Symantec Enterprise Vault™ Whitepaper – Deploying IMAP Access to Enterprise Vault

Who should read this paper

This Whitepaper is intended to assist customers, partners and service providers deploy IMAP access to Enterprise Vault.

If you have any feedback or questions about this document please email them to **iig-tfe@symantec.com** stating the document title.

This document applies to the following version(s) of Enterprise Vault:

11.0.1 CHF1 and later

Confidence in a connected world. Symantec

Table of Contents

Document Control

Contributors

Who	Contribution
Dan Strydom	Author

Revision History

Version	Date	Changes
0.1	October 2013	Draft
1.0	May 2014	Published
2.0	March 2015	Updated for 11.0.1 CHF1, Improved Scalability

Related Documents

Document Title	Document Location	Version
Requesting and Applying an SSL Certificate	www.symantec.com/docs/HOWTO83452	10.0.3
Setting up IMAP.pdf	Product Media, Documentation folder	11.0.1
SQL Best Practice Guide for EV 11	www.symantec.com/docs/DOC6863	11.0.1

Scope of Document

This document provides information, options and best practice guidelines on how to deploy IMAP access to Enterprise Vault archives. This document should be used in conjunction with other performance and best practice guides as outlined in the "Related Documents" section of this document.

Terminology Used In This Document

Term	Description
EV	Enterprise Vault
IMAP	Internet Message Access Protocol
SMTP	Simple Mail Transfer Protocol
IMAP Server	IMAP v4 standards compliant server used to access archives
Fast Browsing	A new technology to allow very fast listing of items within a folder
IMAP End Point	Server or DNS alias to be used by users when configuring their mail account
Internet Mail Archives	Archive type used for non-Exchange archives enabled for IMAP access
IMAP Provisioning	Ability for an admin to choose who to enable for IMAP access
User Account	Combination of AD logon account and IMAP Archive ID
IMAP Archive ID	Unique ID given to identify an archive
MDM	Mobile Device Management

Introduction

Today's information workers expect to be productive with all of their devices; desktop, laptop or mobile. To help users manage their email archives with the most intuitive client possible Enterprise Vault 11 introduces IMAP access to email archives.

Internet Message Access Protocol (IMAP) is a widely used Internet protocol that enables end users to access email messages stored on a remote server. Enterprise Vault 11 introduces a new server feature, the Enterprise Vault IMAP Server which enables any IMAP v4 standards compatible client to access the archived email stored on the Enterprise Vault server.

With this feature enabled end users are able to:

- Connect to an archive as though it's a mailbox
- Browse their archived email messages
- Access, view, forward, reply any archived message or attachment
- Manage archived items by flagging, moving, copying or deleting
- Manage the folder structure within their archive (create, delete and rename folders)
- Archive new items (manually or automatically using client-side rules)
- Search their archived items downloaded onto the device or client, or alternative search on the Enterprise Vault server (if the client supports searching on an IMAP server).

IMAP Access Architecture Overview

Any existing Enterprise Vault server can be enabled for IMAP Access. The IMAP clients are configured to connect to the IMAP service via a DNS alias, known as the IMAP End-point. A single IMAP End-point can be used to distribute the load to multiple IMAP enabled EV servers. DNS round robin or hardware/software load (such as Microsoft NLB) can be used to distribute the IMAP client connections between servers.

As depicted in Figure 1 an Enterprise Vault server enabled for IMAP can serve clients locally on the internal network, or devices outside of the corporate network such as Smartphones and Tablets.

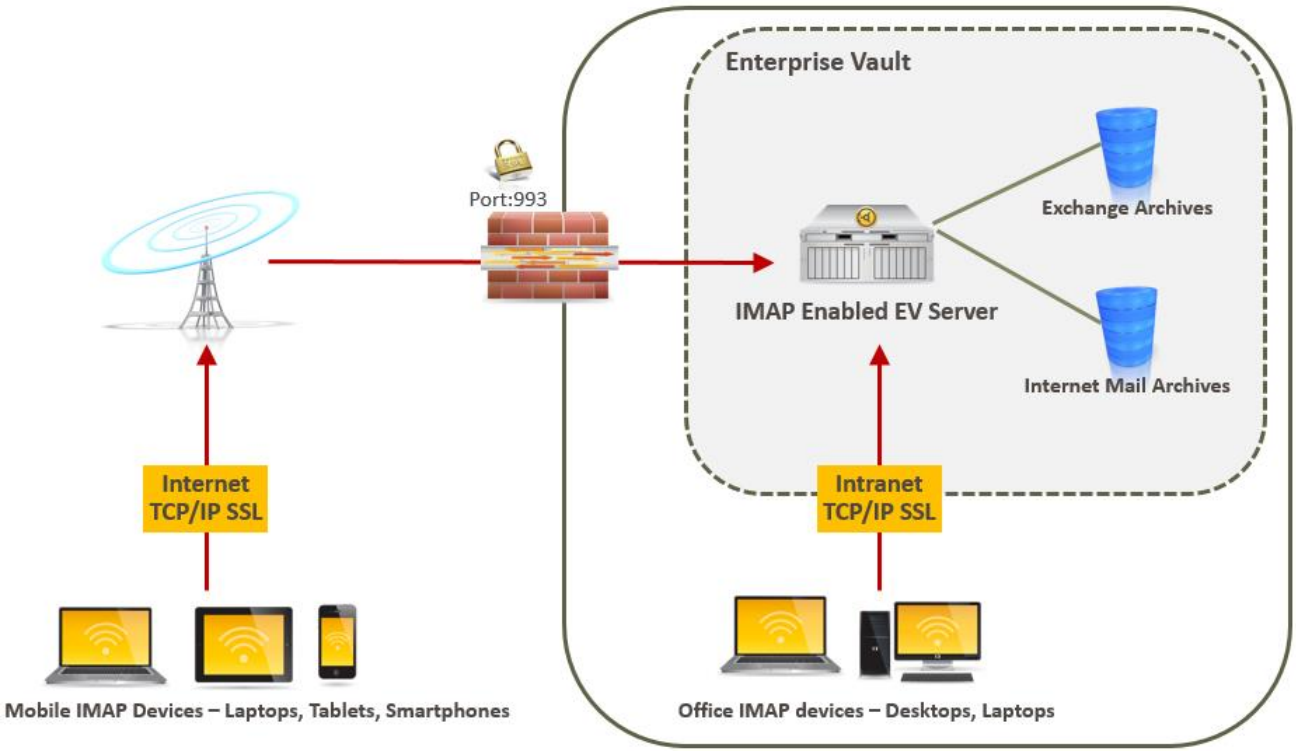


Figure 1 – IMAP Access Architecture Overview

Architecture and Sizing Considerations

Depending on the load on your existing Enterprise Vault servers it may be required to add one or more dedicated Enterprise Vault IMAP servers, specifically to host IMAP Access. For best performance however it is recommended to co-locate the IMAP service with each Storage service for which archives will be enabled for IMAP access.

The performance of the IMAP service depends on a number of factors, including:

- EV Server specifications
- Performance of Vault Store storage device & options such as collections
- Network bandwidth and latency
- Number of concurrent end-users
- Archived data characteristics (size, type)
- Client applications in use
- Other Enterprise Vault loads placed on the server, such as archiving and eDiscovery.

Note that the IMAP service is not designed for PST or mass upload of data to be archived.

Deployment Recommendations

Existing feature deployment such as Virtual Vault clients do not need to be replaced and the impacts of changing should be carefully considered; all data would need to be re-downloaded and Virtual Vault provides additional functionality over IMAP Access.

When sizing for IMAP Access consider that not all IMAP clients will have the same usage profile. For example a mobile device is likely to place less load on the server as it will have stricter download limits, compared to a desktop client. A mobile device is also more likely to connect regularly on a 24hr schedule, compared to a typical workstation only used during working hours.

