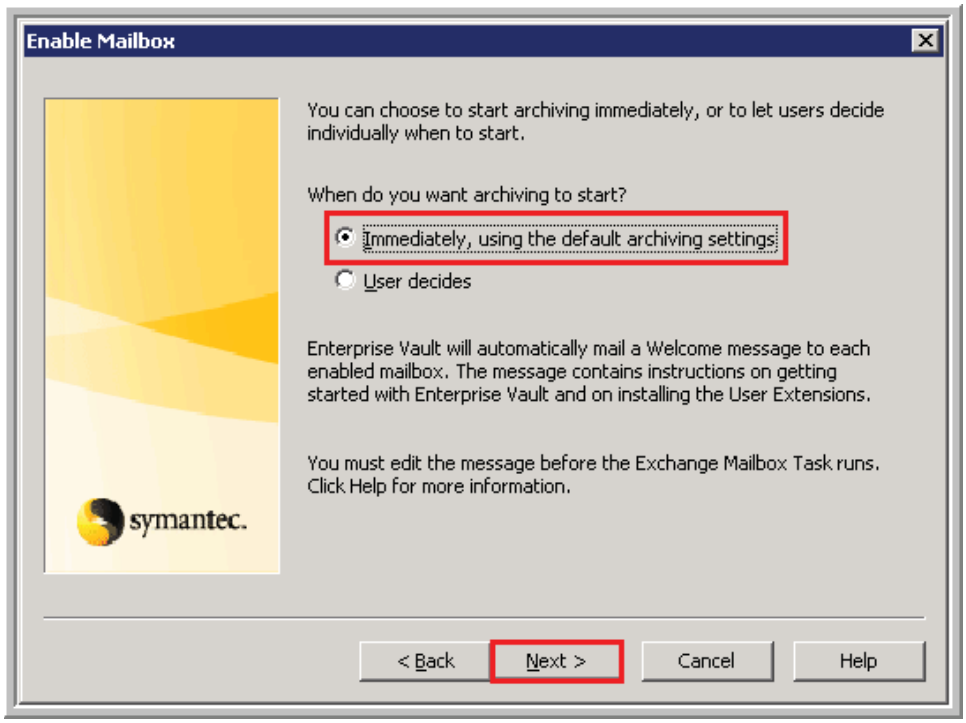
Confirm the mailbox and click on Next.



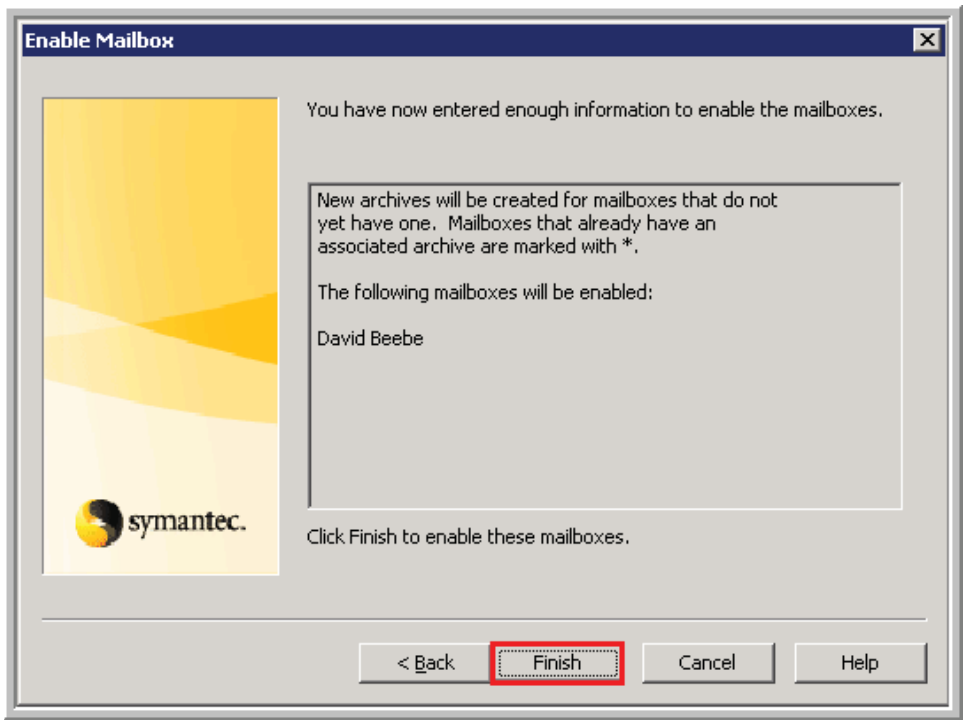
Select the radio button “The mailbox’s primary account” and then click on Next.



Select to enable immediately or user decides and then click on Next. Usually you would want to enable the mailbox immediately.



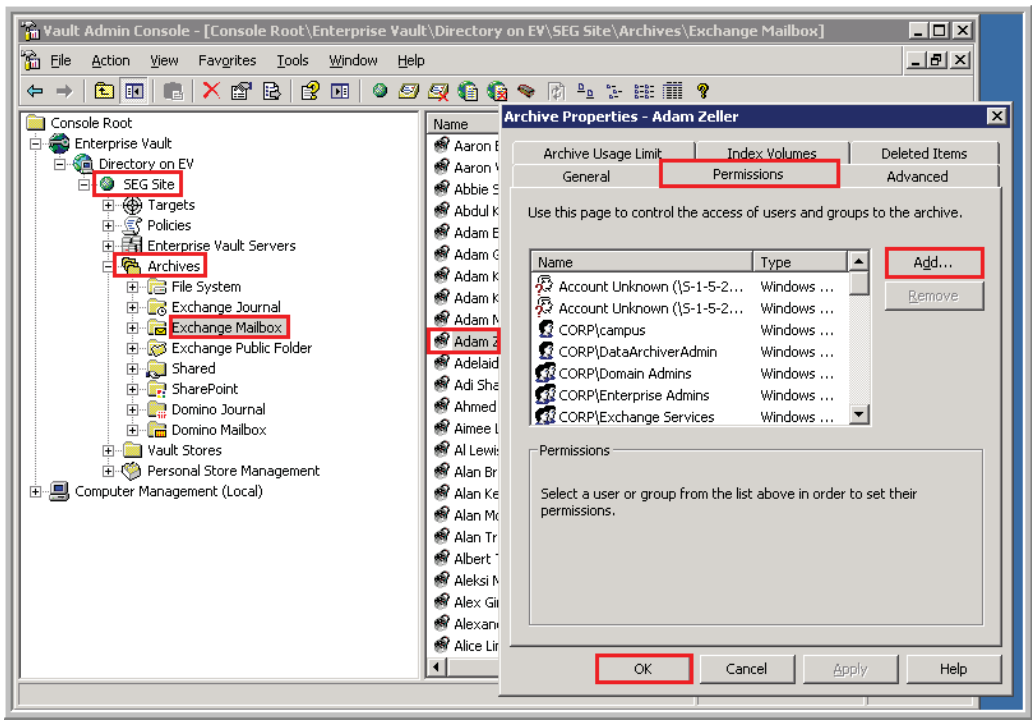
Confirm the final settings and click on Finish.



Granting Access to an Archive

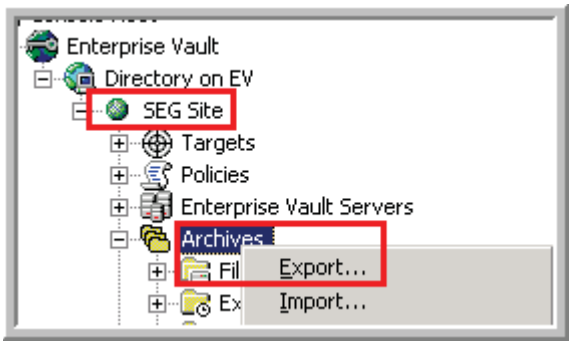
Occasionally another employee will need access to another users archive. Note that this does not give access to the whole mailbox unless the employee is no longer with the company, in which case the whole mailbox should have been archived.

Open up the Vault Admin Console and browse to SEG Site > Archives > Exchange Mailbox. Then in the right pane right-click on the mailbox you want to grant permissions to and click on Add and add the necessary user. Click on OK and have the user test access by going to Archive Explorer. Note that these permissions do not replicate back to Exchange, so until you remove access from the archive the user will retain access.

