symantec™
Confidence in a connected world.

Enterprise Vault 8.0 Security Model for Lotus Domino Archiving

Rob Forgione
Technical Field Enablement
March 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:

- Can securely access data to be archived
- Provides security surrounding end-user access
- Provides a means for administrators to securely manage Domino data

This document will give readers a better understanding of how the Enterprise Vault (EV) solution integrates with security features already built into a Lotus Domino messaging solution as well as Windows Active Directory. It will also provide insight as to how to change some of the settings 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

This whitepaper is intended to train the reader the concepts behind Enterprise Vault 8.0 security for Lotus Domino servers and users of Lotus Notes and Domino Web Access.

Enterprise Vault Services and Tasks

Enterprise Vault’s Lotus Domino archiving solution uses the following Enterprise Vault Tasks:

- Domino Provisioning Task
- Domino Mailbox Archiving Task
- Domino Journaling Task

Domino Journaling

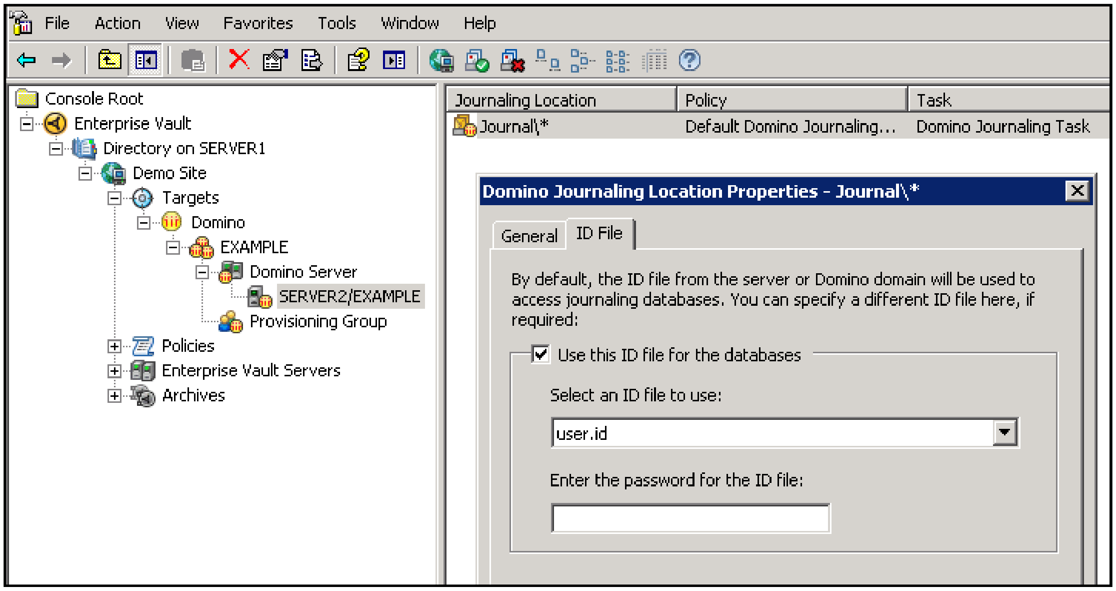
Domino Journaling Task

Access to the Domino journaling databases must be granted to a Lotus Notes ID file in order for the Domino Journaling task to function correctly,. The journaling task will run under the context of this ID referred to as the **archiving ID**. The archiving ID is specified in the Vault Administration console and can be used for all access levels. Alternatively, a different ID file for each level can be used. The access levels are as follows:

- **Domino Domain –** This ID must have Read access to the Domino Directory.
- **Domino Server** – This ID must have access to the Domino server and its directories.
- **Domino Journaling Location** – This ID must have *Editor*, *Designer*, or *Manager* access to the journaling databases, and the *Delete documents* permission. If journaling is configured on the server document to encrypt items when they are journaled to this database, this ID file must be the one that is used to encrypt the items.

Unless specified, Enterprise Vault will use the same ID file used to access the Domino domain to access the Domino servers and journaling locations. Figure 1 shows how the ID File can be selected at the Journaling Location level.