Due to the different content download and connection profile of mobile devices and computers, there are differences in the deployment and sizing recommendations for each, as detailed in Table 1.

Deployment recommendation	Mobile devices	Desktop/Laptop clients	Mixture of Desktop/Laptop clients and Mobile devices
Maximum number of clients supported per EV Storage Server	4,000	3,000	4,000
Maximum number of new clients enabled per EV storage server per day	1,000	250	250 Desktops/Laptops 700 Mobile devices

Table 1 – Deployment recommendations

Note: Further deployment and tuning advice is targeted for a future publication.

Metadata Store Considerations

Before an archive can be enabled for IMAP Access, the user's archive must have a Metadata Store (MDS) cache enabled. Metadata Store is the new technology in Enterprise Vault 11 that adds information to the Vault Store database that in turn speeds up folder and item listing. This technology is also known as Fast Browsing, and is required for IMAP Access. Archives created on Enterprise Vault 11 will already be enabled for MDS by default, and archives created on earlier versions can have the MDS cache built as needed.

When provisioning a user for IMAP Access, the Client Access Provisioning task will check first if the archive is MDS enabled. If the archive is not MDS-enabled, the task will create an indexing subtask to build the MDS cache the next time the Index Administration task runs.

It is recommended that MDS is only enabled for archives that require IMAP, or for archives that use the Enterprise Vault Search feature.

Typically the MDS cache will only take a short while to build, depending on the schedule of the Client Access Provision task and Index Administration task. MDS information can be added at ~2.5million items per hour.

By enabling MDS the Vault Store databases will grow. As mentioned earlier in this section it is only recommended that Fast Browsing is enabled for active archives that require IMAP or Enterprise Vault search. For the purpose of sizing the additional storage required for the database, if all archives were to be enabled within an Exchange Mailbox Vault Store, it is expected that the database size can grow up to 100% in size, depending on the type and size of items archived.

For more information please refer to the Enterprise Vault performance guide and SQL Best Practice Guide for Enterprise Vault 11 (available at **www.symantec.com/docs/DOC6863**).

Deployment Scenarios

The single biggest benefit of this feature is that end users are able to access their archived email from a wide range of devices and clients, without the need to install an application or client extension. The vast majority of email clients support IMAP access, including most smartphones and tablet devices available on the market today.

The IMAP access feature can be made available to clients on the internal network (such as Apple OS X workstations using the Mail client) or the service can be extended to mobile clients (such as Apple iOS devices using native Mail app) outside of the corporate network, using 3G or other wireless networks. For mobile device access Symantec recommends deployment using a Mobile Device Management (MDM) product.

Users are enabled for IMAP using the new IMAP provisioning functionality built into the Vault Admin Console. It is possible to enable any Enterprise Vault Exchange mailbox archive or create a new Internet Mail archive. Internet Mail archives allow users to archive messages from any (Cloud or non-Exchange) email provider by moving mail items into the archive using drag-and-drop or client rules.

Deploying IMAP access to internal users

In this scenario internal users are given the ability to access their Enterprise Vault Exchange or Internet Mail archive from any compatible IMAP email client. There is no need to deploy any software to clients – users are natively presented with a folder list view and feature rich interface to their archive that compares to a mailbox.

Figure 2 shows a screenshot of a Mac user accessing their archive through Microsoft Outlook for Mac.

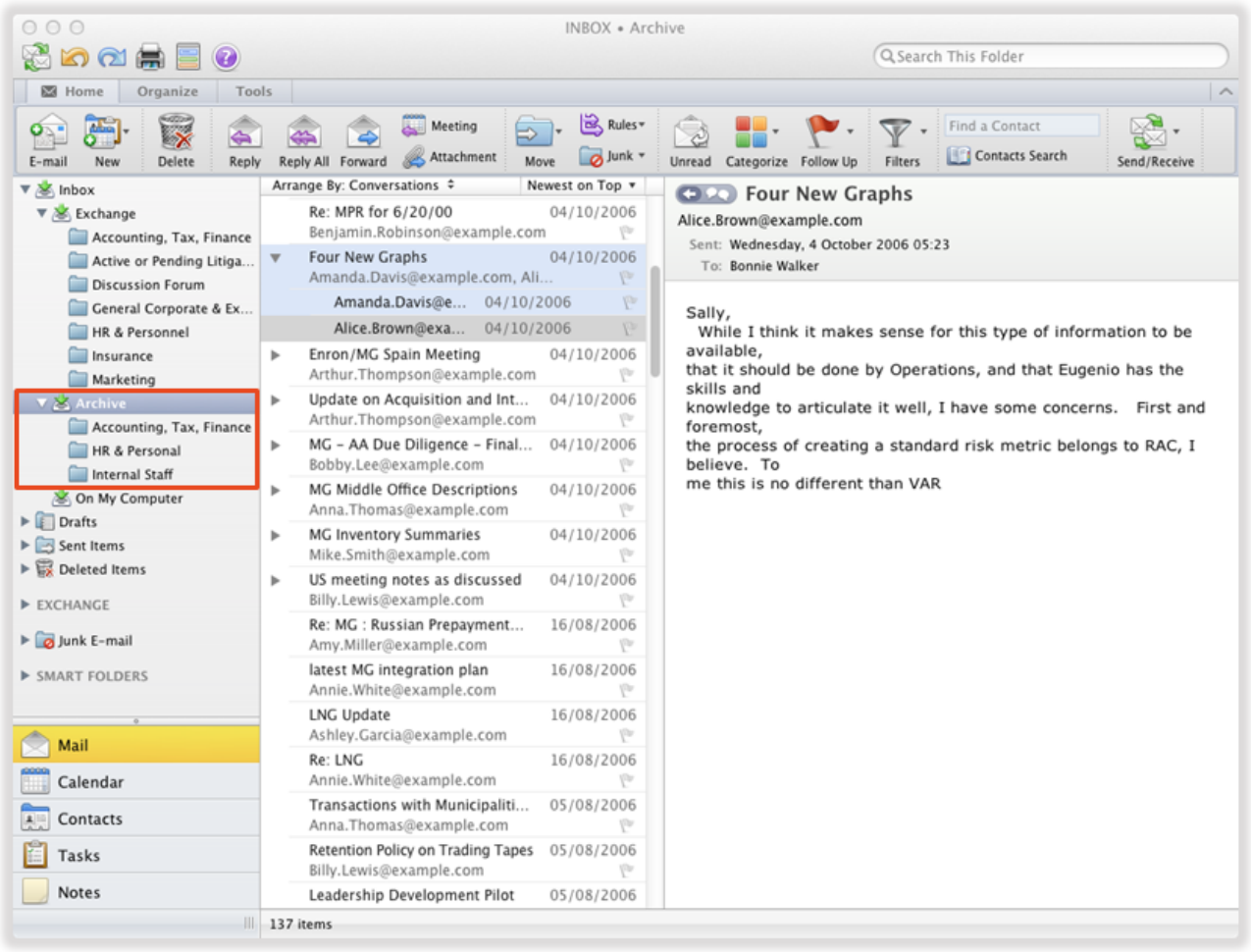


Figure 2 – Screenshot of a Microsoft Outlook for Mac user accessing their archive

In this scenario the IMAP Server has been enabled on the Enterprise Vault server, and end users connect directly to the Enterprise Vault server on the internal network. To reply to archived email, the email client can either be configured to

a) Use another profile already set up on the email client (such as an existing profile set up to send and receive email through their mailbox); or

b) Authenticate and send email via the existing internal Exchange (or any other messaging platform) SMTP Receive connector.

Note: Throughout this whitepaper the standard secure IMAP (993) and SMTP (587) ports are referenced.

