Enterprise Vault

Enterprise Vault 7.0
What’s New?

January 2007
# Table of Contents

**Introduction** ................................................................................................................................. 3  

**Intelligent Archiving** .................................................................................................................. 4  
- Automated Classification Engine ................................................................................................. 4  
- User Classification Engine ........................................................................................................... 5  
- Enterprise Content Management Integration .............................................................................. 7  

**Best In Class Microsoft Integration** .......................................................................................... 8  
- Exchange 2007 Support ................................................................................................................ 8  
- Windows Desktop Search .............................................................................................................. 9  
- Windows Rights Management Services ....................................................................................... 9  
- Instant Message Archiving ........................................................................................................... 10  
- Microsoft Cluster Server support .............................................................................................. 11  
- Microsoft Entourage and Safari ................................................................................................ 11  

**Enterprise Scale Administration** .................................................................................................. 12  
- Granular Provisioning ................................................................................................................... 12  
- Roles-based Administration ........................................................................................................... 13  
- Advanced Reporting, Monitoring & Diagnostics ........................................................................ 14  
- Reporting ...................................................................................................................................... 14  
- Monitoring ................................................................................................................................. 15  
- File System Archiving Management ........................................................................................... 16  
- FSA Reporting ............................................................................................................................... 17  
- Push-Install of the Placeholder Service ....................................................................................... 17  
- Data Mover Utility ....................................................................................................................... 17  
- File Groups ................................................................................................................................. 17  
- EMC Celerra Support .................................................................................................................. 18  

**Conclusion** ...................................................................................................................................... 18
Introduction

The pressure on organizations to protect and manage data as intensified with the recent growth in unstructured data and the reliance on email to communicate and exchange documents. Many companies now consider email to be mission critical. In fact, recent studies suggest that email and other messaging applications store as much as 75 percent1 of a company's intellectual property. So, how do organizations protect their email data when email is expected to be available 24 hours a day, seven days a week? And what if a legal challenge requires IT to find files and email related to last quarter's earnings? With little extra time to maintain backup windows, IT administrators are challenged to meet stringent business requirements. Also, in spite of exponential data growth and increasing user demands for data recoverability, IT budgets remain flat.

Symantec Enterprise Vault software answers these challenges. Managing millions of mailboxes for thousands of customers worldwide, Symantec Enterprise Vault provides an intelligent archiving platform that stores, manages, and enables the discovery of corporate data from email systems, file server environments, instant messaging (IM) platforms, and collaboration and content management systems. Because not all data is created equal, Enterprise Vault utilizes intelligent classification and retention technologies to capture, categorize, index, and store target data to enforce policies and protect corporate assets while helping to reduce storage costs and simplifying management. It also provides specialized applications, such as Discovery Accelerator and Compliance Accelerator, that mine archived data to support legal discovery, content compliance, knowledge management, and information security initiatives.

On December 14, 2006 Symantec released the Enterprise Vault 7.0. This version is by far one of the most important Enterprise Vault releases in recent history. Why? The features and functionality introduced take enterprise archiving to a whole new level, raising the bar on what archiving is and how companies can use it. From integrating with existing enterprise content management (ECM) systems to automated or user classification engines, Enterprise Vault 7.0 continues on the tradition of adding structure to traditionally unstructured or semi-structured data.

As the name implies, this white paper is intended to introduce you to some of the new features of Enterprise Vault 7.0 and help you understand their importance and how you can benefit from them.
Intelligent Archiving

Many companies use e-mail as a primary business tool. Orders, contracts, and other similar types of data need to be maintained either voluntarily or due to regulations. Intelligent Archiving brings the benefit of controlled preservation and disposition of these documents with granular retention of record and non-record items. Intelligent Archiving can also extend corporate policies into the archive which will preserve and hold items in place. Enterprise Vault 7.0 introduces several new features that enable the intelligent archiving of corporate information, including:

- Automated Classification Engine - Automatically classify and archive email based on content and metadata reducing archive sizes and minimizing search times.
- User Based Classification Engine - Enable user-driven classification of email to tag items for faster and more efficient search and review.
- Enterprise Content Management System Integration - Enables companies to incorporate archiving with their records management systems.