Figure 1 - Journaling ID File



Journaling Location	Policy	Task
Journal*	Default Domino Journaling...	Domino Journaling Task

Domino Journaling Location Properties - Journal*

By default, the ID file from the server or Domino domain will be used to access journaling databases. You can specify a different ID file here, if required:

☑ Use this ID file for the databases

Select an ID file to use: user.id

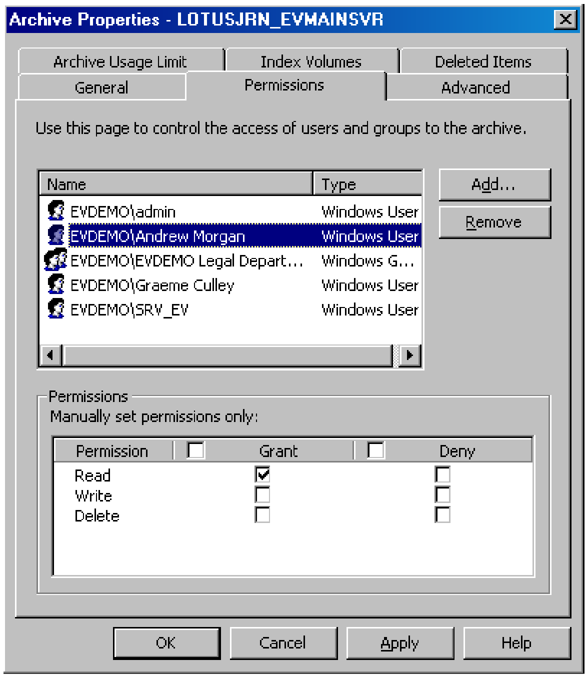
Enter the password for the ID file:

When configuring Enterprise Vault to archive a Domino Journaling location, the archiving ID file(s) must be placed in the Lotus Notes data folder on the Enterprise Vault server that will run the Domino Journaling task (typically C:\Program Files\lotus\notes\data).

Controlling Access to the journal archive

Access to Domino Journal archives is only granted to Windows accounts. This is due to the fact that there is no account or ID associated with a Domino Journaling mail file for Enterprise Vault to authenticate. Therefore, access to the Domino Journaling archives in a pure Domino environment will be granted to the Vault Service account so that applications such as Discovery Accelerator can search the archived data. **Read** permissions must be manually granted for any other accounts that require access to this archive such as auditors or administrators. Permissions can be granted to both Windows Users and Groups. Read permissions, as shown in Figure 2, allow users the ability to search, view, and retrieve items from the archive.

Figure 2 - Domino Journal Archive permission properties



Archive Properties - LOTUSJRN_EVMAINSVR

Use this page to control the access of users and groups to the archive.

Name	Type
EVDEMO\admin	Windows User
EVDEMO\Andrew Morgan	Windows User
EVDEMO\EVDEMO Legal Depart...	Windows G...
EVDEMO\Graeme Culley	Windows User
EVDEMO\SRV_EV	Windows User

Permissions
Manually set permissions only:

Permission	□ Grant	□ Deny
Read	☑	□
Write	□	□
Delete	□	□

Domino Mailbox Archiving

Overview

As noted in the Security Model Enterprise Vault 8.0 and SQL server whitepaper, Enterprise Vault security integrates with an organization's deployment of Active Directory. It is not uncommon to find that some Domino organizations do not employ Active Directory in their environments. If this is the case, an organization must deploy a small Active Directory environment on the Enterprise Vault server to suit the needs of Enterprise Vault mailbox archiving and security.

Authentication across Domino environments, where mail files reside, and Active Directory, where the associated archives reside, is achieved through interaction between the users' mail server and the Enterprise Vault **Extension Manager** installed on the **Enterprise Vault Domino Gateway (EVDG)**. The EVDG is a Domino server that provides the security interface between the Domino security model and the Active Directory based security of Enterprise Vault data access control. All the major actions on archived data such as opening, restoring, deleting and searching, are handled by the EVDG when permitted by Enterprise Vault policy. As already mentioned, archiving of Domino documents leverages the IBM C API in the Lotus Notes client using NRPC. Both archiving and access functions can be installed on the same physical hardware. This means that Domino Server and Lotus Notes can co-exist on the same server (IBM/Symantec supported configuration).