Figure 3 shows a client configured to send SMTP email via the Exchange SMTP connector.

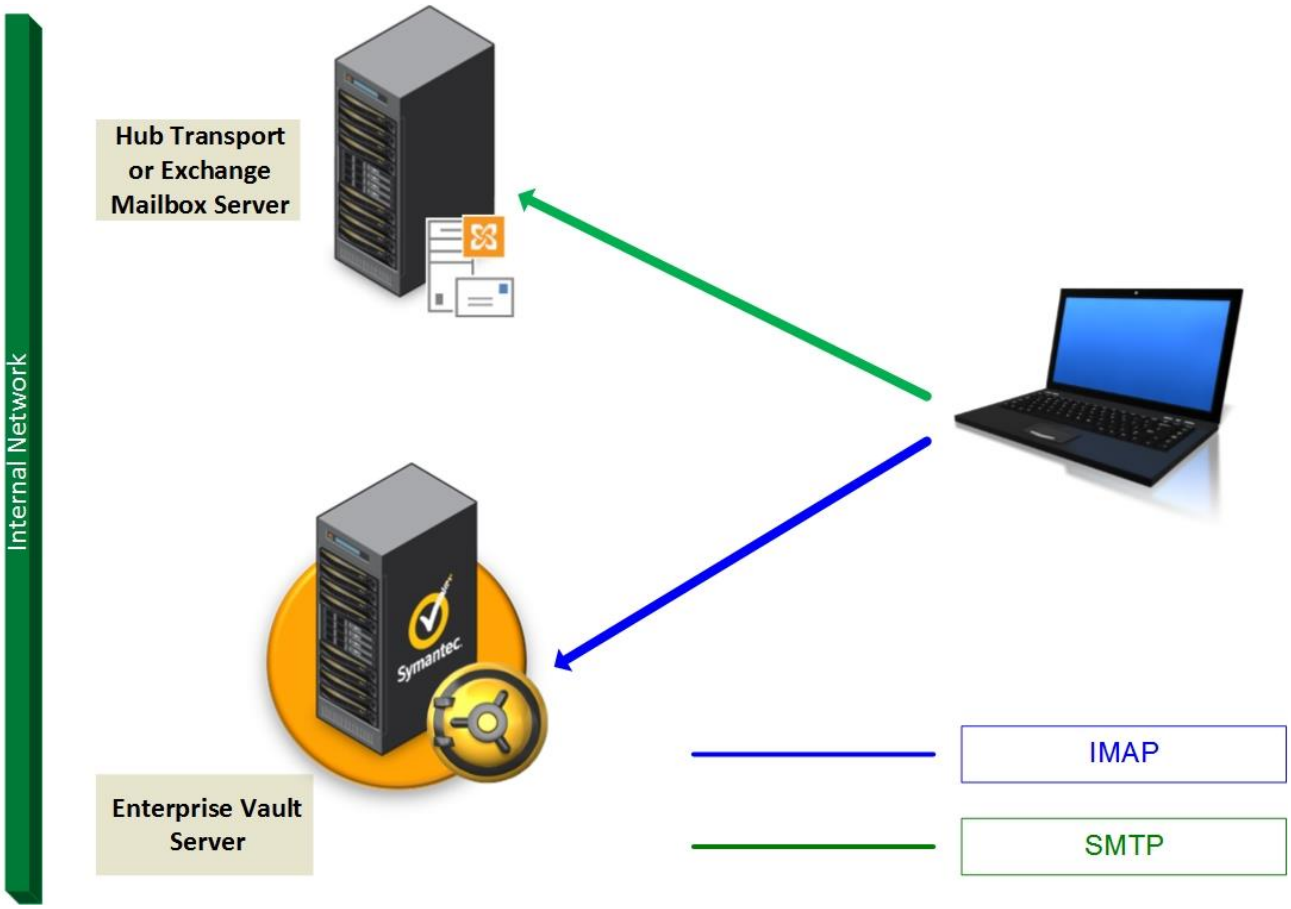


Figure 3 – Internal email client protocol overview

When setting up an email client (whether it be a mobile device or desktop application) it is normally necessary to supply both IMAP and SMTP server details for the configuration steps to complete.

When creating an IMAP account on the client the following details are required:

Term	Description
Description	A simple name the account will be referenced by, “Archive” is a good suggestion
Full Name	The Users name to be used on any sent emails
E-mail address	The email address to be populated on any sent emails
User Name	The User Account of the IMAP enabled archive. The user account is the combination of the users AD logon and the IMAP Archive ID of the archive to be accessed. Such as mydomain\myuser\7175665
Incoming Server	The Enterprise Vault IMAP Server(s) End Point(s)
Outgoing Server	The SMTP server (if required)

Figure 3 shows a typical client configuration for IMAP.

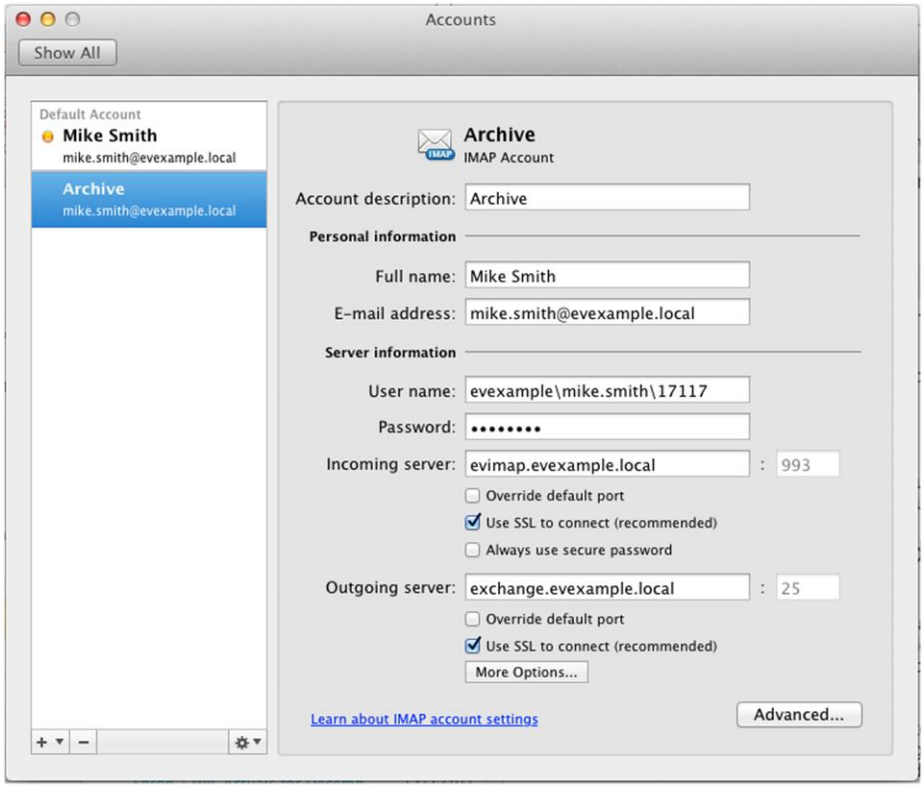


Figure 4 – Typical client configuration

If users do not require the SMTP functionality to reply to, or forward archived email it is possible to supply false SMTP details such as the IMAP Server details, in order for the new mail profile wizard to complete.

Note: Depending on the email client it may also be required to untick the "Test this configuration" setting to allow the account wizard to complete.

End users can choose to use the existing email profile such as the user's Microsoft Exchange Server profile to send mail, and using this profile as the default send account the user will therefore be able to reply to or forward archived email.