Automated Classification Engine

Symantec Enterprise Vault 7.0 Automated Classification Engine (ACE) software extends the existing capabilities of Enterprise Vault 7.0 to include intelligent, content-based categorization and tagging of email for Microsoft Exchange environments. Specifically, automated classification enables Enterprise Vault to apply rules to email and categorize messages according to content or context.

Symantec Enterprise Vault 7.0 ACE enables content-aware archiving by:

- Determining whether email needs to be archived or discarded.
- Assigning appropriate tags to each email. One tag corresponds to a retention category, which determines how long the email is retained in the archive.
- Enabling greater efficiency by the Symantec Enterprise Vault Discovery Accelerator and Compliance Accelerator tools. These tools leverage the tag categories to enable managers to zero in on items of interest when searching for and reviewing archived email, or including or excluding content for review.
- User-based Classification Engine
- ECM Connectors

Key Benefits

- Automatically classify and archive email based on content and metadata
- Lower storage costs and resources
- Avoid archiving junk or irrelevant content (e.g., newsletters, bounce messages)
- Provide context and insight into what is archived
- Enable granular retention
- Search and review faster and more efficiently
Symantec Enterprise Vault™ 7.0 User Classification Engine (UCE)

Symantec Enterprise Vault 7.0 User Classification Engine (UCE) software extends the email classification, capture, and retention capabilities of Symantec Enterprise Vault to every user’s desktop. By providing a comprehensive, policy-based email capturing process, it enables all business-critical and regulated email to be classified as each item is created or read by the user. This helps enforce user retention policies more effectively by taking control of records where they are most vulnerable—under the control of employees on personal workstations.

Symantec Enterprise Vault 7.0 UCE software applies a flexible classification process that automatically collects metadata about an email message (e.g., sender, recipient, date, attachments). UCE then determines candidate classifications from the available predefined categories based on the metadata of the message (e.g., Personal, Business, Junk). UCE presents the candidate classifications to the user through a policy-controlled pop-up menu. Some information may have multiple classifications determined by different users within the enterprise and can be classified accordingly.

Key Benefits
- Enable user-driven classification of email
- Lower storage costs and resources
- Avoid archiving junk or irrelevant content (e.g., newsletters, bounce messages)
- Enable granular retention schedules
- Tag items for faster and more efficient search and review
Enterprise Content Management Integration

Many organizations have made considerable investments in ECM/RM technology and would like to leverage those policy definition and end user interfaces for their official corporate records, while physically storing, indexing, and potentially searching those records in the Enterprise Vault behind the scenes. These integrations are provided and supported by Symantec in the form of several “ECM Connectors” in Enterprise Vault 7.0, and they ultimately prevent conflicts between retention policies and the storage of content in two physical repositories.

Using the ECM Connectors, organizations can manage retention policies and view archived content within their existing ECM application, while utilizing Enterprise Vault for the cost-effective and long-term storage, E-Discovery workflow, and legal hold capabilities.

ECM is ideal when companies are simply looking to incorporate a records management solution to their archiving solution. Some of the ECM choices that Enterprise Vault provides are

- Documentum Content Server, Retention Policy Svcs v5.3
- IBM DB2 Content Manager, Records Manager v8.3
- Open Text LiveLink Records Manager v9.5
- Stellent Universal Records Manager v7.5 (connector available from Oracle)
- MDY FileSurf v7.5 (connector available from Computer Associates)

The ECM connectors are designed to let the existing ECM solutions continue to provide the policy configuration and primary end-user interfaces, while storing, searching and securing the content behind the scenes in Enterprise Vault. The ECM system creates a new reference to archived items and sets retention. In many, but not all cases, end users “drag and drop” items into managed folders to define the classification for each message. The physical content is de-duplicated (“single instanced”) by Enterprise Vault behind the scenes.

Key Benefits:

- Integrate email archiving with ECM environments
- Help reduce and control storage costs
- Let ECM system set retention policies
- Archive records and preserve them in place
- Archive nonrecords (e.g., contents of mailboxes)
- Integrate search of records and email
- Preserve and hold items in-place
Best In Class Microsoft Integration

Exchange 2007 Support
The Enterprise Vault Engineering team has worked with Microsoft on Exchange 2007 (formerly Exchange 12) since 2004. In the early days, Symantec provided feedback which was one of the inputs that led to the new style of journaling in Exchange 2007.