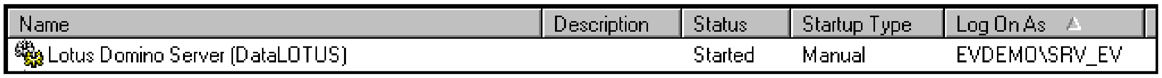
Seamless access to archived items from Lotus Notes or Domino Web Access (DWA) is provided using Enterprise Vault client extensions. The client extensions are installed using the Lotus Notes application, Symantec Enterprise Vault 8.0 - Domino Installer (**EVInstall.nsf**) which essentially enhances an organization's already deployed Lotus Notes and DWA mail templates. No additional applications or third party code needs to be installed on user workstations or production Domino mail servers. The updated mail templates are simply deployed to target Domino mail servers and DWA servers throughout an organization using EVInstall.nsf. The Enterprise Vault design templates need to be signed with the signing user ID that has all the required access within the workstation Execution Control List (ECL) on all Lotus Notes clients. The signing user also needs to be able to run agents on the Enterprise Vault Domino Gateway (EVDG) and Domino mail servers.

The following sections detail what permissions must be configured for user access and the client features to function properly.

Enterprise Vault Domino Gateway

As stated earlier, the Enterprise Vault Extension Manager provides the main functionality of the Enterprise Vault Domino Gateway. This is a Domino server side extension that processes requests from Lotus Notes and DWA clients before passing them onto Enterprise Vault. When the Extension Manager intercepts a user request, it gathers the user's credentials, the requested action and the targetted Enterprise Vault data, then determines if the user has the necessary authority to perform the request by communicating with Enterprise Vault. In order for the Extension Manager to have unrestricted access to Enterprise Vault data, the vailidity of the user request must be determined. Thus, the **Lotus Domino Server** service on the EVDG must run under the context of the Vault Service account as in Figure 3 to accomplish this.

Figure 3 – Domino Server service running on an EVDG



Name	Description	Status	Startup Type	Log On As ▲
Lotus Domino Server (DataLOTUS)		Started	Manual	EVDEMO\SRV_EV

Prior to installing the extension manager on the EVDG, changes must be made to the **server document of each EVDG**:

- The server document must have all target mail servers added as trusted servers so that the Enterprise Vault retrieval code can interact between databases on the target mail server (mail files) and the EVDG (temporary retrieval databases).
- The signing ID that will be used to sign the Enterprise Vault client templates needs to be given the permission "**Sign agents to run on behalf of the invoker of the agent**" to enable the Enterprise Vault retrieval code to run on the EVDG.
- The ID that will be used to run EVInstall.nsf requires the 'Create Master templates' right. This requirement is only a temporary need when running EVInstall so that Enterprise Vault can correctly configure the evdg_*.ntf customized templates on the EVDG.
- Single Sign-On must be configured for the Enterprise Vault search application to work and interact with its IIS based codebase without requiring constant re-authentication.
- Enterprise Vault requires the HTTP task to be configured on the EVDG as Enterprise Vault requires both IIS for the search application and Domino HTTP for retrieval. As IIS and the Domino server HTTP task both use port 80, it is suggested to change the port used by the Domino server to 8080.
- If deploying Vault Cache, users need the right to 'Create Databases' so that the agents can create the temp database on the EVDG to download items from.

Domino Server Targets

The following configuration changes must be made to the **server document** of each target Domino Server:

- The server document must have all EVDG's added as trusted servers so that the Enterprise Vault retrieval code can interact between databases on the target mail server (mail files) and the EVDG (temporary retrieval databases).
- The signing ID that will be used to sign the Enterprise Vault client templates needs to be given the permission "**Sign agents to run on behalf of the invoker of the agent**" to enable the Enterprise Vault retrieval code to run on the target Domino server.
- The ID that will be used to run EVInstall.nsf requires the 'Create Master templates' right. This requirement is only a temporary need when running EVInstall so that Enterprise Vault can correctly configure the ev_*.ntf customized templates on the target mail servers.
- Single Sign-On can be optionally enabled for DWA users.

EVinstall.nsf

The following ECL permissions are a one-time requirement when running EVInstall to allow it to run all the necessary code in the database to create the EV customized templates:

- Access to File System
- Access to Current Database
- Access to External Code
- Ability to Read Other Databases
- Ability to Modify Other Databases
- Ability to Export Data

These permissions are only required in the ECL of the Notes client that will run EVInstall. If organizations sign EVInstall with the SigningID before running it, then these rights will be present in the ECL by default. However, if EVInstall is signed by any other ID than the SigningID, organizations will most likely be prompted to trust the ID to allow the following when running EVInstall.

Client Workstation Security

The signing user ID or **SigningID** must be in the ECL of all workstations to enable the client side Enterprise Vault template updates to function without causing 'Trust Signer' prompts. It is recommended that a generic user account be created for the signing user ID. Alternatively, it can be the same ID as the archiving ID if the customer security model allows, or an existing generic user account that is used for signing in-house development and has the necessary ECL permissions.