Configure Internal IMAP access

To configure IMAP access for internal users the following steps will be required:

1. Configure a CNAME DNS alias to point to any or all Enterprise Vault servers with IMAP enabled, for example evimap.evexample.local.
2. Obtain an SSL certificate[1] with the End Point alias in the subject or alternate subject. Authentication on unsecured IMAP will result in a clear text password being sent over the network. Symantec does

[1] The alias that clients will use needs to be on the certificate as the subject name or alternate subject name to avoid certificate warning messages on the device

not recommend enabling an unsecured IMAP Server as it is possible for packet analyzers to read clear text passwords. An internal Certificate Authority can be used, providing the certificate is deployed to the end user devices (otherwise the device will prompt that the certificate is not trusted). For additional information on creating certificates visit **http://www.symantec.com/business/support/index?page=content&id=HOWTO83452.**

3. If using a segmented network, ensure that internal clients have access to the Enterprise Vault server on the chosen port (the standard port for IMAP access over SSL is port 993).
4. Configure the Enterprise Vault IMAP Server[2].
5. Provision archives for access.

Configure Internal SMTP access

Generally speaking organizations do not allow internal clients to relay email though SMTP connectors without any form or authentication, or at minimum only very specific internal services are allowed to relay. As already mentioned in this document most email clients include the ability to select an alternative account to send email.

For customers that prefer to allow end users to send email directly using an internal SMTP server, the following configuration is typically required:

- Either modify the existing Exchange Receive Connector, or create a new Receive Connector[3] specifically for the purpose of allowing internal (authenticated) clients to relay email
- Ensure that the connector clients will use is configured to use authentication. Note that if choosing Basic Authentication, the username and password will be sent using plain text, and is therefore vulnerable to packet sniffers or analyzers. It is recommended that TLS is used, for which an SSL certificate will be required. Microsoft Technet provides extensive information on configuring SMTP connectors[4] for authentication.

Organizations that require all end user email to be captured using Exchange Journaling should consider whether their Journal configuration will allow end user relay email to be captured.

---

[2] The references document "Setting up IMAP.pdf" in the product media "Documentation" folder lists the detailed steps required to configure the Enterprise Vault Server and provision the archives for IMAP access.

[3] **http://technet.microsoft.com/en-us/library/bb125159(v=exchg.141).aspx**

[4] **http://technet.microsoft.com/en-us/library/bb690954(v=exchg.141).aspx**

Deploying IMAP access to clients on the Internet via VPN

Similar to the above scenario, end users can be given the same level of functionality when outside of the corporate network through the use of a VPN client. Desktop (i.e. typical remote laptops) use of VPN for remote network connection is in wide spread use, and the use of mobile VPN clients on smartphones or tablets are becoming more popular. If your organization currently use a VPN client for laptops, this method of network/service connection may well be the most secure and simplest way to configure for mobile access to IMAP.

The VPN connection will need to be configured to allow IMAP access on the chosen port (e.g. 993), and optionally secure SMTP submission on the chosen port (the standard port for secure SMTP submission is port 587).

Figure 4 shows how a VPN can be used from a mobile device or laptop to connect to the IMAP server.

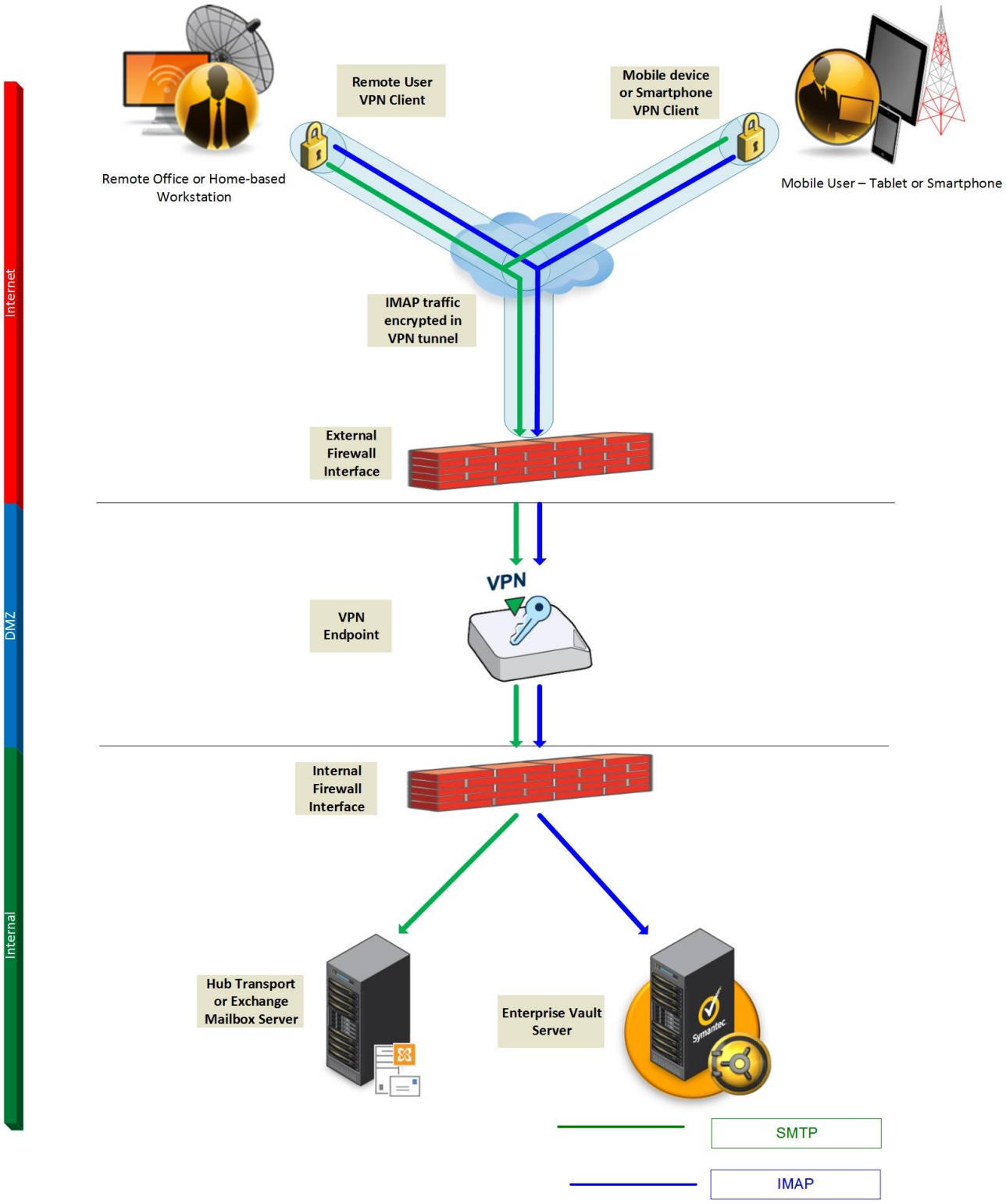


Figure 5 – Remote IMAP access using a VPN client

Deploying IMAP access to clients on the Internet

As with any application or website published externally there many security aspects that should be considered before making resources available on the Internet. Many organisations have dedicated security personel that will be familiar with the security measures deployed to protect the company's resources from unauthorised access, and it is recommended that these personel are engaged to provide the recommended means of deploying IMAP, and optionally SMTP access from the Internet.

The benefit of deploying IMAP to end users is that they can have access to archived items from any Internet enabled device with a compatible IMAP client. Figure 6 shows a screenshot of a user accessing their archive from an Apple iPad as an example.