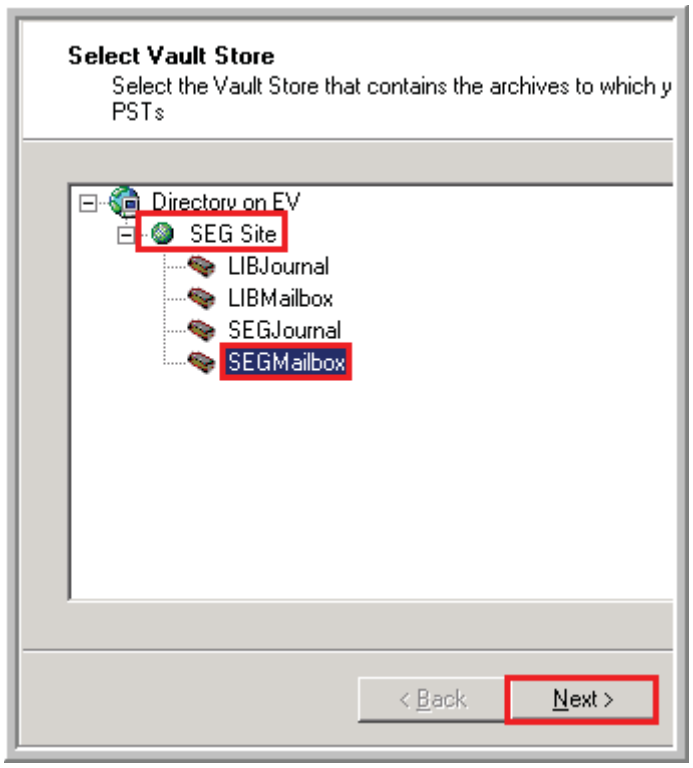


Restoring an Archive to a mailbox

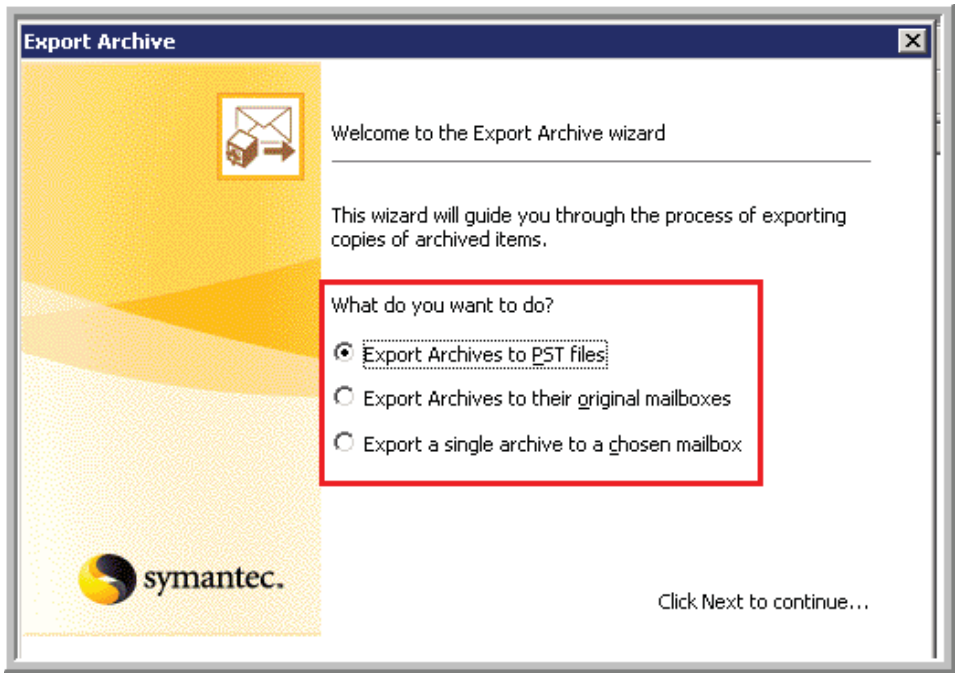
Browse to the Site > Archives and right-click on Archives and select Export.



Click on the Vault Store that the mailbox is that you want to import. The company users are in SEGMailbox and the parent company are in PARMailbox.



Select the option you want, in this case to export an archive back to the original mailbox.

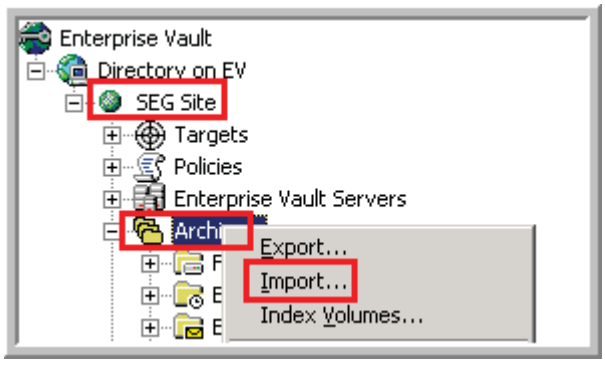


Then just follow the wizard to archive all the items back to the original mailbox, or selected mail back to the mailbox. Then just confirm that it processed.

Importing a PST to an Archive

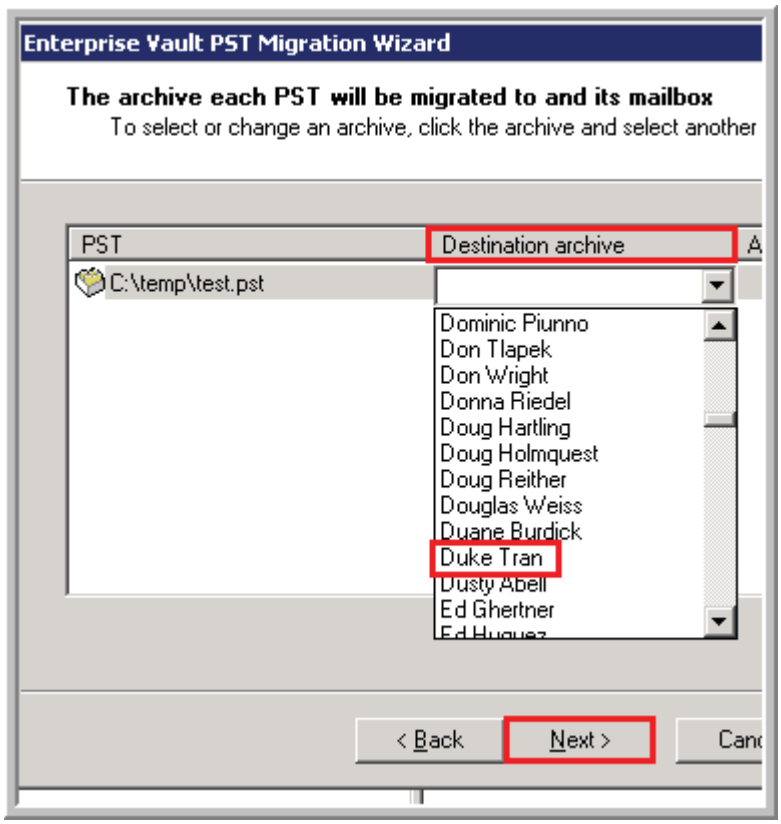
Copy the PST to a location accessible from where you are running the Vault Admin Console, i.e. you can put it on STEVAULT01 in the Temp directory. The PST cannot be open when copying. In the support center documentation it is requested that they instruct the user how to remove the PST from their mailbox and then give us the location of the PST. Then we can import this to their mailbox while they are accessing it. This should not have much of an impact to their quota, but you should still check. Roughly 20 MB will be added for a 2 Gig PST.

Open up the Vault Admin console and browse to the Site > Archives and right-click on Archives and select Import. Pick the vault store that the mailbox resides in that you will be importing the PST to and then click on Next - SEGMailbox for the company mailboxes and PARMailbox for parent mailboxes.

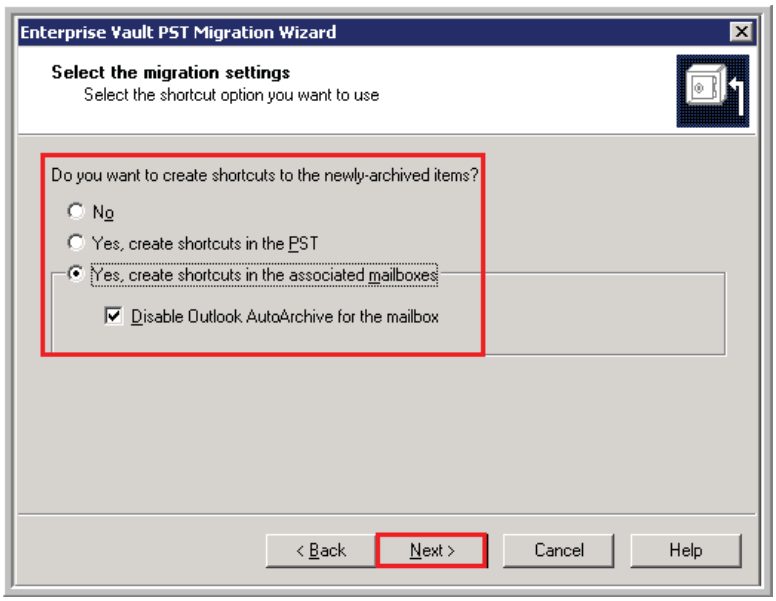


Browse to the PST and click on Next. Then keep the radio button chosen to browse to an archive to restore the PST to and then select a retention category. This is not a concern until retention categories are defined.

