WHITE PAPER: TECHNICAL

symantec.

Confidence in a connected world.

Security Model for Discovery Accelerator 8.0

Rob Forgione
Technical Field Enablement
April 2009

Contents

If you have any comments on this Whitepaper please email EV-TFE-Feedback@Symantec.com

Purpose

The purpose of this document is to detail how Enterprise Vault:

- Provides security surrounding data access for Legal Discovery
- Provides a means for administrators to securely manage the application

This document will give readers a better understanding of how the Enterprise Vault (EV) solution integrates with security features already built into Active Directory. It will also provide insight as to how to configure Discovery roles to be configured in line with organizational preferences.

This whitepaper assumes the reader has already read the Security Model for Enterprise Vault 8.0 and SQL server whitepaper and is familiar with the security concepts of Enterprise Vault. The Security Model series consists of:

- Security Model Enterprise Vault 8.0 and SQL server
- Enterprise Vault 8.0 Security Model for Microsoft Exchange Archiving
- Enterprise Vault 8.0 Security Model for Lotus Domino Archiving
- Enterprise Vault 8.0 Security Model for File System Archiving
- Enterprise Vault 8.0 Security Model for Microsoft SharePoint Archiving
- Enterprise Vault 8.0 Security Model for SMTP Archiving
- **Security Model for Discovery Accelerator 8.0**
- Security Model for Compliance Accelerator 8.0
- Enterprise Vault 8.0 Security Model for Automatic Classification Engine 8.0
- Enterprise Vault 8.0 Security Model for Secure Messaging 8.0

This whitepaper is intended to train the reader the concepts behind security for Discovery Accelerator 8.0.

Enterprise Vault Services

Enterprise Vault uses the following services for Discovery Accelerator:

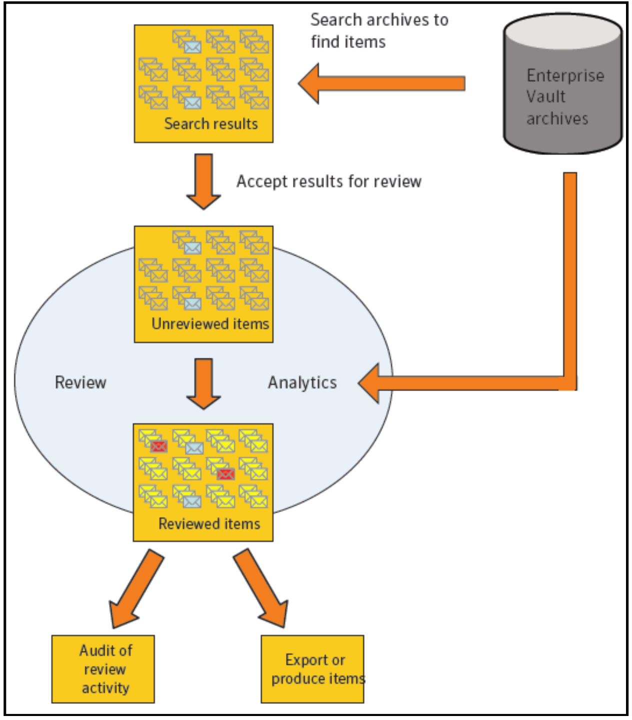
- Enterprise Vault Accelerator Manager Service

This service must run within the context of the Vault Service account.

About Discovery Accelerator

Discovery Accelerator is a fully managed legal discovery and review system that integrates with Enterprise Vault services and archives. Discovery Accelerator enables authorized users to retrieve, review, mark, and publish emails and other electronic messages for lead counsel examination or court-ready production. Using lawyers to review large numbers of items is costly. With Discovery Accelerator, a hierarchy of reviewers can be created for a case, with different levels of reviewers able to assign certain review marks. In this way, less expensive, non-legal staff can perform an initial review of search results, leaving only the relevant or questionable items for lawyers. The relevant items are then assigned an appropriate "Bates" number and published, typically in a PST file, for presentation as evidence in court. Figure 1 illustrates this process. Note here that the application only deals with items that have already been archived by Enterprise Vault.

Figure 1 - Discovery Accelerator workflow



Required Application Permissions

Windows Server Permissions

To ensure that reviewers can view HTML versions of messages, the **Authenticated Users** group must be given **Full Control** access to the Windows Temp folder on the Discovery Accelerator server (typically C:\WINDOWS\Temp). This group also requires Full Control access to the ASP.NET Temp folder on the Discovery Accelerator server (typically: C:\WINDOWS\Microsoft.NET\Framework\v2.0...\Temporary ASP.NET Files\evbadiscovery) so users can mark items if necessary. When setting the permissions, **Allow inheritable permissions from parent to propagate to this object** should be checked.