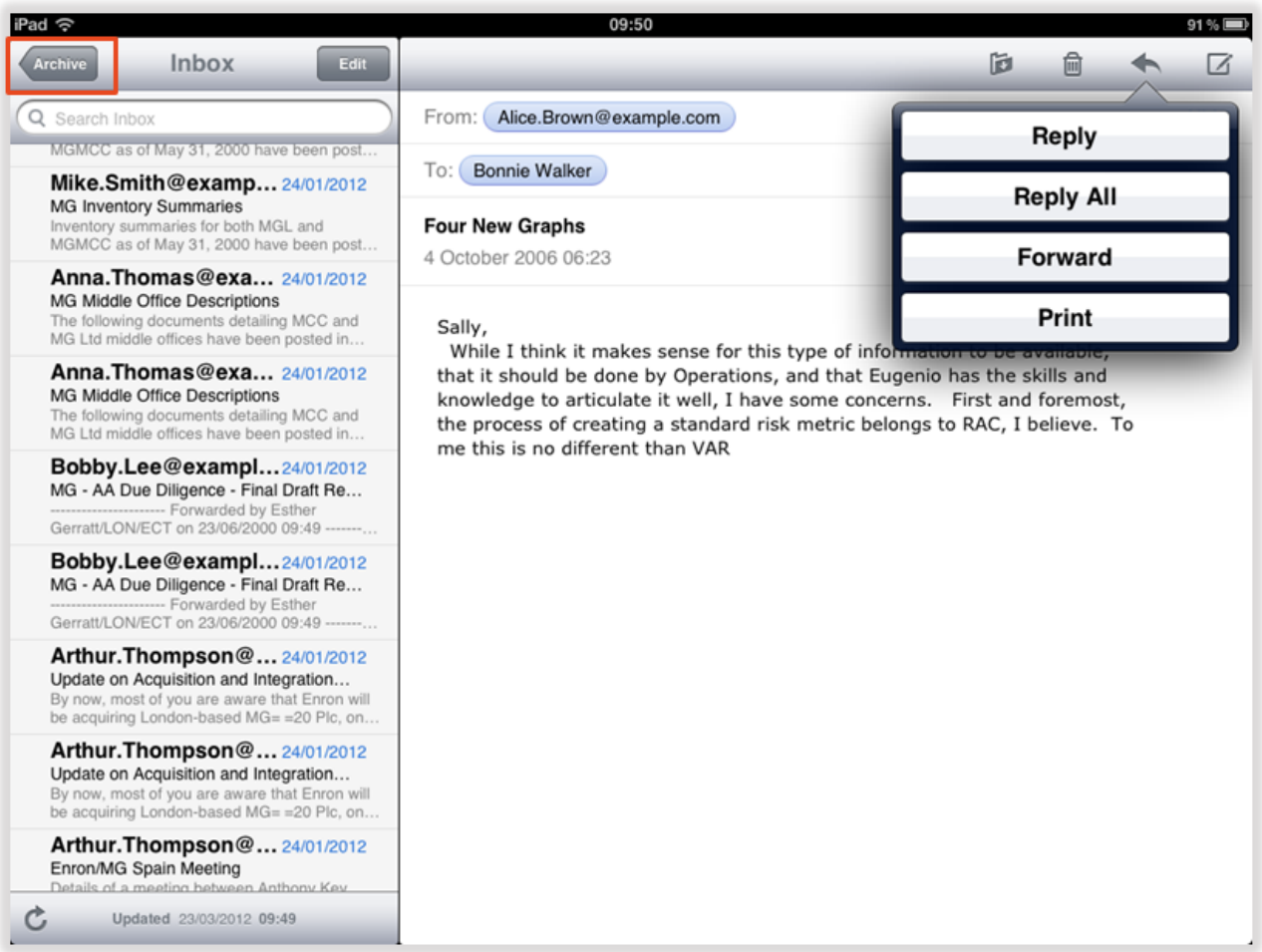


Figure 6 – Apple iPad access to the user's archive, using the native Mail app

Figure 7 shows an overview of a typical configuration required to allow IMAP access from any external client to the Enterprise Vault server.

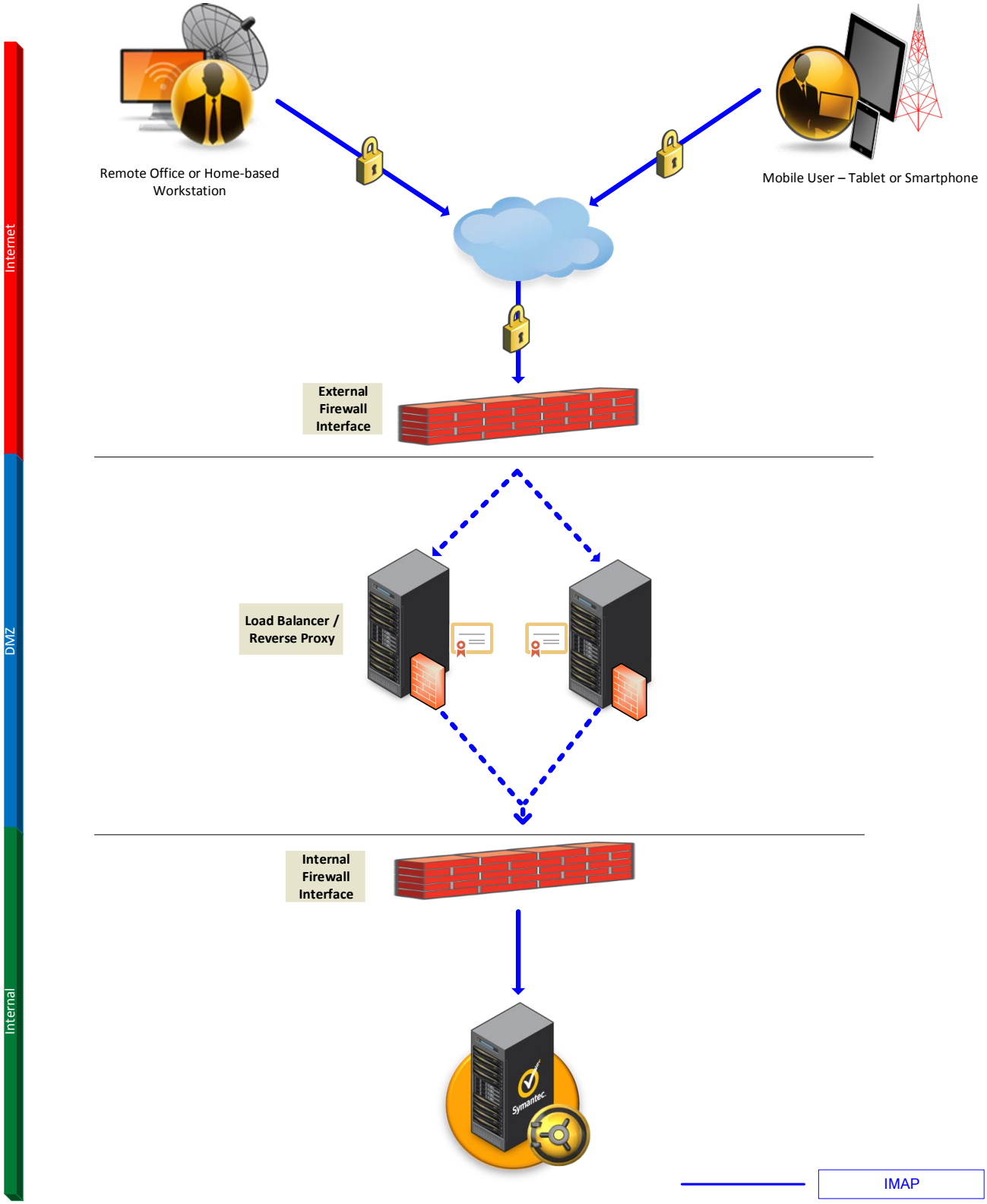


Figure 7 – Example IMAP configuration for External/Internet clients

In the example used in Figure 7 clients on the Internet use secure IMAP, and the external facing firewall is configured to permit IMAP access on port 993. The firewall then passes the connection to the cluster address

of the reverse proxy device (for example Microsoft TMG or UAG server). The reverse proxy server is configured with a listener rule to accept secure IMAP traffic on the particular domain name (myarchiveimap.mycompany.com) and performs additional security checks to ensure the traffic is not malicious.