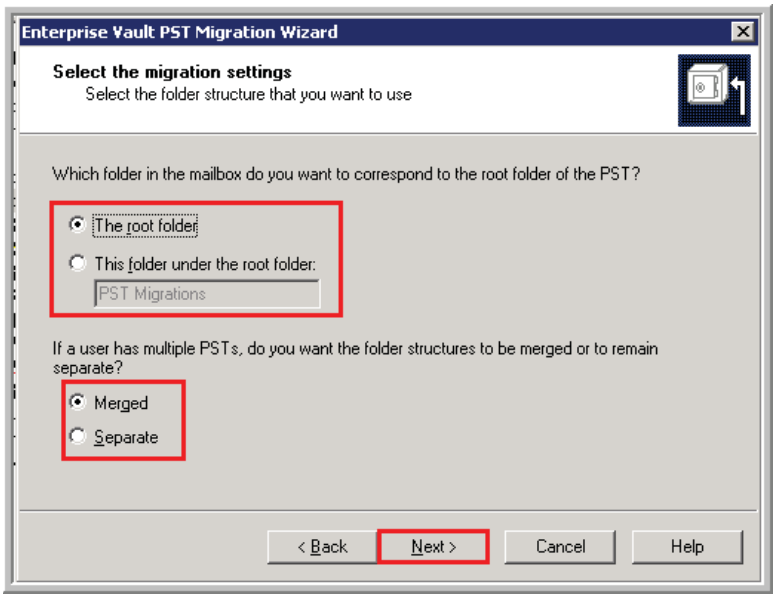
Pull from the drop down the user that you want the PST imported to.

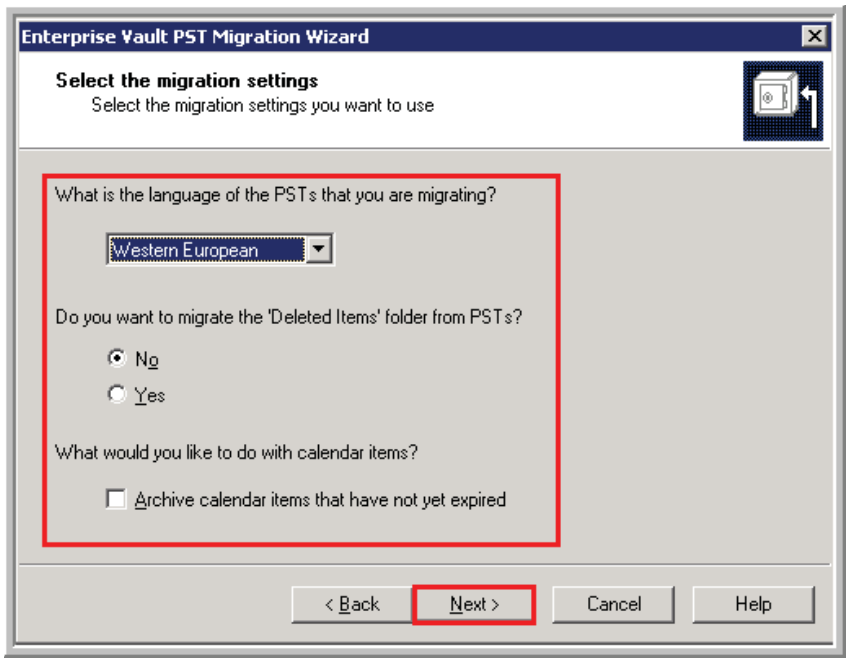


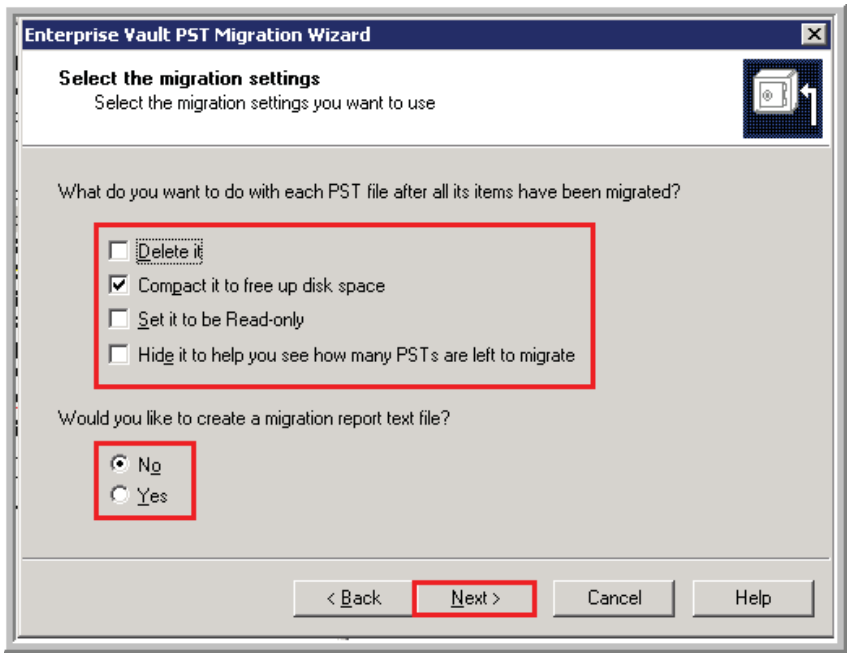
Chose the option to create or not create shortcuts. You would almost always want shortcuts, otherwise the newly imported data would not be visible from the users inbox. You can also choose to disable Outlook Auto-Archive. Ideally this is a setting you would want to disable, but be sure that the end user no longer wants to use this feature.



Then review the settings on the following three screenshots to determine how you want the data imported. You should not delete the PST until you are sure the data is in the users mailbox.





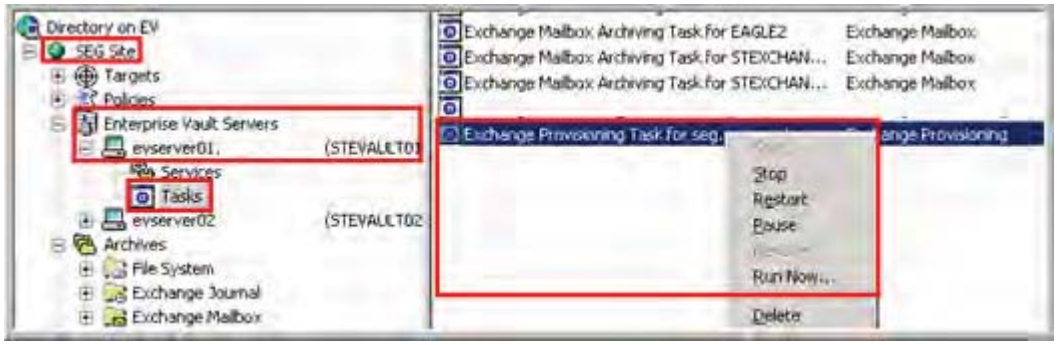


Confirm the settings you chose and click on Next to complete the import. Then make sure the customer sees the data.

Moving Mailboxes – Manually Updating for Archive Access – Running Provisioning and Synchronization

When moving a mailbox to another store if a user wants immediate access to their archive provisioning and synchronization will need to be run manually, otherwise they will run within 24 hours and then the user will need to close and re-open outlook to get the new hidden message which includes all the settings.

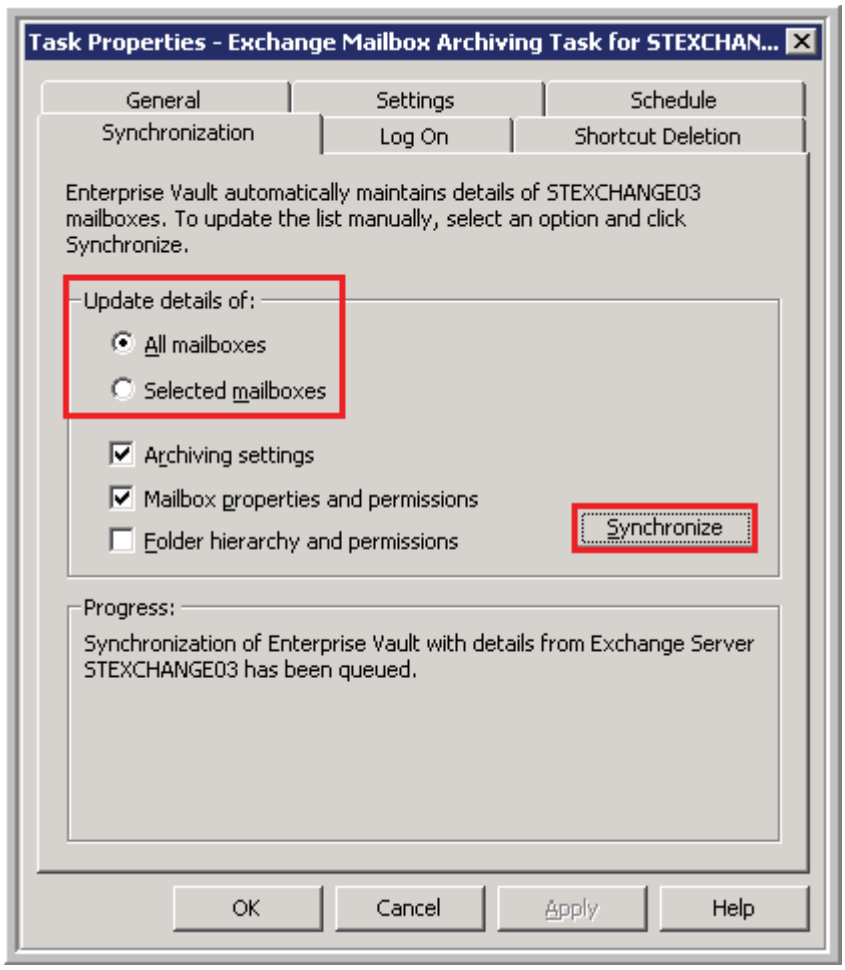
Open up the Vault Admin Console and browse to SEG Site > evserver01 > tasks and on the right side right click on the Exchange Provisioning Task for SEG and select Run Now.