To allow for any exports from Discovery Accelerator, administrators should ensure that the Vault Service account (VSA) has sufficient Read and Write permissions on the target directory.

SQL Permissions

Discovery Accelerator makes use of 3 types of SQL databases, Configuration, Customer, and Custodian. The **Custodian** database is used for **Custodian Manger** feature which will be discussed shortly. The **Configuration** database specifies the location of the Customer database(s) and stores details of the SQL Server, database files, and log files to use. The **Customer** database is where Discovery Accelerator stores details of cases, user roles, search results, review marks and tags, and more. Organizations can have multiple customer databases. The facility to create Configuration and Customer databases with Discovery Accelerator is dependent on the Vault Service account having the SQL server role of database creator (dbcreator).

Discovery Accelerator provides the facility to create schedules with which organizations can conduct searches repeatedly or at some future time. Search schedules use SQL jobs in SQLSERVERAGENT. To enable creation and modification of these jobs, the VSA must be a **SQL system administrator** (sysadmin)**.** For organizations that do not want to assign the VSA sysadmin permissions, they must grant sufficient permissions and roles to make the VSA a creator and owner of Discovery Accelerator search schedules. Do this by adding the VSA to the msdb system database. Then, grant the VSA Select permissions on the **sysjobs**, **sysjobschedules**, **sysjobsteps**, **sysschedules**, **sysjobsservers**, and **sysjobhistory** msdb tables as well as the **Execute** permission on the **sp_add_category** msdb stored procedure. Finally, assign the VSA the **SQLAgentUserRole** database role.

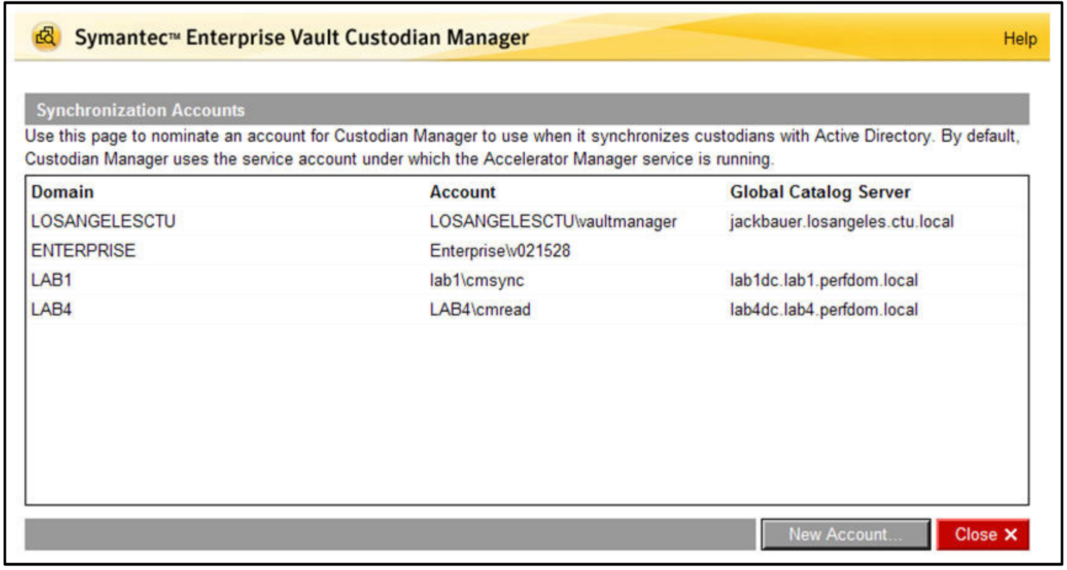
Organizations planning to create the Discovery Accelerator database and Enterprise Vault databases on different servers must create a SQL logon for the Enterprise Vault Service account that is identical to the one on the Enterprise Vault database server.

Custodian Manager

Custodian Manager stores the details of custodians or custodian groups in a database that organizations can search using Discovery Accelerator. A custodian is defined as an individual user. A custodian group is any collection of employees, such as Windows or Domino groups and distribution lists, Active Directory or Domino LDAP searches, and Active Directory containers. Custodian Manager is installed by default with the installation of Discovery Accelerator and uses a Custodian database. The name and account used to manage the database are defined by the installer during the configuration of Custodian Manager.

The process of populating and maintaining the custodians and custodian groups in Custodian Manger is called Directory Synchronization. Directory Synchronization requires a Synchronization Account. By default, Discovery Accelerator will attempt to use the account in which the Enterprise Vault Accelerator Manager Service is running to synchronize with Active Directory and Domino. However, as this might not be ideal for some organizations, designated accounts for synchronization can be defined.