The following ECL permissions are required rights for the SigningID in the ECL of every Enterprise Vault enabled user's notes client so that the customizations in the EV templates are allowed to run:

- Access to File System
- Access to Current Database (this must be permitted on the EVDG as well)
- Access to Environment Variables
- Ability to Read Other Databases
- Ability to Modify Other Databases
- Ability to Send Mail

The above rights could be deployed by the Administration ECL / Domino Directory Policy method to all users. Alternatively, organizations may use an already existing ID that already has these rights in the ECLs across their environment as the SigningID.

NSF Migration

If an organization is going to use the NSF Migrator, then Domino archiving user account requires the Access to current Database ECL permission so that users do not receive Execution Security Alerts when they use the Enterprise Vault client.

Enterprise Vault Search and SSO

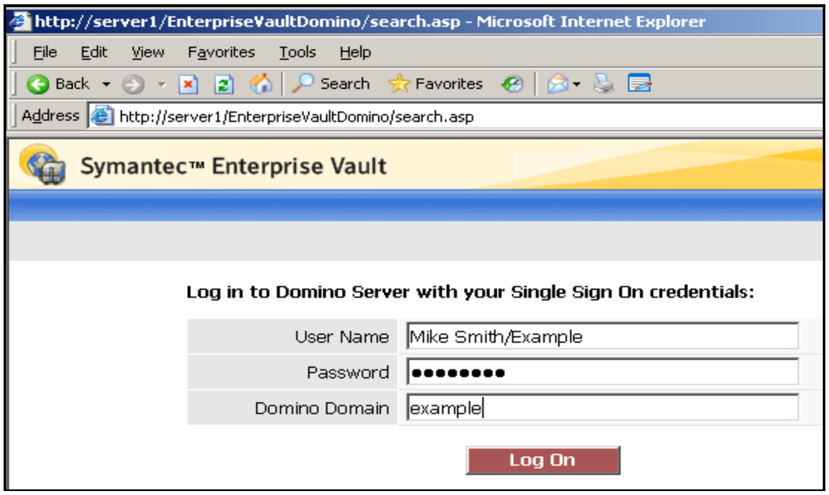
The Enterprise Vault search application differs from client and DWA requests by interacting with an IIS interface, using an LTPA token that is generated by using Domino Single Sign On.

Single Sign-On is required to be configured on the EVDG to enable users to use the Enterprise Vault search feature. It can optionally be configured on the target mail servers to use the same LTPA token to avoid DWA users needing to re-enter authentication details when accessing the search application and subsequently opening archived items from the search application.

Single Sign On can be configured at either the server document level or via Internet Sites. Refer to the Lotus Domino Administrator help and/or any existing processes organizations may have for their environment.

To launch the integrated search, the user selects the option, **Enterprise Vault Search**, within the Tools or More (depending on Notes version) menu in Lotus Notes or DWA. This displays the SSO login box. The user then enters their Lotus Notes user name (common name or full hierarchical name) and their Internet password. The Internet password is defined within the user's person document, and may or may not be the same as their Lotus Notes user ID password. The user must have an Internet password in order to login to the integrated search. Optionally, end users can access the Browser Search directly from an internet browser and browsing to http://<EV*server*>/EnterpriseVaultDomino/search.asp as shown in
Figure 4.

Figure 4 - Single Sign On



http://server1/EnterpriseVaultDomino/search.asp - Microsoft Internet Explorer
File
Edit
View
Favorites
Tools
Help
Back
Search
Favorites
Address
Symantec™ Enterprise Vault
Log On

Address: http://server1/EnterpriseVaultDomino/search.asp

Log in to Domino Server with your Single Sign On credentials:

User Name	Mike Smith/Example
Password	●●●●●●●●
Domino Domain	example

When users attempt to search an archive, an Enterprise Vault agent in EV\evdomino.nsf on the EVDG intercepts the request, the user details, and the LTPA token, and interacts with the **EnterpriseVaultDomino** virtual directory on the EVDG. This is used to authenticate the user's access to Enterprise Vault. The virtual directory points to a WebApp folder (typically C:\Program Files\Enterprise Vault\webapp) which has anonymous access enabled but will only accept requests from the Domino Web Application account. For security, a Domino Web Application account is required for this virtual directory. It is recommended to create an account specifically for the purpose of this. A basic Windows domain account should be used. Do not use a local machine account.