Browse to SEG Site > evserver01 > Tasks and double click on the relevant archiving task for the mail server the user resides on.



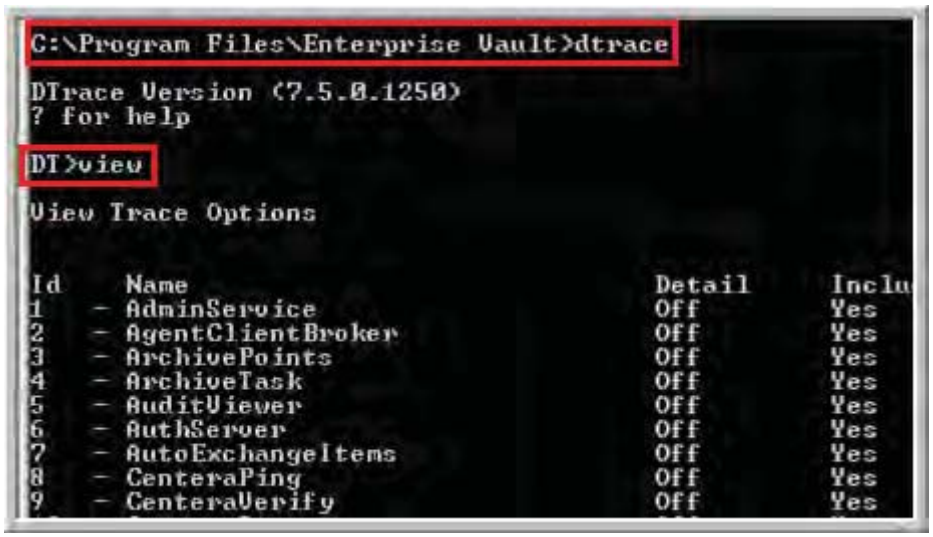
Select the synchronization tab and then either click on Synchronize for either the whole server or more specifically just select the specific mailbox.



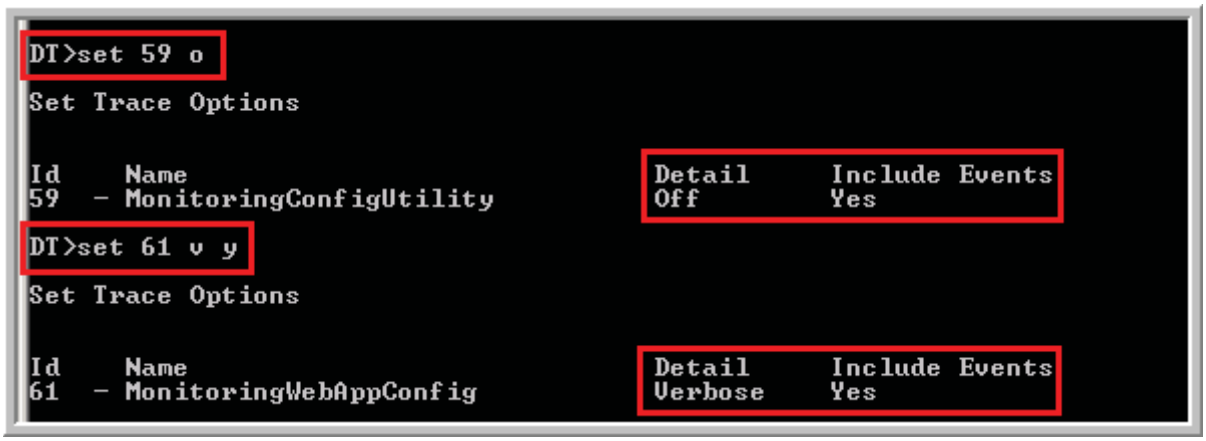
Then close and re-open Outlook and confirm they can archive and restore.

Troubleshooting Server and License Issues

One common method of troubleshooting server issues is to run dtrace at a command prompt. Go to the Enterprise Vault installation directory (Program Files\Enterprise Vault) and type in dtrace and hit enter. Then type view to see all of the trace options.



Set the options that you want, i.e. “set 59 v y” turns events and verbose monitoring of the variable 59 on. Once you close this window monitoring should turn off, but best practice would be to run “set 59 o” which would turn it off. You can see these logs that it creates in the application directory



Type mon to monitor the trace output.



Performance Issues on Application Servers – For the initial installation we are not separating the Operating System and Application on separate drives, to increase performance this should be done and the MSMQ queues should be moved to the application drive as well as the page file.

For new licenses or if you are having issues with the existing licenses place the licenses in the Program Files\Enterprise Vault directory and restart services. You can confirm this worked by checking to ensure they were copied into C:\Program Files\Enterprise Vault\Installed Licenses and in the C:\Program Files\Common Files\Symantec Shared\Licenses. To re-apply the EV 2007 licenses get them from \\Hpnas01\install\Enterprise Vault 2007\EV2007Licenses.

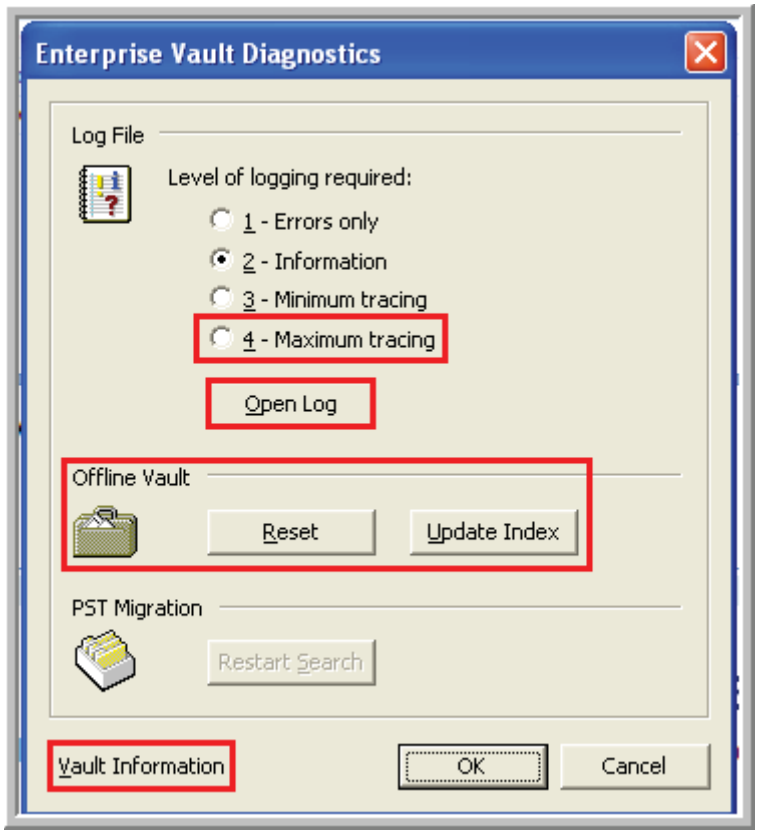
Troubleshooting Client Issues

Synchronization – run this from properties of the task of the exchange server if you are changing archive, desktop, OWA, outlook settings. Then close and re-open outlook and the hidden message should update so you can test any client side issues.

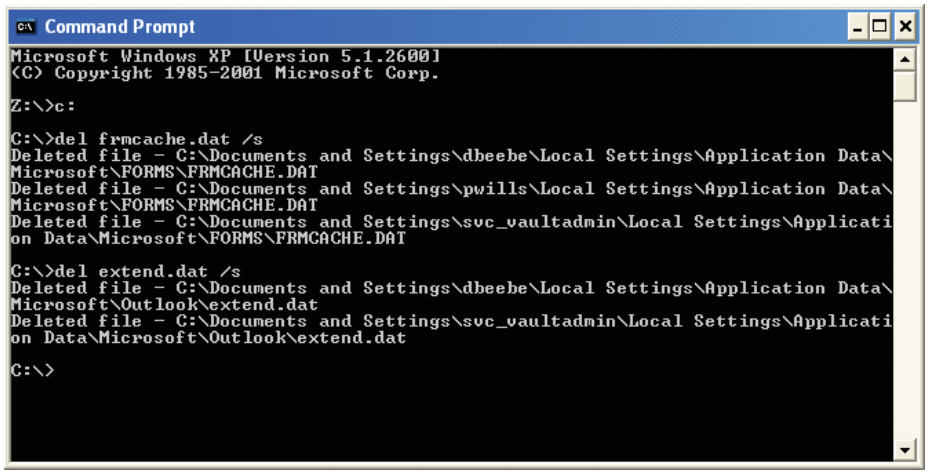
There are reports generated in the C:\Program Files\Enterprise Vault\Reports that are automatically run and you might want to review, in particular the provisioning reports

to see what users have been provisioned. This might be necessary when troubleshooting client side issues.