We also joined the partner Technology Adopter Program (TAP) which is Microsoft’s vehicle for working with partners, testing integration and getting feedback. We first saw a preview of Exchange 2007 in March 2005. We did our first integration testing in early 2006 and worked extensively with Exchange Engineering on ensuring the integration is robust from the onset. We made our TAP integration code available to customers of Enterprise Vault in the summer of 2006.

Although many new features in Exchange 2007 appear to be similar to Enterprise Vault we have identified many areas where Enterprise Vault continues to add value to Exchange environments including:

- **Moving inactive data out of Exchange altogether.** While mailboxes are bigger in Exchange 2007, they are still not big enough to cope with the volume of email organizations send, receive and retain today. So migrating inactive email is still a best practice.
- **Reducing email duplication and compressing email.** Email in Exchange 2007 continues to be highly duplicative, with large email forwards with big attachments using up significant storage space. Enterprise Vault continues to provide single instance storage and compression of data from Exchange 2007.
- **Migrating email to cheaper storage.** While Exchange 2007 allows for cheaper storage such as NAS, the truth is many customers look at long-term, less active data in archives as having a lower performance and availability SLA as compared to Exchange (and therefore a lower cost per TB).
- **Reducing backup, recovery and defrag windows.** While Exchange 2007 allows more data to be kept online, traditional backup, recovery and defrag windows continue to grow with the size of the message stores. Enterprise Vault, as always, allows customers to shrink these windows and improve operational efficiency.
Windows Desktop Search

For many years, Enterprise Vault customers have requested to extend the powerful search in Enterprise Vault to index messages still residing in Exchange and to make the full-text search across attachments also available when offline. Benefits of this include both an increase in functionality as well as a decrease in end-user training and frustration. The new search integration delivered in Enterprise Vault 7 allows end users to search non-archived content together with archived content that is currently stored in their offline vault.

In the last couple of years, Desktop search tools are gaining traction in general. First the focus was clearly on private usage, such as finding a specific Word document on the local disk, but in the recent months the “hype” has reached the business world. Deployment is easy, training is limited, and users are familiar with the comprehensive search paradigm from the Web.

The value proposition of a unified search has led to a viral adoption with millions of WDS client downloads already. With Microsoft pushing Windows Desktop Search for Windows XP (which is freely available via download) and by embedding the same search technology in Windows Vista and Outlook 2007, it is not a question of “if” companies will use it, but “when”. For any organization answering that question with “Now”, Enterprise Vault 7 is already there to help.

Windows Rights Management Services

Enterprise Vault 7.0 provides native integration with Microsoft’s Rights Management Services so that encrypted messages that need to be archived are decrypted and indexed applying the necessary retention policies and enabling these messages to be searched and retrieved in the event of litigation or regulatory investigations.

The integration of Enterprise Vault and RMS (See Figure 1 below) allows customers deploying for information protection can now protect messages from unauthorized view, edit, copy, print or
forward...basically maintaining the rights management enabled fields within the message. This also helps to limit file access to authorized users and keeps an audit trail for tracking usage of protected files.

Enterprise Vault is the first archiving solution to integrate with Microsoft RMS in a way that provides the ability to discover information that is protected by the Windows Rights Management Services and RMS-enabled applications, such as Microsoft Office.

Once installed, the Enterprise Vault Adapter for RMS ensures that any email protected and encrypted using Microsoft Windows RMS is stored safely in the Enterprise Vault and fully searchable from the Discovery and Compliance Accelerator products. Specifically, the Adapter for RMS decrypts email messages so that they are stored in the archive "in the clear." The content is now protected by the Enterprise Vault security system and AD-based authentication mechanism.

Therefore this does not mean a reduced security of the information, as the RMS protection of mail accessible by end users remains intact. For example a RMS policy that defines the expiry of the content, such as a number of days after publishing, would render the document useless for further usage by the end-user in his personal archive. Still it could be searched and produced by authorized staff from the journal, but only after authenticating against Enterprise Vault and in conjunction with a full audit trail.