Figure 2 – Custodian Manager Synchronization Accounts



Symantec™ Enterprise Vault Custodian Manager

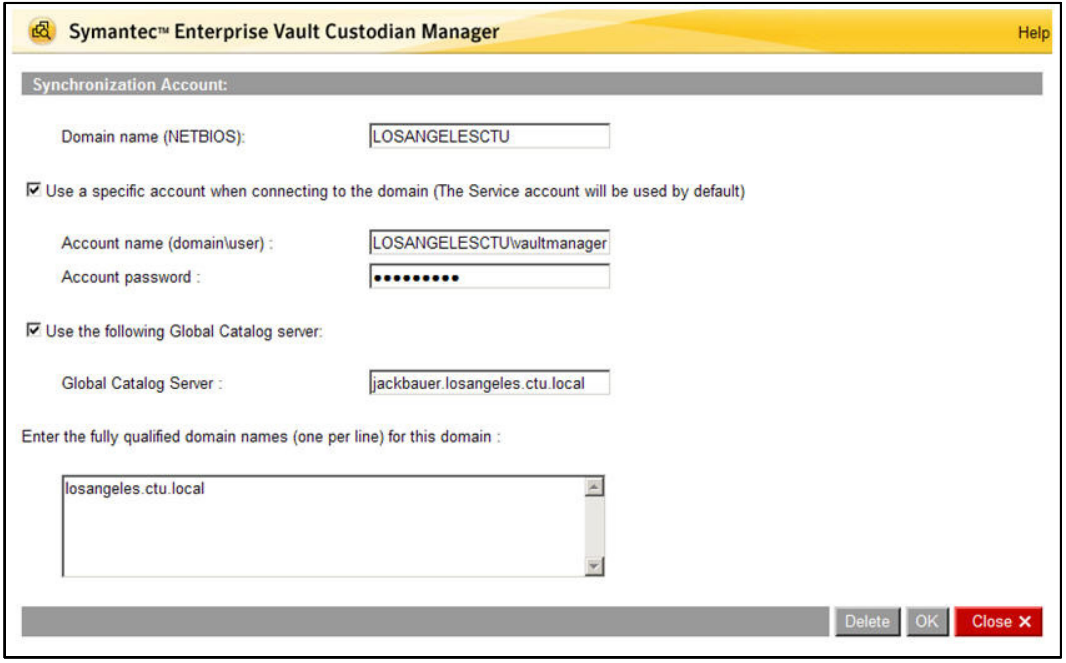
Synchronization Accounts

Use this page to nominate an account for Custodian Manager to use when it synchronizes custodians with Active Directory. By default, Custodian Manager uses the service account under which the Accelerator Manager service is running.

Domain	Account	Global Catalog Server
LOSANGELESCTU	LOSANGELESCTU\vaultmanager	jackbauer.losangeles.ctu.local
ENTERPRISE	Enterprise\w021528	
LAB1	lab1\cmsync	lab1dc.lab1.perfdom.local
LAB4	LAB4\cmread	lab4dc.lab4.perfdom.local

Figure 2 shows 4 domains that contain custodians that an organization wants to manage. Each domain has been assigned a specific synchronization account.

Figure 3 – Defining a Synchronization Account



Symantec™ Enterprise Vault Custodian Manager

Synchronization Account:

Domain name (NETBIOS): LOSANGELESCTU

☑ Use a specific account when connecting to the domain (The Service account will be used by default)

Account name (domain\user) : LOSANGELESCTU\vaultmanager

Account password : ••••••••••

☑ Use the following Global Catalog server:

Global Catalog Server : jackbauer.losangeles.ctu.local

Enter the fully qualified domain names (one per line) for this domain :

losangeles.ctu.local

Figure 3 shows how a specific account and Global Catalog Server can be applied for synchronization. The account password entered here is stored in the custodian database using SQL server encryption which uses a database master key, a certificate, and a TRIPLE DES algorithm. The database master key is created when the first non default synchronization account is defined.

Web Application Port

The Discovery Accelerator web applications use TCP/IP port 8085 by default. If another application on the Discovery Accelerator computer needs to use this port, the Discovery Accelerator configuration files can be configured to use different ones.

To change the port that administration and Custodian Manager sites use, make the following change to both **Web.config** files located in the **AcceleratorAdminWeb** and **CustodianManagerWeb** subfolders of the Discovery Accelerator program folder. Using a text editor find the following line and change the port number to a suitable alternative.