When working on client side issues you can click on CTRL and SHIFT at the same time and then click on any of the EV icons, i.e. Search Vault. It will bring up the menu below in which you can set the log to Maximum and then restart the Outlook client for it to take effect. You can update the index for the Offline Vault if there are issues searching it and here is where you would also view the log created when increasing logging. Last you can click Vault Information and get all kinds of details about the settings the client is getting to verify consistency with what you believe you should be seeing.



If the forms are not working for Outlook Web Access then you can close Outlook and clear the forms cache. Just open up a command prompt and enter “frmcache.dat /s” and then “del extend.dat /s” and then re-open outlook and it should download the forms locally again given that is the current setting.



If there are problems disabling and re-enabling a mailbox or the icons are not showing up correctly in Outlook you may need to “zap” the mailbox from Enterprise Vault.

Create the .ini file saved in Unicode and move it to STEVAULT01 to run a script against. The file should contain the following information. To find the DN for the mailbox go the registry key under the user profile on the computer – Current User – Software – Microsoft – Windows NT – CurrentVersion – Windows Messaging Subsystem – Profiles - Outlook. Under this key, select the key that begins with “13db”. This contains the properties of the primary mailbox. The mailbox distinguished name is stored in the registry value 001e6603. The server distinguished name is stored in the registry value 001e6612. These values are in the formats

(/o=MyOrg/ou=MySite/cn=Container/cn=Name, etc.) noted in the Additional Mailbox dialog box in ProfileMaker or PolicyMaker.

```
[Directory]

DirectoryComputerName = EVSERVER01

Sitename = SEG Site



[Mailbox]

DistinguishedName = /O=MS

Exchange/OU=CompanyOU/cn=Recipients/cn=name

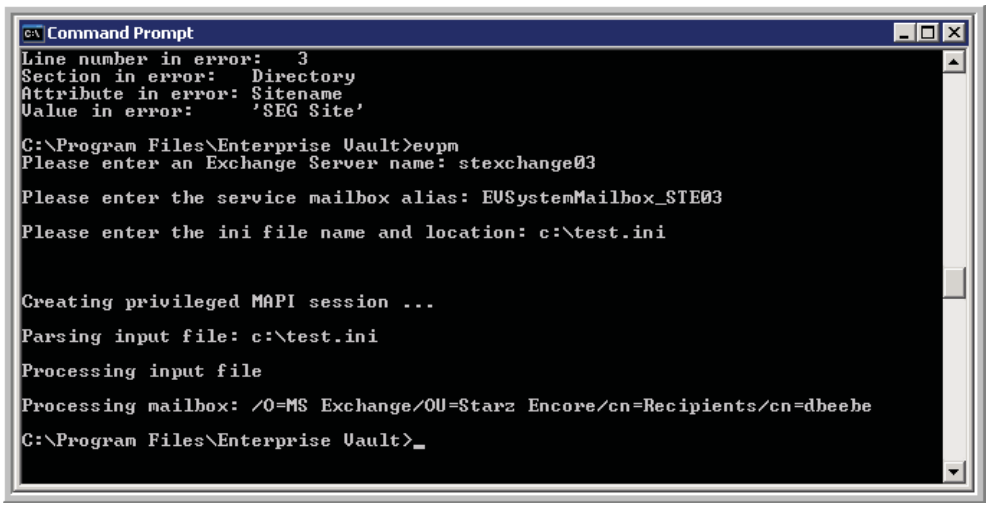


[Folder]

Name = Mailboxroot

Zap = True
```

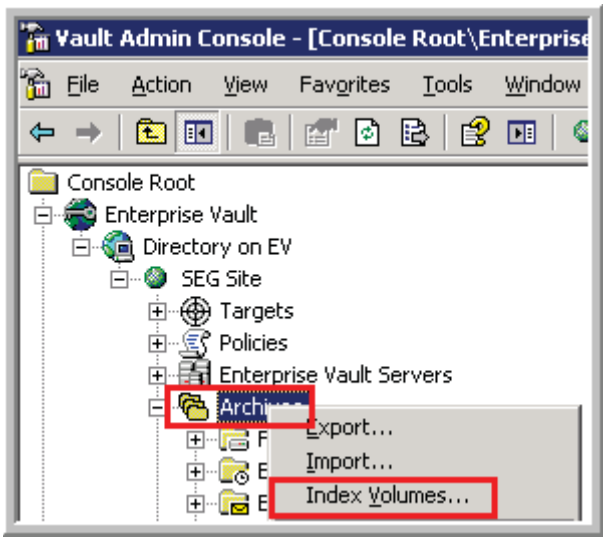
Open a command prompt on the STEVAULT01 and browse to Program Files\Enterprise Vault. Run “evpm” and enter the Exchange Server, System Mailbox and file created above. See below.



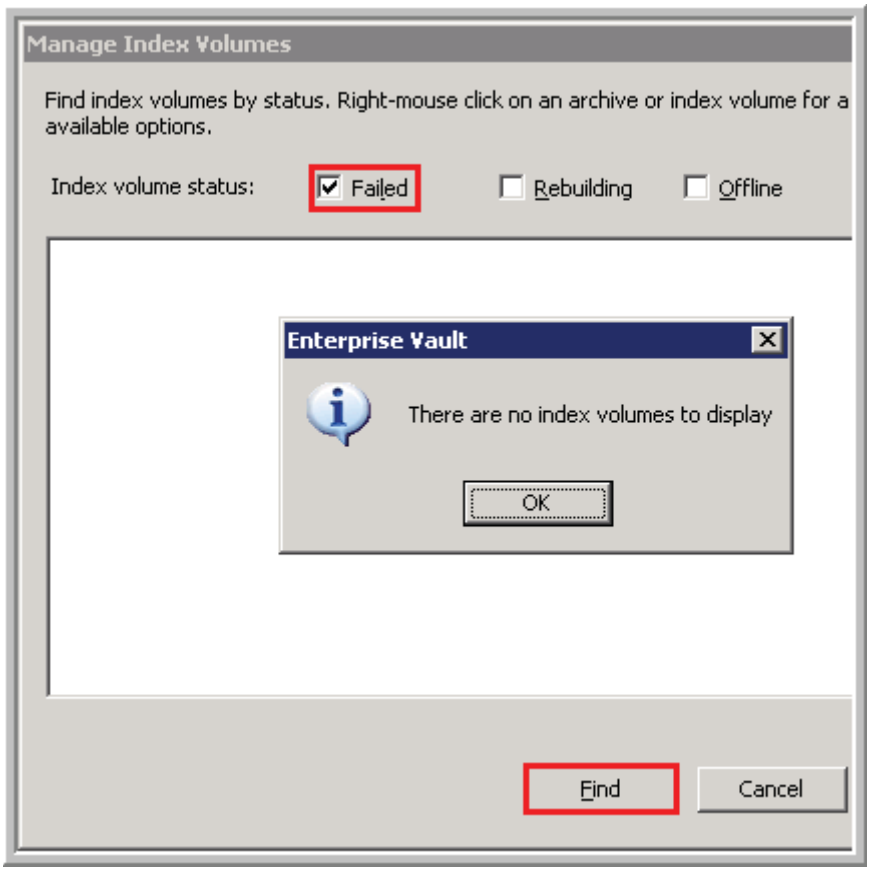
Rebuilding Indexes

If a user is getting errors when searching their archive there is a possibility that the index is corrupt and will need rebuilt. This would be a last option and needs to be taken seriously, in particular this could cause significant issues if any cases are open that have mail from this mailbox in its search results.

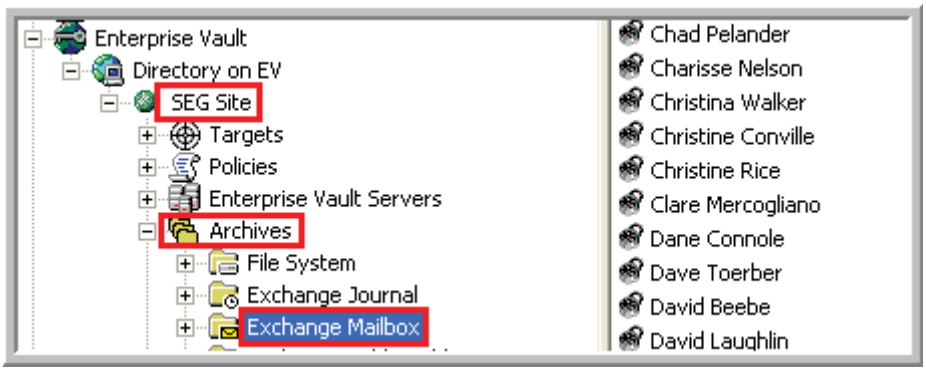
First check for failed indexes by going to SEG Site and right clicking on Archives and selecting Index Volumes.