Figure 1

Instant Message Archiving

Enterprise Vault now contains an embedded version of Symantec’s IM Manager to provide a single point of storage and review for Instant Messages and E-Mail. Instant Messages are captured by an embedded version of Symantec IM Manager across 13 major protocols including Microsoft Live Communications Server (LCS), IBM/Lotus Sametime, AOL, MSN, Yahoo, Bloomberg, Reuters and Google. IM Manager and Enterprise Vault ensure that all electronic messaging can be reviewed, filtered and stored according to policy.
Microsoft Cluster Server support

Because archiving has become as mission critical as email itself it is important that Enterprise Vault offer our customers their choice of HA solutions. This escalation of criticality is primarily driven by 1) the archiving application is often tied to the “Tier 1” status of email and 2) driven by e-discovery and compliance requirements. In addition to the previously supported Veritas Cluster Server, Enterprise Vault 7.0 we have added Microsoft Cluster Server to the supported HA solutions that enable Enterprise Vault to be clustered and made highly available.

Making Enterprise Vault and Exchange highly available customers can significantly reduce the risk of downtime of both the email system as well as the archive. This is supported by automated monitoring and failover of systems and services in the event of failure due to mechanical, human or natural disaster. All adding up to providing users with flexible configuration and deployment options with solutions they are familiar with to easily add high availability to their archiving environment.

Microsoft Entourage and Safari

Many organizations have subset of Mac users who are often in critical roles (executives, creative, etc.). Enterprise Vault 7.0 introduces support for Microsoft Entourage and Safari to enable access to archived items via the Entourage email client and archive search and retrieve functionality via web based search in Safari. Adding support for Entourage and Safari allows Enterprise Vault to be deployed in mixed Windows/Mac environments and providing an integrated user experience for Mac users.
Enterprise Scale Administration

Archiving has quickly moved beyond an Exchange administrator’s pilot project for reducing Exchange storage to an integral part of an information lifecycle strategy for many companies. This often requires many different types of users to manage parts of the archive. Because email is a mission critical application, archiving should be treated equally mission critical. To do this it is critical the archive administrator has access to real time performance metrics, reports and analytics to ensure the application and the archive are running as expected. Enterprise Vault 7.0 introduces new features to make the management of the archive simple while maintaining the power and flexibility our customers demand.

Granular Provisioning

Enterprise Vault 7.0 provides granular policy management to make it easy for administrators to automatically enable new and existing Exchange users with tailored mailbox archiving policies. Provisioning can be used to identify users who require unique archiving settings, such as terminated employees, or VIP individuals, and give them distinct archiving and retention policies that are different from the majority of the user population. Macintosh and laptop users may need unique client settings, due to the capabilities of their mail client and the way it is used. It is also possible to use Enterprise Vault’s granular policies and provisioning features to properly scale a large archiving implementation, dividing the user population evenly across multiple Enterprise Vault servers and storage devices.

Because not all users are created equal and one size should not fit all IT organizations need any easy way to manage the exception user(s). This is accomplished in Enterprise Vault 7.0 through a new administrative feature called Granular Provisioning. Granular provisioning ensures every user gets the what they require while providing variances for the “exception” user. Variances include different age-based policies, they could be different retention policies or even short cut expiry for a given set of users. For example, The Boss may have a different requirement from the
rest of the Exec Staff. And specific users in a given Line of Business may be regulated and have a different retention policy than the other knowledge workers. Granular provisioning enables these variances to be put in place. Policies can be configured by Active Directory attribute via LDAP, AD group, or even down to an individual mailbox.

**Key Benefits:**
- Simplifies management of Enterprise Vault
- Easier to handle exception users
- Enables IT to respond to user needs quickly
- Allows more effective control of Exchange storage

**Roles-based Administration**

As organizations grow and IT teams specialize in application and hardware tiers, there are increasing demands for enterprise-class software to provide granular security control to portions of the product. As an enterprise-wide platform for content archiving, Enterprise Vault is often administered by many diverse, and at times disparate, individuals and teams. These administrators often need only limited access to manage their own part of the application, both for security concerns, as well as to limit liability and risk to the fewest number of individuals.

For instance, network administrators may need to manage and archive their own file servers, without being exposed to email archiving objects and functions. Or, there may be a separate storage team that should only have archive storage access for backups, while the desktop team should only be able to enable users for mailbox archiving. And, in a distributed environment, local teams may need to narrow their focus to only their own Enterprise Vault site.