The Domino Web Application account requires the following rights:

- Access this computer from the network (SeNetworkLogonRight)
- Bypass traverse checking (SeChangeNotifyPrivilege)
- Log on as a batch job (SeBatchLogonRight)
- Allow log on locally (SeInteractiveLogonRight)

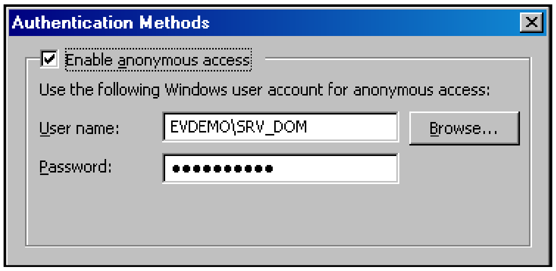
These rights are configured automatically when configuring the Domino Web Application account on the Directory properties in the Vault Administration console. Additionally, the following registry value is also created during configuration:

- HKEY_CURRENT_USER\Software\KVS\Enterprise Vault\AnonymousUser

HKEY_CURRENT_USER is that of the Vault Service account. The value of this setting is the full name, including the Windows domain, of the Domino Web Application account, for example, EVDEMO\SRV_DOM.

The AnonymousUser registry setting ensures that only the Domino Web Application account can access Enterprise Vault and obtain a list of archives accessible by the Domino User passed to it during the Enterprise Vault search application authentication and retrieve only relevant search results and data for this user.
Figure 5 shows what the EnterpriseVaultDomino virtual directory will be set to.

Figure 5 – Properties of the EnterpriseVaultDomino virtual directory



Authentication Methods

☑ Enable anonymous access

Use the following Windows user account for anonymous access:

User name: EVDEMO\SRV_DOM

Password: ●●●●●●●●●●●

Domino Mailbox Archiving Task

In order for the Domino Provisioning and Mailbox Archiving tasks to function correctly, they need access to user mail databases. This provides the tasks the ability to:

- Add hidden views
- Add or update the hidden Enterprise Vault profile document
- Change mail items into shortcuts

To allow this while complying with the Domino security model, access to the Domino mail databases needs to be done by an authenticated user using a Lotus Notes ID file. The archiving, journaling, and provisioning tasks will run under the context of this **archiving ID**. The archiving ID can be specified in the Vault Administration console on the target Domain as well as the Server properties. A single archiving ID file can be used for all access levels. Alternatively, a different ID file for each level can be used.

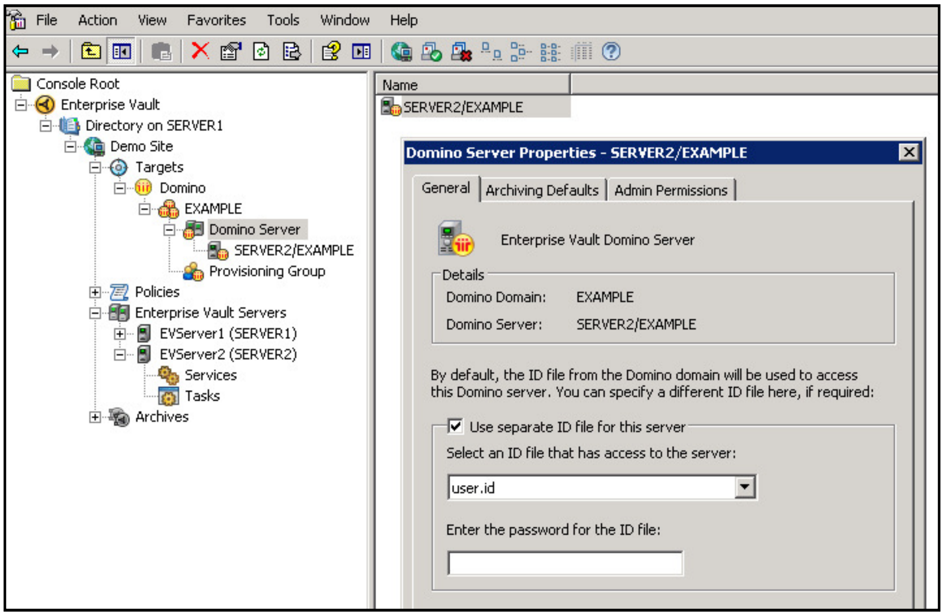
The access levels are as follows:

- **Domino Domain** – This ID must have the following permissions:
  - Read access to the Domino Directory.
  - At least Depositor access on the mail files (to allow the required “Read public documents” permission).