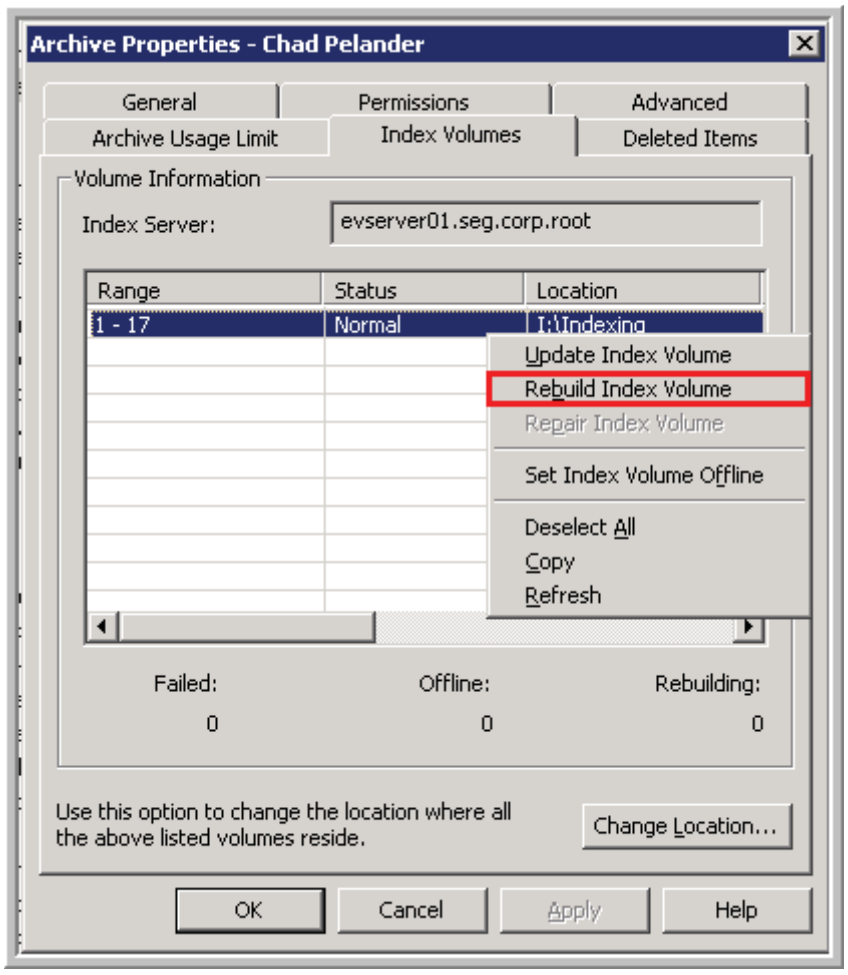
Check Failed and then Find and it should show if the index is failed or not. If so proceed to next step.



To do this browse to the SEG Site – Archives – Exchange Mailbox.



Right-click on the mailbox and click on Properties than click on the Index Volumes tab and right-click on the Index and select Rebuild Index Volume.



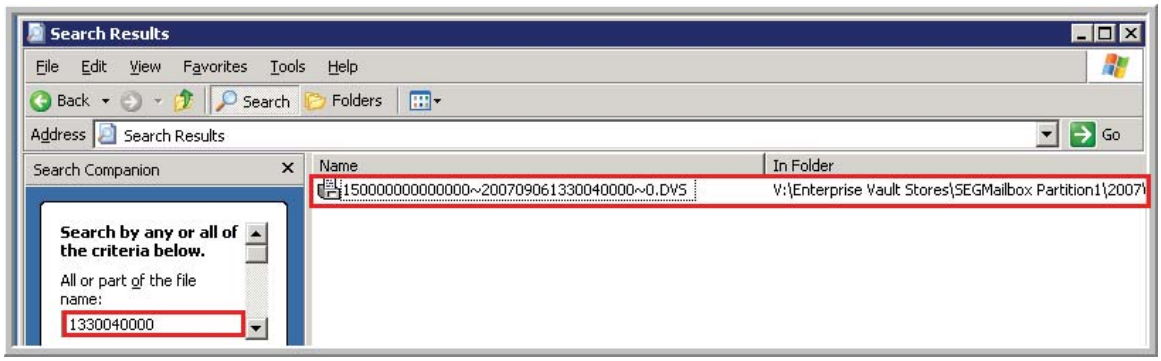
Advanced Search Troubleshooting

You can use Archive Explorer to search for a file and when it is found when you open it up you can look in the browser address and get the vault and saveset ID to find the related .dvs file in the vault partition. For example I pulled up the following document with the URL below. The SaveSetID is shown in the URL. Starting with the 2007 (or whatever year the email is from) until the ~ you can search for on the vault and find the DVS file and then just open with Outlook.

http://evserver01.seg.corp.root/EnterpriseVault/ViewMessage.asp?VaultID=1DD89A7C0421BCF4B9C86F10B9C34E4A31110000EV&SaveSetID=150000000000000~20070906

1330040000~0~50E93064A44E48D6BC9B7CD4F631651&SettingsBtn=0&ArchiveExplorerBtn=0

Find the DVS file on STEVAULT01 and double click on it to open with Outlook.



Help Desk Troubleshooting Steps – FAQ

Refer to this table for questions listed below regarding Enterprise Vault employee configuration

Distribution List	**Offline Vault?**	**Distribution List**	**Offline Vault?**
DL - PAR - EVault – Executive	Yes	DL - PAR - EVault – Legal	Yes
DL - PAR - EVault – HR	Yes	DL - PAR - EVault – Parent	Yes
DL-SEG-EVault-Executive	Yes	DL-SEG-EVault-Legal	Yes
DL-SEG-EVault-HR	Yes	DL-SEG-EVault-Company	No
DL-SEG-EVault-Company-Lap	Yes	DL-SEG-EVault-IT	No
DL-SEG-EVault-IT-Lap	Yes	DL-SEG-EVault-ITIS	Yes

DL-SEG-EVault-ZeroDay	No	DL-SEG-EVault-Generic	No
DL-SEG-EVault-UK	Users in this group are exempt from archiving		

Question: Why can't I see the icons for Enterprise Vault in Outlook? When launching Outlook why do I get an error loading the "valkyrie.dll"?

Answer: **Restart Outlook** – The client installation is deployed by SMS and is silent and no reboot is required, so if the user never restarted Outlook they will not be able to see the icons. **Run Fixmapi.exe for the Valkyrie and/or missing icon issue** – Close Outlook and go to Start –> Run and enter "fixmapi.exe" – you will not get a confirmation saying this was successfully run. Open Outlook and see if that fixed the issue. This seems to be the most common resolution for the icons missing or the DLL error. **Confirm Client Installation** – Go to Add/Remove programs and verify that "Symantec Enterprise Vault for Outlook Add-In" is listed, if not have user install it manually by double clicking on company_setup.exe located in \\sms2003\Packages\Evault Client. Note this is a silent install so the user will not get an installation completed confirmation. **Check Group Membership** – The user must be a member of one of the distribution lists that is provisioned for Enterprise Vault (see table above), if not add the user to appropriate group and send the ticket to ITIS for the employee's mailbox to be enabled. **Macintosh Users** – There is not a client for Macintosh users so they will have to use OWA to see the icons or click on the links in the shortcut emails to read an archived email. **Conflict with Exchange System Manager, Outlook 2007 and the EV Client** – See if they have Exchange System Manager (ESM), Outlook 2007 and the Enterprise Vault Outlook Add-In on the same computer. If so the user might get an error loading

the “valkyrie.dll”. Close Outlook and go to Start –> Run and enter “fixmapi.exe” – you will not get a confirmation saying this was successfully run. Launch Outlook and if you still get an error then the user will need to uninstall and reinstall the ESM client and run fixmapi again.

Question: Why do I see mailboxes other than mine when I go to search my archive?

Answer: **Check Permissions in AD** – Employees will see all mailboxes when searching their archive if they are granted access to the mailbox in Active Directory. Confirm with the employee whether they believe they should have this access or not, if they should not confirm on the account they have access to that they are added in the mailbox rights and then remove their access. If they have access from a group membership further research will need to be done by ITIS. **Delegate Access** – This type of permission should not grant access through archive explorer or vault search.

Question: Why does an email have an archived icon next to it but when I try to restore it from the vault I get the error “Unable to restore because you have not selected any archived items?

Answer: **Backup Needs to Run** – If any email was archived, either manually or during the nightly process, a backup must be completed to turn that email into a “shortcut”. Check and see if that email is a shortcut, i.e. only the first 500 characters are displayed in the body of the email, or if the entire email is intact. If the whole email is there than it most likely means that the backup has not run since the email was archived. If this email was archived two days earlier than send to IT IS for further research, but if it was archived in the last day wait one more day to see if the issue is resolved with the completion of the next nightly backup.

Question: Why doesn't my search result return emails when I search for xyz or why do I get a failure message when trying to search my archive?