The traffic passes through the internal firewall interface before being directed to the Enterprise Vault server, where the user credentials are authenticated against Active Directory before access is granted to the archive.

Configuring IMAP access to External/Internet clients

To configure IMAP access for external users as described above the following configuration will be required:

1. Create an external Internet DNS A record to point to the external firewall interface, for example archiveaccess.mycompany.com.
2. Obtain an SSL certificate with the End Point alias in the subject or alternate subject.
3. Configure the external firewall interface to allow port 993, and route the traffic to the reverse proxy server.
4. Create a new listener on the reverse proxy server, and publish a rule to accept secure IMAP traffic for your domain name. Traffic will be passed to the Enterprise Vault server running the IMAP service on the internal network.
5. Configure the Enterprise Vault IMAP Server (as described in the “Setting up IMAP.pdf” referenced document.
6. Provision archives for access.

Configure SMTP relay for External/Internet clients

The configuration required to allow clients on the Internet to relay email is only necessary if end users require the functionality to directly reply to or forward archived email – as discussed earlier in this document it is possible to use an existing account on the email client to send email.

Careful planning and consideration is required to allow clients to relay email directly from the Internet, and the authentication of clients is absolutely essential to prevent an SMTP connector from being abused as an open relay.

Configuration will vary widely depending on how the SMTP environment is set up, but typically in a Microsoft Exchange environment the only way users can be authenticated by the SMTP receive connector is if the server is part of the Active Directory domain. Edge Transport servers located in a DMZ are typically not part of the domain, and Microsoft do not provide the “Client” connector usage type functionality for Edge Transport servers. An Exchange Hub Transport or Mailbox server is the only Exchange server suitable for authenticating and providing relay services to users (alternatively other on-site or cloud-based SMTP services can be used, providing they can authenticate the credentials supplied in the user’s SMTP profile).

As this configuration will effectively expose the server to the Internet it is therefore recommended that a dedicated server is used for this purpose (as opposed to exposing an existing production Exchange Hub Transport server).

Any unnecessary services on this server should be disabled, and the operating system should be locked down in addition to anti-virus protection installed on the server.

It also makes sense from a security perspective to separate general everyday SMTP traffic coming in on port 25 from the secure and authenticated relay traffic, and therefore it is recommended that a unique record is set up for this purpose – for example archivesmtp.mycompany.com.

The new connector you create on the Hub Transport server should be configured to listen only on port 587. The most common authentication type suitable for this scenario is “Basic Authentication Requiring TLS” as this is supported by the majority of email clients.

Figure 8 shows a suitable Receive Connector configuration capable of authenticating users in a secure fashion.

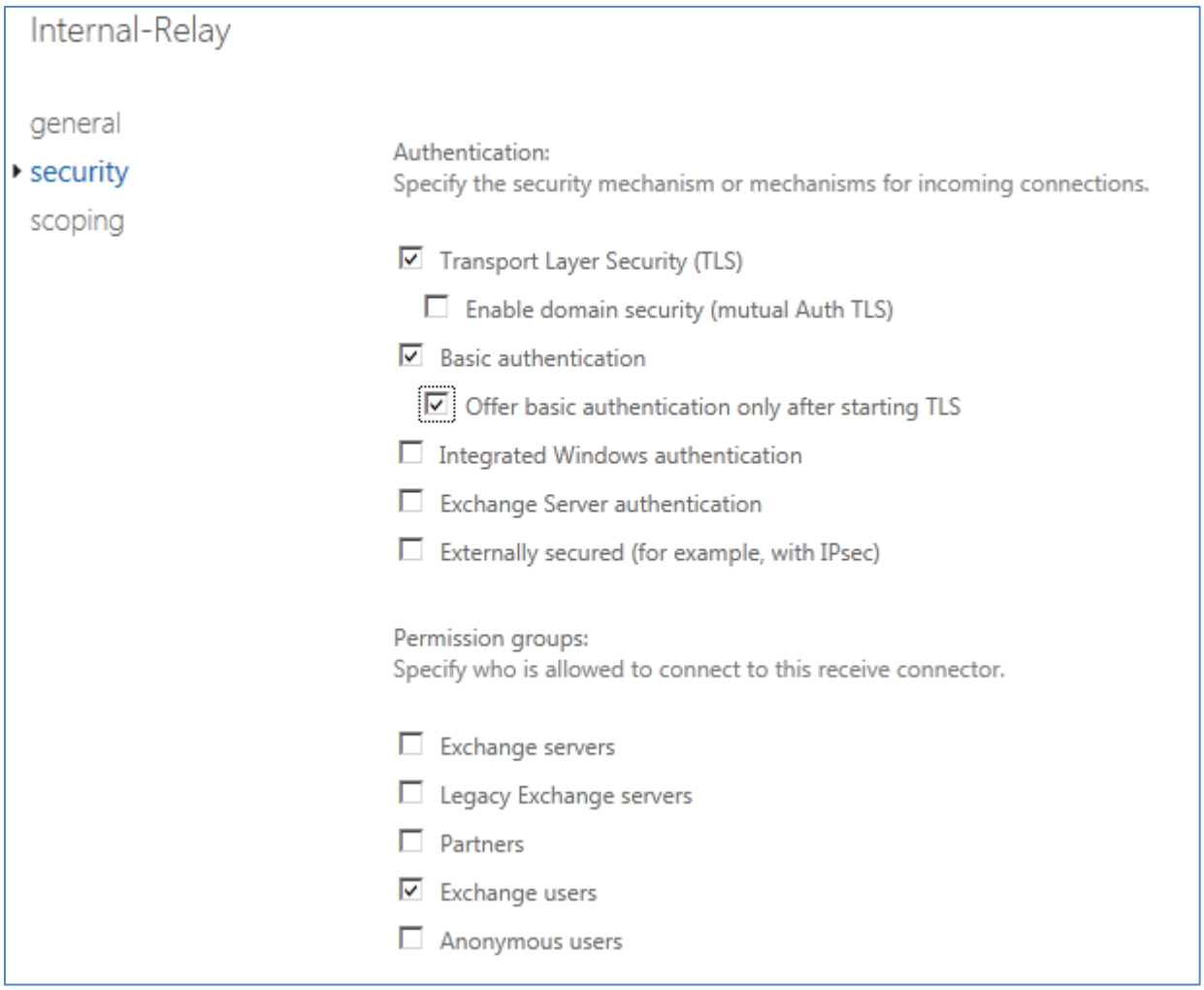


Figure 8 – Exchange 2013 Receive Connector properties

Figure 9 shows the configuration described above, with clients authenticating against a dedicated Hub Transport server.