- **Domino Server** – This ID must have read access to the Domino Directory on the server.

Unless specified, Enterprise Vault will use the same ID file that is used to access the domain to access the Domino servers within the domain as shown in Figure 6. The ID details, including the password, are encrypted and stored in the Enterprise Vault directory database.

Figure 6 - Archiving ID at Domino Server Level



Domino Server Properties - SERVER2/EXAMPLE

Enterprise Vault Domino Server

Details

Domino Domain: EXAMPLE

Domino Server: SERVER2/EXAMPLE

By default, the ID file from the Domino domain will be used to access this Domino server. You can specify a different ID file here, if required:

☑ Use separate ID file for this server

Select an ID file that has access to the server:

user.id

Enter the password for the ID file:

The archiving ID that will be used at the server level will also require **Editor** access, with the **Delete Documents** and **Create Shared Folders/Views** attributes. Organizations that do not want *unread* items archived must grant the ID **Manager** access so it can determine the read status of a message.

If Domino administrators have Manager access to all mail files, then the Manage ACL tool in the Domino Administrator client can be used to add the archiving ID to all mail databases. It is very important to set the archiving ID's User Type to Person to prevent any user from creating a group within the Domino directory of the same name as the Domino archiving user and granting the group access to all mail databases. Equally the selected archiving ID can be granted the required access by being added to an existing access group that is already established in the environment with the required access to all mail files. Although any user ID file that has the correct level of access can be used, it is recommended that a generic user account be created with the correct access permissions specified above. Alternatively, an existing generic user account that has the required access to all mail files can also be used. It is ultimately up to the organization to use sound judgment when determining which ID file to use. If required, a separate archiving ID can be configured for each Domino Mail target.

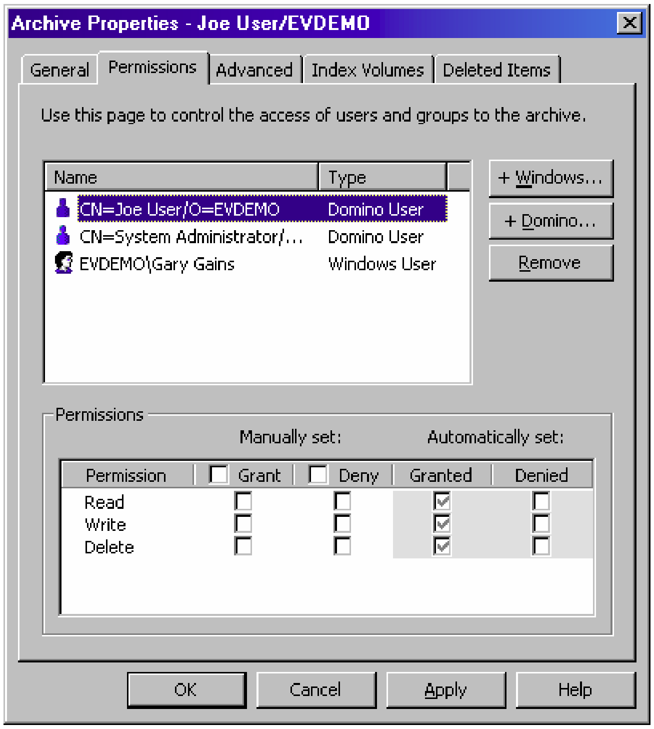
The Lotus Notes client installation on the Enterprise Vault server archiving a Domino Server needs to be manually configured to use the archiving ID. This is because the Domino Provisioning and Archiving tasks leverage the client's IBM C API using Notes RPC (NRPC) to interact with the Domino environment. It must also be installed in single user mode.

Controlling Access to user archives

Enterprise Vault will always automatically grant a mail file owner Full Control access to their archives. Figure 7 below, shows how to manually edit additional archive permissions for a Domino mailbox archive. By clicking the **+ Windows** or **+ Domino** button, a dialog box opens. Clicking **+ Domino** will read the accounts listed in the Domino Directory (See Figure 8). From here, accounts can be added to the permissions list of the archive.

Windows Active Directory accounts can also be added to a Domino archive's permissions list. By clicking **+ Windows**, EV will read the accounts available in Active Directory.