Answer: **Reproduce in their Archive** – Since CSS has access to all archives step through the same search steps they are doing to see if you get the same results. Try searching using different methods, i.e. the Vault Search and then Archive Explorer. From the Vault Search you can launch "Browser Search" in the upper left of that pane or "Advanced Find" in the upper right for further search options. From the "Advanced Find" search if you don't enter any search criteria it will return all items in the archive, which might help to determine if the search results are accurate. **Rebuild Index** – If you can see an email in their archive but can't search on the details the index might need rebuilt, in which case ITIS will need to initiate a rebuild of the index.

Question: When I try to archive an email I get the error "You cannot archive items from this location" or "You cannot restore items to this location".

Answer: **PST's** – PST's will most likely cause confusion to many users as any email stored in a PST cannot be archived or restored while in a PST. It seems that there are certain users that immediately move all their email to a PST, in which case a user might not be aware they are even using a PST instead of their mailbox on the mail server. The first error above indicates they tried to archive an email while stored in their PST and the second error message indicates that a user tried to restore a message to their PST, this may occur if a user moved a shortcut from their mailbox to a PST. This may be a good opportunity to educate the user about starting to use their mailbox from this point forward since this solution will dramatically reduce the data stored on the Exchange server, thereby solving quota issues for most users.

Question: Why don't I see the options for Offline Vault in my Outlook client?

Answer: **No Laptop** – Offline Vault should only be deployed to employees that are using a laptop. There are some exceptions to this, but to confirm if a user should have Offline Vault functionality check the Group Provisioning table above and see what group the user is a member of. If the user has a laptop but is in a group that does not have Offline Vault enabled move them into the appropriate group and then Offline Vault should be created automatically by the next day. **Cached Mode** – If cached mode in Outlook is not turned on then Offline Vault options will not be available. If cached mode was turned on at some point since Enterprise Vault was deployed then Offline Vault will exist, but it only updates while cached mode is enabled. **Tests** – To see if Offline Vault is working go to Outlook –> File –> Work Offline (or just unplug the network cable) and then double click on an email that is stored in the vault and it should open up. Another option is to go to the directory C:\Documents and Settings\USER PROFILE\Local Settings\Application Data\KVS\Enterprise Vault and ensure there is a folder there that has at least one .db file.

Question: Why didn't an email automatically archive since it is older than three months for the company (or larger than 2 MBs and 1 month old) or six months for the parent company?

Answer: **Check Modified Date of the Email** – Enterprise Vault checks the modified date of the message to determine whether it is old enough to be archived, so even though it might have been received eight months earlier the email might have been modified which changes this date. Go to the Field Chooser in Outlook by right clicking on the From category above the inbox and selecting Field Chooser. Then in the pull down

choose All Mail Fields and drag the Modified date over. If this date is older than six (three) months it should be archived. If an email was archived and then restored it resets date so it won't be automatically archived for six more months.

Question: Can I import my PST into my mailbox?

Answer: **Yes** – With Enterprise Vault there are two options to put email from PST's into a mailbox. The first is simply to copy the email into the mailbox and then email older than 6 months will archive overnight. A better option is to send the ticket to ITIS and we can manually import the PST into their mailbox, in which case it will be automatically archived and shortcuts created immediately and the user should see very little impact to the size of their mailbox. For example a 2 gig PST could be archived and take up as little as 20 megs against the mailbox size. For this to be completed efficiently it is ideal to instruct the user how to remove the PST from their outlook client and then put in the ticket the location of the PST and queue to ITIS. In this case we can easily import it while they are accessing their email.

Question: When I view email in groups by going to View –> Arrange By –> Show in Groups and try to delete a whole group I get an Enterprise Vault error.

Answer: **Known Limitation in Enterprise Vault Client** – The client by default does not allow group deletions, but you can select all messages under a group to delete or you can select the group name and one email under the group and delete it.

Question: Why does Outlook crash or hang when I try to archive many emails at once? How can I automatically have emails archived sooner?

Answer: **Known Enterprise Vault Limitation** – Enterprise Vault does not work effectively when the client tries to manually archive many emails at once, in particular usually over 20 emails at once. Results can vary, but I generally find I can archive many emails at once but Outlook will crash, although the emails will still get archived. There is no way to schedule many emails to archive overnight; rather they have to meet the age/size requirements that have been configured. Currently there is no way to configure a folder to have all email automatically archived in that folder.

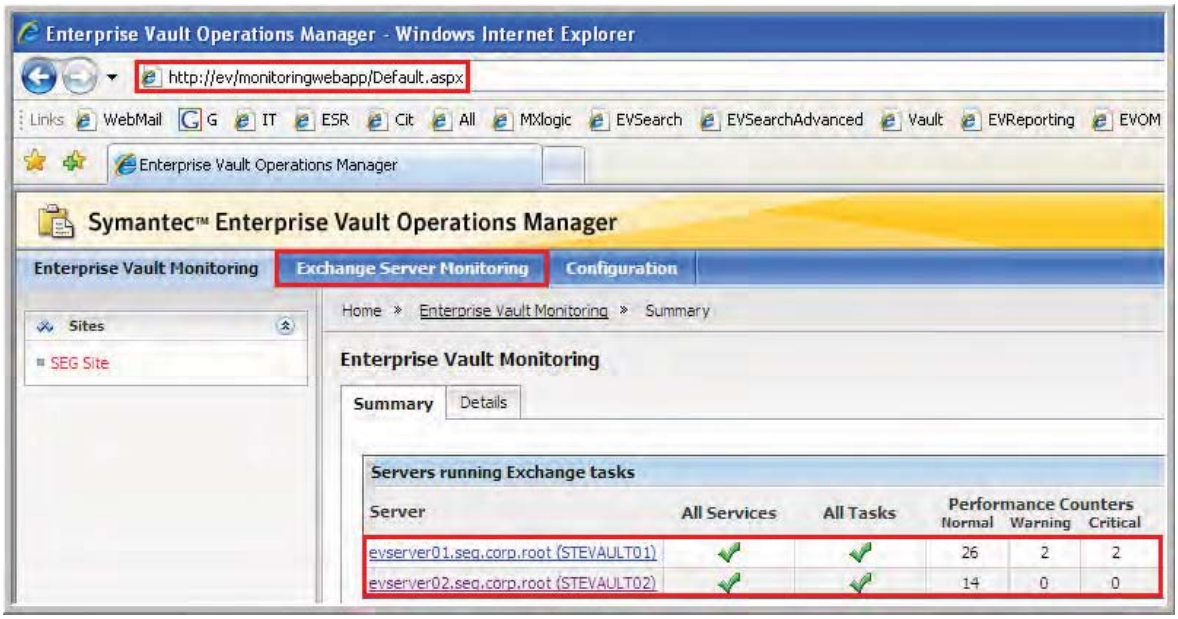
Daily/Monthly/Quarterly Administration and Maintenance

Below is a checklist to follow to ensure that all checks are completed.

□	**Frequency**	**Task**
	Daily	Enterprise Vault Operations Monitor - **http://ev/monitoringwebapp**
	Daily	Journaling - **http://esr/evreport.asp**
	Daily	Vault Store Usage - **http://ev/enterprisevault/usage.asp?AltServer=**
	Weekly - Wednesdays	Scheduled Tasks on STEVAULT01 and STEVAULT02
	Weekly - Wednesdays	Enterprise Vault specific event logs on STEVAULT01 and STEVAULT02
	Weekly - Wednesdays	Maintenance Tasks on STEVAULTSQL01
	Weekly - Wednesdays	Enable all new mailboxes on Eagle1, Eagle2, STEXCHANGE03, STEXCHANGE04
	Monthly - 1st of Month	Check Message Queues on STEVAULT01 and STEVAULT02
	Monthly - 1st of Month	Drive Space on STEVAULTSQL01, STEVAULT01 and

		STEVAULT02
	Monthly - 1st of Month	EV Patches - http://seer.entsupport.symantec.com/docs/EVME_digest.htm
	Quarterly - Jan/Apr/Jul/Oct	Audit of mailboxes - ensure all mailboxes are enabled for archiving