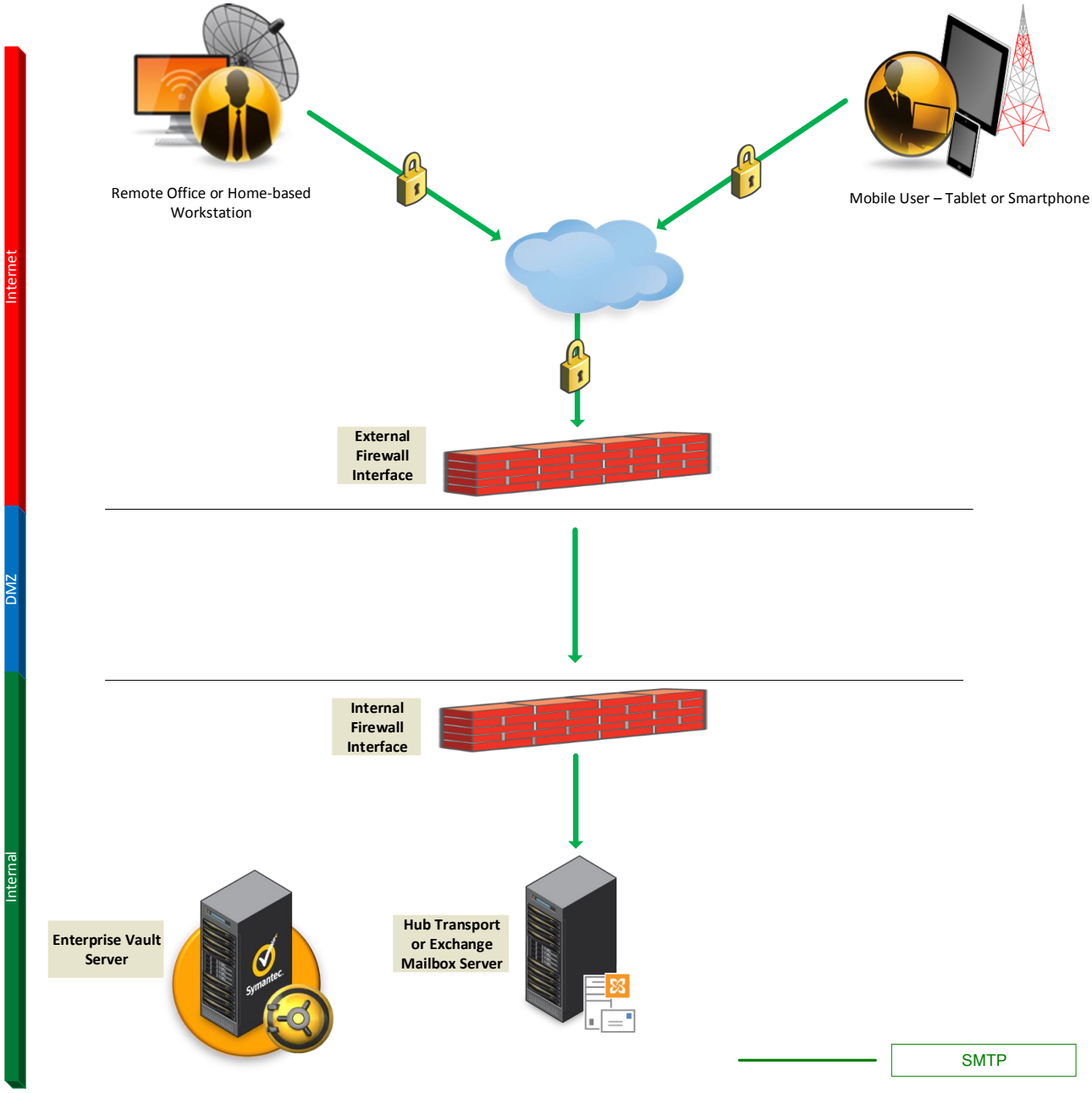


Figure 9 – Secure SMTP Relay through Hub Transport Server

Client Configuration

Once provisioned for IMAP access, the end user will receive a notification email containing the detail required to set up their mobile device or client. This message can be customized by the administrator. Alternatively end users can access their account configuration settings through an IMAP Landing page, a feature provided by the Enterprise Vault administrator. Figure 9 shows an example page where the end user is provided with configuration details for their device/email client.

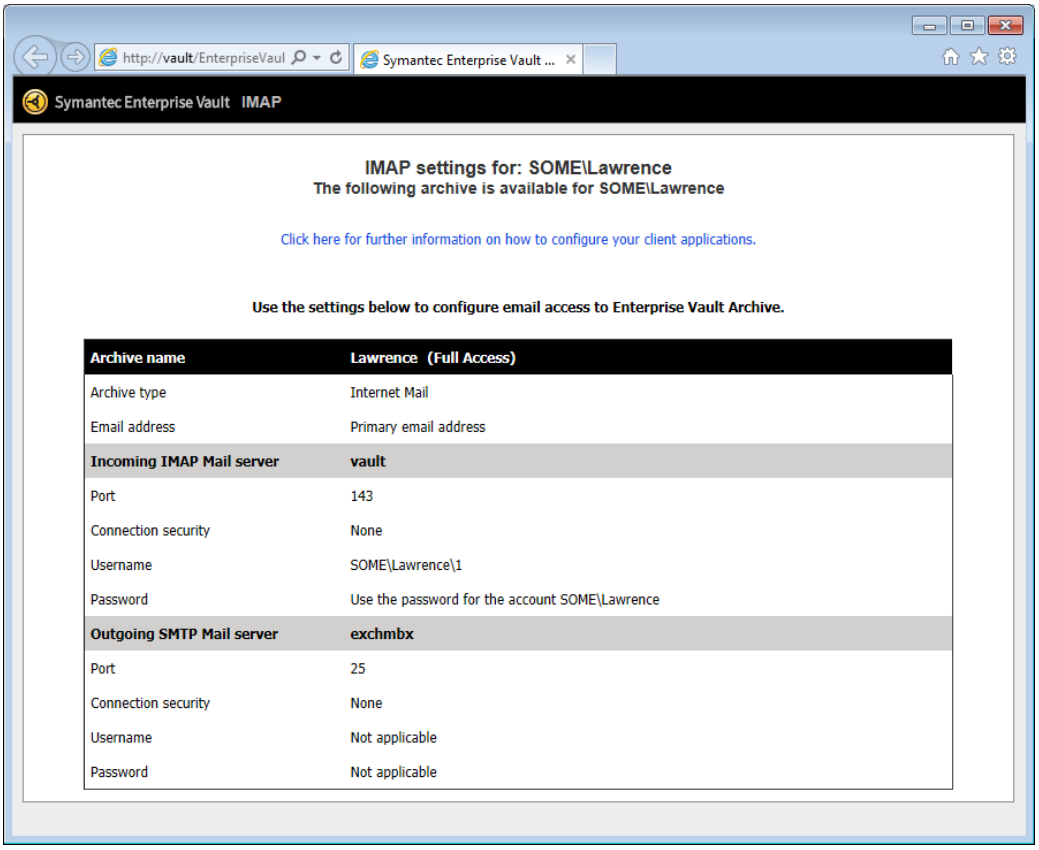


Figure 10 – Client configuration through the IMAP landing page

Enabling an archive for IMAP access is not always an instantaneous operation, as the Metadata Store build needs to take place for archives created on earlier versions of Enterprise Vault. The process has a minimum 20 minute wait for storage cache to recycle, and the user enablement notification will only be sent once this process has completed, and the Client Access Provisioning task has been run (manually or by the configured schedule).

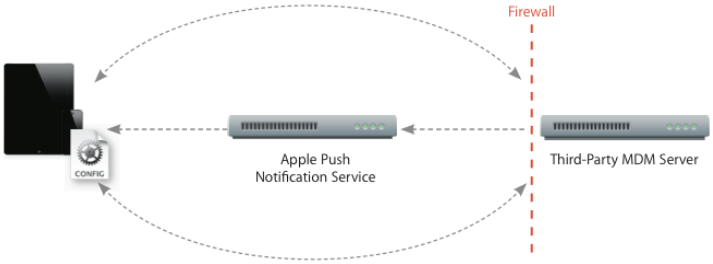
Licensing Considerations

IMAP enablement of Enterprise Vault Exchange mailboxes is provided as part of the Storage Management for Microsoft Exchange License. Creation and enablement of Internet Mail archives is provided as part of the Enterprise Vault Archiving Volume Tier License.