Figure 7 - User archive security box



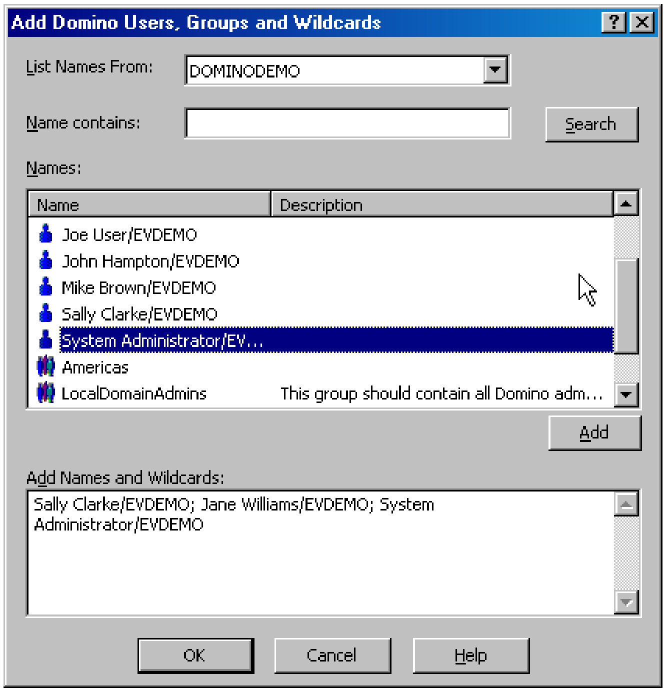
Use this page to control the access of users and groups to the archive.

Name	Type
CN=Joe User/O=EVDEMO	Domino User
CN=System Administrator/...	Domino User
EVDEMO\Gary Gains	Windows User

Permissions

	Manually set:		Automatically set:	
Permission	□ Grant	□ Deny	Granted	Denied
Read	□	□	☑	□
Write	□	□	☑	□
Delete	□	□	☑	□

Figure 8 - Adding Domino accounts (+ Domino)



Add Domino Users, Groups and Wildcards

List Names From: DOMINODEMO

Name contains:

Names:

Name	Description
Joe User/EVDEMO	
John Hampton/EVDEMO	
Mike Brown/EVDEMO	
Sally Clarke/EVDEMO	
System Administrator/EV...	
Americas	
LocalDomainAdmins	This group should contain all Domino adm...

Add Names and Wildcards:

Sally Clarke/EVDEMO; Jane Williams/EVDEMO; System Administrator/EVDEMO

Enterprise Vault fully supports and honors permissions and delegate access granted to users that are not the owners of the mail file. Users that have **Editor**, **Designer**, or **Manager** access to a mail file will have Full Control to the user's archive which includes the ability to **read** and **delete** items. Users that have **Reader** or **Author** access to a mail file will have the ability to **search** the archive. Users that have **No Access** or **Depositor** access to the mail file will have **no access** to the mail file's associated archive. Enterprise Vault keeps Domino permissions synchronized with the archives twice daily. The time and frequency with which Enterprise Vault keep these synchronized can be configured in the properties of the Domino Provisioning task. Additionally, if new permissions or delegates are added to a mail file, administrators can optionally immediately synchronize the permissions. This is done within the properties of the Domino Provisioning task.

Securing the local Vault Cache

One of the benefits of the Enterprise Vault client extensions is the use of **Vault Cache**. Vault Cache resides on the local user's PC or laptop which allows for access to archived items when not connected to the network, as well as a network bandwidth optimization benefit.

The security of the Vault Cache itself is typically left to the devices of the host operating system such as encryption methods and file security. Client workstations must be configured to **Enable Local Security Agents** in the user's client user preferences in order for Vault Cache to work correctly.

Conclusion

In this whitepaper we have discussed the security aspects of archiving and retrieving from Lotus Domino with Enterprise Vault 8.0. We have discussed how Enterprise Vault can securely archive mailboxes and Journal databases and provide secure access for Lotus Notes and DWA users. We have also detailed how we can securely bridge the Domino Security model with Active Directory using an Enterprise Vault Domino Gateway.

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

- Security Model for Discovery Accelerator 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 SMTP Archiving
- Enterprise Vault 8.0 Security Model for Microsoft SharePoint Archiving
- Enterprise Vault 8.0 Security Model for Microsoft Exchange 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