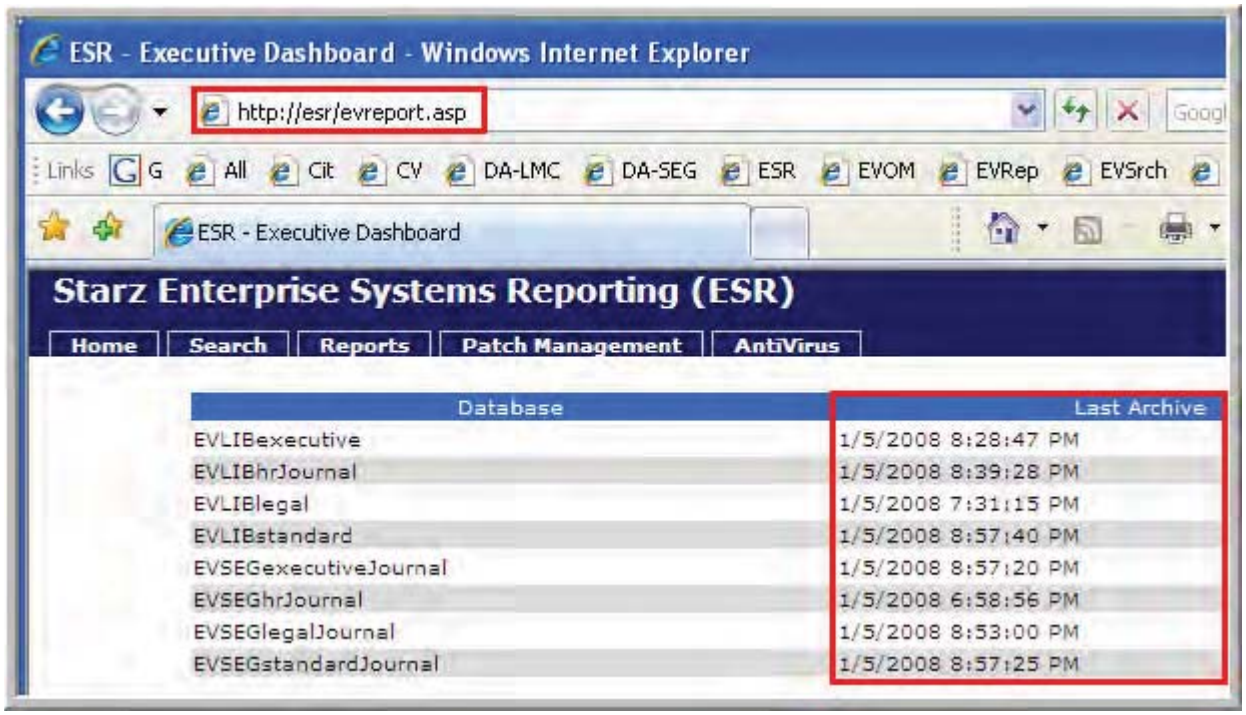
Daily - Check the Enterprise Vault Operations Manager to note if there are any obvious issues with services, exchange journaling, critical and warning event logs. You can access the site by going to http://ev/monitoringwebapp. Then click on the server to get detailed information as to what the warning messages are.



Weekly - Check the EV related Event logs on all of the Enterprise Vault application servers (STEVAULT01 and STEVAULT02 for email archiving and journaling), in particular if errors were noted in EVOM. It is a good practice to review these logs ever week or so as time permits.

Weekly - Confirm that the scheduled tasks on the application servers are running. These put the database in read only mode so that the database and vault can be backed up properly. The vault usage and EVOM checks will most likely catch any issues with these scheduled tasks, but occasionally they should be checked to make sure they ran the night before.

Daily – Check the following website to confirm that journals are being updated on a consistent basis. http://esr/evreport.asp. The journal time stamp should be close to the current time. Note that the EVHRJournal at this time has only one mailbox, so it might have a longer lag in time, but it should still not be too long. If the journal does not show up to date the index might need to be rebuilt. The best step to initially take is to open the journal mailbox – see Section IV in the master document for detailed information on that configuration.

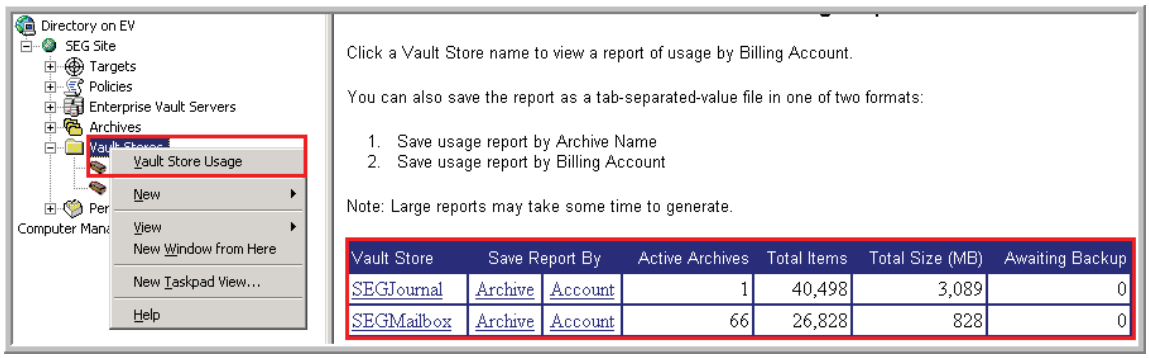


Monthly - On a monthly basis go to computer management and connect to STEVAULT01 and browse to Services and Applications > Message Queuing > Private Queues and click on the queue that ends with "a5" and then click on queues. This queue should never go over 2 times the number of mailboxes that are enabled. If it does then there is not enough time to archive mailboxes and this will need adjusted. Check the J3 queue on the STEVAULT02 and confirm this queue is not getting backed up as this is the automatic archiving queue for journaling.

Monthly - Keep track of drive space on the SQL server and EV Application servers. Ensure SQL backups are truncating the logs and deleting old database backups. These have SAN connected storage so space can be allocated as it becomes necessary. You can also create a new vault partition, but this isn't really necessary and when you do this Single Instance Storage no longer works in connection to that closed partition.

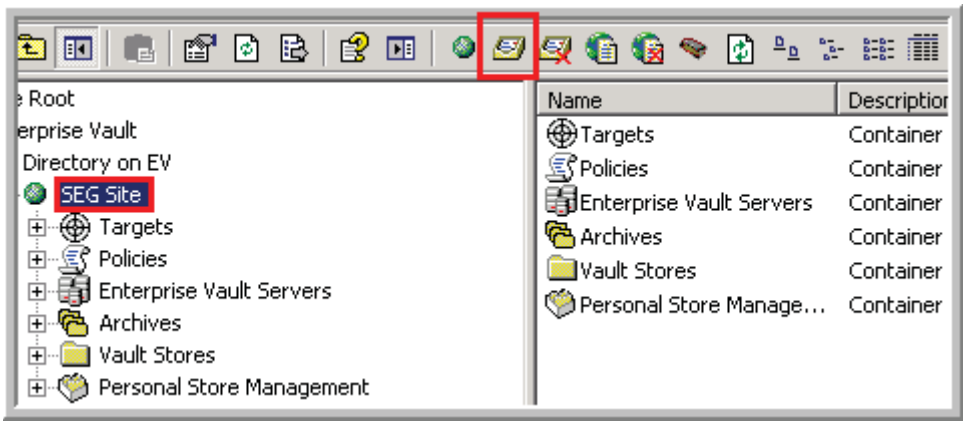
Monthly - Check the following site monthly for known issues, patches, etc. http://seer.entsupport.symantec.com/docs/EVME_digest.htm

Daily - Check the Vault Store Usage daily. You need to do this from the one of the EV App servers by browsing to the Vault Stores and right clicking and select Vault Store Usage. You want to confirm that the SEGMailbox journal doesn't have much or any awaiting backup. If this number is high it might mean the backup didn't run the night before and reset the archive bit, but if some people manually archived data this number would not be zero.



Weekly - Check the maintenance schedules on STEVAULTSQL01 and ensure the backup and integrity check and the history cleanup jobs completed successfully. In particular the history cleanup as this has had issues. If it hasn't run manually delete all DB backups located on the H drive older than 2 weeks.

Weekly – Every Wednesday enable all new mailboxes on all mail servers, currently Eagle1, Eagle2, STEXCHANGE03 and STEXCHANGE04. To do this click on the SEG site and then the Enable Mailboxes for Archiving Icon shown below. Then select each server and go through the wizard and enable any mailbox that shows up. There often are not any new mailboxes on the EAGLE servers, but almost always on the company exchange servers.



Quarterly - Quarterly run the following query on SMS2003 for a list of all users that have mailboxes in the companies but are not in the database for Enterprise Vault. It doesn't matter if the user is enabled or not, just that they are in a DL that has been provisioned in Enterprise Vault. NOTE: All UK users in DL-SEG-EVault-UK will show up in this audit, but should not be emailed to Robin as they are exempt. Email the results of this query to help desk manager, but most importantly if it contains a lot of mailboxes determine why they were never added to a distribution list, i.e. generic email accounts might not get caught.

```
Select Distinct
Full_User_Name0,a.User_Name0,C.Office,Windows_NT_Domain0,D.AD_Site_name0
from V_R_User A
inner join stitutils01.sysident.dbo.users C on A.user_name0=C.UserName
left join V_R_System D on A.User_name0=D.User_Name0
Where PasswordNeverExpire=0 and AccountDisabled=0
and Firstname<>'' and LastName<>''
and Full_User_Name0 not like '%@%'
And a.User_Name0 not In (
select mbxNTUser
from stevaultsql01.EnterpriseVaultDirectory.dbo.ExchangeMailboxEntry )
```

Patching

Symantec reviews all patches Microsoft releases within 60 days of them being released to determine whether they will impact the application. There might be

information in the following location:

http://seer.entsupport.symantec.com/docs/EVME_digest.htm

The Front-End servers for exchange need controls so the icons show up in webmail, so when patching front end servers at times the controls are updated and any custom controls, like for Enterprise Vault, may not be copied over. If that is the case we will need to reinstall Enterprise Vault 2007 (refer to earlier documented process). The controls can be seen in c:\program files\exchsrv\exchweb