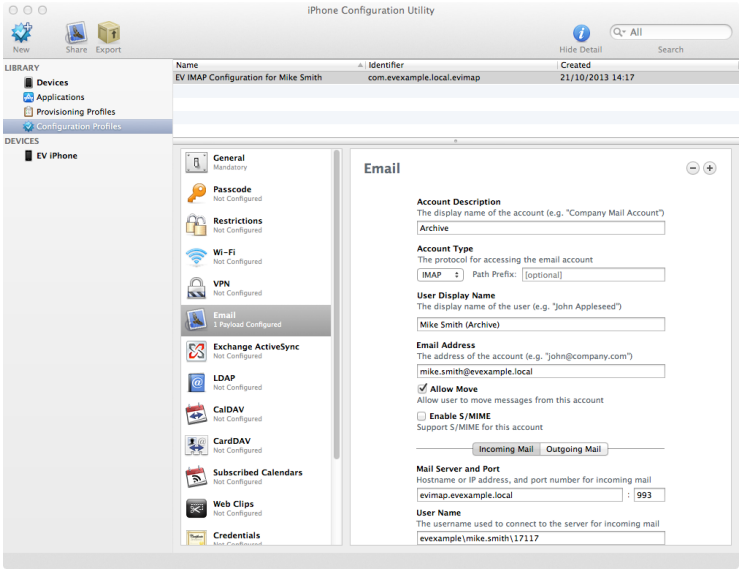
Mobile Device Management

Deployment to mobile devices often requires additional security and configuration techniques. Email accounts configured on phones or tablets are typically configured to use Microsoft's ActiveSync communication methodology either on its own or as part of a Mobile Device Management (MDM) configuration profile. The use of ActiveSync gives IT the possibility to perform some limited device configuration such as passcode enablement and lengths and the ability to remote wipe. Configuring IMAP directly on the device will not provide the same IT controls. Enterprise Vault does not provide a push mechanism for automatically configuring clients, however PowerShell commands are provided to allow an Enterprise Vault administrator to export settings for use in third party management applications. See the "Setting up IMAP.pdf" document for more details.

To allow IT departments to securely enroll devices in an enterprise environment, wirelessly configure and control the deployment of Enterprise Vault's IMAP access along with remotely wiping devices or profiles, Symantec recommends deploying IMAP along with an MDM solution.



iPhone & iPad MDM Overview



iOS Profile Configuration

EV IMAP Access Profile Installed

Figure 11 - iOS Mobile Device Management and Configuration Profile Creation

For more information on iOS mobile device management read Apple's guide at

http://www.apple.com/iphone/business/docs/iOS_6_MDM_Sep12.pdf

IMAP Administration from the Vault Admin Console

Administrators are able to:

- Define the IMAP servers and manage (Add/Remove/Enable/Disable IMAP servers)
- Define the IMAP server connection settings
- Create IMAP Provisioning groups to enable or disable end-user access
- Create and manage archives for IMAP end-users.

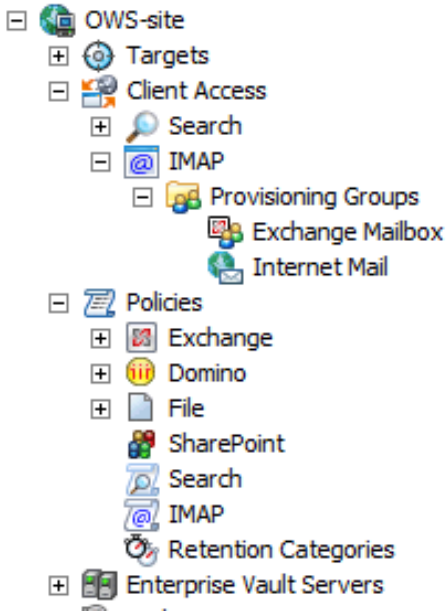


Figure 12 - New Client Access Node expanded within the Admin Console

Step by step instructions on how to configure the IMAP server can be found in the product documentation for Enterprise Vault 11.0.

Archiving of Email into Enterprise Vault using IMAP

Enterprise Vault supports archiving from any on premise or cloud mailbox. The user is in control; they can move items into their archive, or set client rules to decide what gets archived.

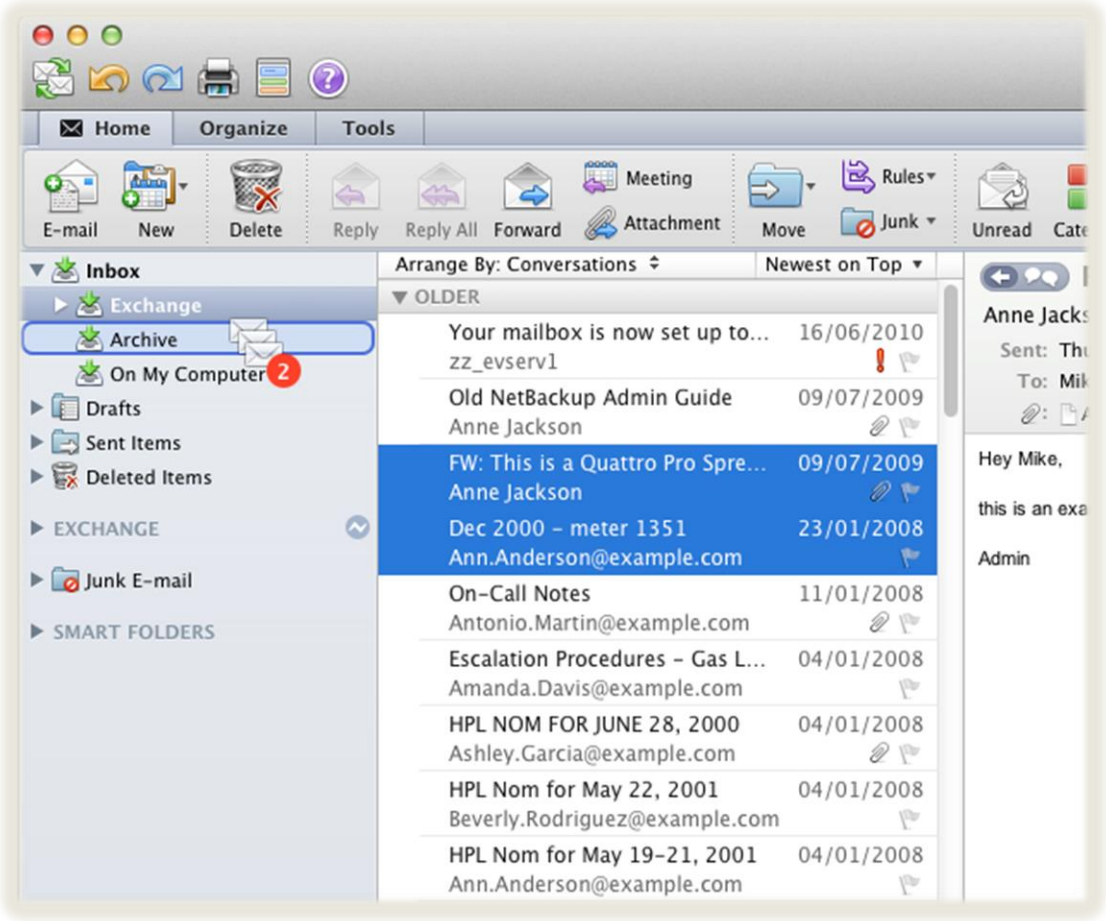


Figure 13 – End user archiving from any on premise or Cloud mailbox

Users can drag and drop messages they want to archive for retention or convenience.

About Symantec

Symantec is a global leader in providing security, storage, and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored. Headquartered in Mountain View, 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 website.

Symantec World Headquarters
350 Ellis St.
Mountain View, CA 94043 USA
+1 (650) 527 8000
1 (800) 721 3934
www.symantec.com