Enterprise Vault 7.0 provides Roles-based Administration just for this purpose. First, it creates a set of roles for grouped functions of the product (e.g., File Administrator role for file archiving functions); next, it allows administrators to modify the defined roles as needed; and finally it allows an administrator to specify which other users or groups belong to the various roles. By doing this, Enterprise Vault administrators no longer need to share a single Vault Service Account (VSA) and password that has complete administrative rights to the entire archiving platform.

**Key Benefits:**
- Reduce cost of management
  - Delegate day-to-day tasks to first tier support
  - Leverage infrastructure across email, file, etc.
  - Leverage infrastructure across sites
- Improve security
  - Remove need for interactive access to VSA
  - Allow separation between business units, etc.
Advanced Reporting, Monitoring & Diagnostics

Reporting

Enterprise Vault has historically allowed administrators to monitor the ongoing status and health of the application through standard Microsoft toolsets such as the Microsoft Management Console, Performance Monitor, and Microsoft Operations Manager. Often, though, many administrators need to quickly and proactively track the health of various services over time, without requiring a MMC plug-in, or creating custom scripts and tools to do so.

Symantec offers just these capabilities through Enterprise Vault’s own web-based application called Enterprise Vault Operations Manager. It monitors local and remote Enterprise Vault servers, allowing administrators to:

- Review the status of Enterprise Vault services and tasks on any server in the same logical Enterprise Vault site.
- View Performance counters for vault stores, disk, memory and processors.
- Monitor Exchange journal mailboxes using a number of message counters for Inbox, Archive Pending, and failed operations such as Failed Distribution List Expansion.

Key Benefits:

- Reduce cost of management
  - Lessen need for custom tools
  - Lessen need for custom scripting
- Allow less experienced admins. to report on EV
  - Easily provide information to IT staff
Monitoring

As discussed earlier archiving has become as mission critical as email. Because of this the pressure has increased on IT to ensure the archive is running as expected. As with email, archiving is made up of many complex operations making for a complex environment. To add fuel to the fire there are different stages of archiving a message can be in. Monitoring today is relatively manual. Typically log files, SQL queries and customer tools are employed to answer questions about the health and wellbeing of the archive.

Enterprise Vault 7.0 eliminates these manual processes and incorporates this critical information into a centralized, web based monitoring tool for admins to proactively track service health, quickly identify journaling issues and customize monitoring thresholds to get alerted in the event anything moves above a pre-defined threshold. The Enterprise Vault monitoring features look at all aspects of the EV infrastructure including: Server status, Tasks status and server health.

Key Benefits:

- Reduce cost of management
- Lessen need for custom tools
- Lessen need for custom scripting
- Allow less experienced admins. to monitor EV
File System Archiving Management

The new management features in Enterprise Vault File System Archiving enables a consistent task model across content types. These new features are now combined in the common Enterprise Vault management console. The new features include new policies, new reporting features and new management tasks easing day to day management, file server consolidation, migration, and recovery.

Enterprise Vault 7 ships with the following new FSA features
- Archive Points can now be set from the Administration Console
- EMC Celerra Placeholders
- EV Task visible in Task Controller Service
- Delete-on-delete & Delete-on-recall
- Pruning can now be controlled from VAC
- Addition of “file-groups” to ease policy and rules management
- Data Mover Utility to help with placeholder maintenance tasks
- Push Installation for Placeholder Service
- Outlook on FSA Server no longer required

Other Version 7 features that provide additional value for FSA customers
- Roles-based Administration
- Reporting and Monitoring with Enterprise Vault Operations Manager
- Microsoft Cluster Support for Enterprise Vault servers.
FSA Reporting

Comprehensive report files can be created either during the production run or in a “report mode” which creates a “what if” analysis without changing the information on the file server. This integrated reporting facility allows administrators to quickly identify which files get archived by which policy and rule, what volume of information can be migrated from the file server and if the files have any explicit permissions.

Push-Install of the Placeholder Service

To help with the deployment of Enterprise Vault – especially in distributed environments – it is possible to “push” the placeholder service out to remote file-servers, without the need to log-in locally on the file-server machine. This streamlines deployments in larger organizations and reduces the burden of managing large numbers of file-servers.