<add value="**8085**" key="RemotePort" />

Additionally, make the following change to the **AcceleratorService.exe.config** file in the Enterprise Vault Business Accelerator folder. Using a text editor find the following line and change the port number to a suitable alternative.

<add key="Remoting Channel Configuration"
value="name=Client Port, port=**8085**,suppressChannelData=false, machineName=, priority=1, secure=true, protectionLevel=EncryptAndSign, useIpAddress=true, bindTo=0.0.0.0, rejectRemoteRequests=false, exclusiveAddressUse=true, impersonate=false, authorizationModule=, typeFilterLevel=Full"/>

After making these changes restart the Enterprise Vault Accelerator Manager service.

Client – Server Communications

Client-server communications are encrypted and digitally signed using port 8086. The user token from the client workstation can only be used by the server for identification, not impersonation. This is provided by the Microsoft.Net remoting framework. If another application on the Discovery Accelerator computer needs to use this port, the Discovery Accelerator configuration files can be configured to use different ones.

To change the ports for client-server communications, make the following change to the **AcceleratorService.exe.config** file in the Enterprise Vault Business Accelerator folder on the Discovery Accelerator server. Using a text editor find the following line and change the port number to a suitable alternative.

<add key="Windows Client Remoting Channel Configuration"
value="name=Windows Client Channel, port=**8086**,suppressChannelData=false, priority=1, secure=true, protectionLevel=EncryptAndSign, rejectRemoteRequests=false, exclusiveAddressUse=true, impersonate=false, typeFilterLevel=Full" />

Additionally, make the following change to the **AcceleratorService.exe.config** file located on every Windows Presentation Foundation (WPF) Discovery Accelerator client. Using a text editor find the following line and change the port number to a suitable alternative.

<add key="AcceleratorServerPort" value="**8086**" />

After making these changes restart the Enterprise Vault Accelerator Manager service.

Roles

Roles are used to maintain security within the application. Organizations configure the Discovery Accelerator roles to suit their business needs. Once set, they can assign those roles to the users who need to fill the roles. The application requires that all people who will use Discovery Accelerator as a system administrator, case administrator, or reviewer must be added to the system. Some roles are effective at the application level, across the entire Discovery Accelerator system, whereas others apply at the case level only. To assist with the creation of roles, a few predefined roles already exist in the application.
Table 1 shows the predefined roles within Discovery Accelerator.

Table 1 – Predefined Discovery Accelerator Roles

Roles	**Description**
Case Administrator	Performs all administrative activities within a specific case. Can search for items to include in the case, review items (and assign work to other reviewers), and export or produce items for offline review.
Folder Capture Messages	Search for new items to add to a research folder.
Folder Export	Export or produce items from a research folder for offline review.
Folder Full Control	Search for new items to add to a research folder, review them, and export or produce them for offline review. Can give access to folders for participation in the review process.
Folder Review	Review and mark the items in a research folder.
System Admin Discovery	Perform all administrative activities within Discovery Accelerator. Can create and manage cases, assign application-wide roles to users, and import configuration data from XML files.

The permissions associated with these roles and their descriptions can be found in the Installing and Configuring Discovery Accelerator PDF that ships with Discovery Accelerator 8.0.

Conclusion

In this whitepaper we have discussed the security aspects of the permissions required on the Discovery Accelerator server as well as the SQL server hosting the databases. We have also discussed the application’s predefined roles.

Below is a list of the other Security Model topics in this series that may be of interest.

- Enterprise Vault 8.0 Security Model for Microsoft Exchange Archiving
- Enterprise Vault 8.0 Security Model for Lotus Domino Archiving
- Enterprise Vault 8.0 Security Model for SMTP Archiving
- Enterprise Vault 8.0 Security Model for Automatic Classification Engine 8.0
- Enterprise Vault 8.0 Security Model for Secure Messaging 8.0
- Security Model for Compliance Accelerator 8.0
- Enterprise Vault 8.0 Security Model for File System Archiving
- Enterprise Vault 8.0 Security Model for Microsoft SharePoint Archiving

About Symantec

Symantec is a global leader in providing security, storage and systems management solutions to help businesses and consumers secure and manage their information. Headquartered in Cupertino, Calif., Symantec has operations in 40 countries. More information is available at www.symantec.com.

For specific country offices and contact numbers, please visit our Web site. For product information in the U.S., call toll-free 1 (800) 745 6054.

Symantec Corporation
World Headquarters
20330 Stevens Creek Boulevard
Cupertino, CA 95014 USA
+1 (408) 517 8000
1 (800) 721 3934
www.symantec.com