Data Mover Utility

The Data Mover Utility enables Enterprise Vault administrators to do a lot of complex tasks with Placeholders that we couldn’t do before. These include; recreating missing placeholders for files that have already been archived, recreating missing Archive Points, restoring some or all files to a volume or folder, and moving placeholders between file servers. Although initially this tool is limited to placeholders on Windows File Servers, this is a major step forward to helping administrators in moving and consolidating file servers. This is also be a great “get out of jail” utility when user accidentally deletes their placeholders and discovers, too late, that their backup software was not configured to back them up.

File Groups

In Enterprise Vault it is possible to specify a “File-group” based on the standard file extensions of the file-types belonging to the group. A typical example would be to create a group called “Office Files” and add the extensions “*.doc, *.xls and *.ppt” to it. These groups can be referenced later during the policy creation and simplify the rules management in more complex deployments. Instead of changing dozens of policies once a new file-type is added to Office, a simple update of the file-group will take care of all necessary changes.
EMC Celerra Support

To provide the same seamless access to data archived from a Celerra NAS device, Enterprise Vault delivers a comprehensive integration with the Celerra dhsm-API, including the capability of tracking delete actions (Delete-on-delete) and optional pruning when multiple versions of an item have been archived.

This integration is available on all Celerra systems that run the “DART” NAS-operating system in version 5.5 or higher. For tracking deletions the Celerra Logging needs to be enabled and configured.

Conclusion

With the recognition over the past five years that email has become as mission critical as any other IT system, most organizations are evaluating their overall policies and systems for managing email. Across many business industries and public sector organizations, IT professionals are being called on to address the three most common management concerns around email:

- **Resource management**: How do we keep these systems up and keep our costs under control? With sprawling message stores, longer backup windows, annoying end-user quotas and out-of-control “rogue” archives (e.g., Microsoft .PST files), IT is struggling to keep email “up and running” without breaking the budget.

- **Retention management**: How can we enforce a consistent retention policy on email? At the same time, IT organizations are being mandated by legal and compliance groups to implement enterprise-wide policies on retention for email – rather than leaving it in the end-users’ hands.

- **Discovery management**: How can I quickly get to what I need within our mass of email? Finally, as email has increasingly become the “smoking gun” in litigation and regulatory investigations, most large organizations now know that if the email is out there, they may be asked to find it.

Email has not only evolved into a primary form of business communication, but also has become a primary weapon in a prosecutor’s arsenal. A 2004 survey of 840 US companies, co-sponsored by the ePolicy Institute, found that 21% of respondents had had their employee email and instant messaging subpoenaed in the course of a lawsuit or regulatory investigation, up from 14% in a 2003 survey.1. This trend of using emails as evidence in court is expanding outside of the United

---

States. In June, 2005, the Singapore High Court allowed emails presented as evidence in a dispute over negotiations for the lease of a warehouse.

Searching through volumes of backup tapes for requested emails and documents is costly and time-consuming, with no guarantee that all the requested records will be recoverable. A company’s inability to produce all subpoenaed records can result in multimillion dollar fines and long-term damage to its reputation. It is now recommended that companies use archiving and discovery software technologies to ensure that records are retained in a secure repository. This will make records readily available for everyday business use—and companies can quickly and completely respond to an electronic discovery (“e-discovery”) request.

Gartner Group recommends enterprise architects and IT operations managers should include content archiving in their long-term planning. An ICA [Integrated Content Archiving] strategy is needed to respond efficiently to increasingly complex and frequent demands from inside and outside the business. Today, these requests cause unnecessary pain, because content is divided according to the applications that created it and the repositories where it is stored. This siloing of content requires too much time and too many resources to hunt down when a regulator or lawyer asks for it.

Legal departments and IT also must work together to develop document retention systems that not only ensure that records are not accidentally lost or deleted, but can also ensure rapid recovery. And organizations faced with litigation involving e-discovery must be able to apply indefinite litigation hold of relevant content with minimal strain on storage and IT resources. Symantec’s solutions can help your organization close the gap between technology and policies in order to eliminate the risk associated with non-compliance.

We are very excited about this latest release and hope you are too. If you have any questions please contact your Symantec sales rep or account manager for more information. As always you can call us toll-free 1 (800) 745 6054 or find more information anytime on the web at http://www.symantec.com/enterprisevault.