Symantec Enterprise Vault™ Technical Note

OWA Internal and External WebApp URLs

2007 SP4 and later

Symantec Enterprise Vault: OWA Internal and External WebApp URLs

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Last updated: November 26, 2010.

Legal Notice

Copyright © 2010 Symantec Corporation. All rights reserved.

Symantec, the Symantec Logo, Veritas, Enterprise Vault, Compliance Accelerator, and Discovery Accelerator are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This Symantec product may contain third party software for which Symantec is required to provide attribution to the third party (“Third Party Programs”). Some of the Third Party Programs are available under open source or free software licenses. The License Agreement accompanying the Software does not alter any rights or obligations you may have under those open source or free software licenses. Please see the *Third Party Software* file accompanying this Symantec product for more information on the Third Party Programs.

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Symantec Corporation and its licensors, if any.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. SYMANTEC CORPORATION SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, "Rights in Commercial Computer Software or Commercial Computer Software Documentation", as applicable, and any successor regulations. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.

Symantec Corporation
350 Ellis Street, Mountain View, CA 94043

http://www.symantec.com

Technical Support

Symantec Technical Support maintains support centers globally. Technical Support's primary role is to respond to specific queries about product features and functionality. The Technical Support group also creates content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering and Symantec Security Response to provide alerting services and virus definition updates.

Symantec's support offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and/or Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers software upgrades
- Global support purchased on a regional business hours or 24 hours a day, 7 days a week basis
- Premium service offerings that include Account Management Services

For information about Symantec's support offerings, you can visit our Web site at the following URL:

www.symantec.com/business/support/

All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policy.

Contacting Technical Support

Customers with a current support agreement may access Technical Support information at the following URL:

www.symantec.com/business/support/

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to replicate the problem.

When you contact Technical Support, please have the following information available:

- Product release level

- Hardware information
- Available memory, disk space, and NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description:
  - Error messages and log files
  - Troubleshooting that was performed before contacting Symantec
  - Recent software configuration changes and network changes

Licensing and registration

If your Symantec product requires registration or a license key, access our technical support Web page at the following URL:

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

Customer Service is available to assist with non-technical questions, such as the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates, such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information about product updates and upgrades
- Information about upgrade assurance and support contracts
- Information about the Symantec Buying Programs
- Advice about Symantec's technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs or manuals

Support agreement resources

If you want to contact Symantec regarding an existing support agreement, please contact the support agreement administration team for your region as follows:

Asia-Pacific and Japan	customercare_apac@symantec.com
Europe, Middle-East, and Africa	semea@symantec.com
North America and Latin America	supportsolutions@symantec.com

Configuring Internal and External WebApp URLs for OWA

This document includes the following topics:

Overview

The Enterprise Vault OWA Extensions for Exchange Server 2007 and later do not implement the `EnterpriseVaultProxy` mechanism that was used in the OWA 2003 extensions for accessing the Enterprise Vault server through the Exchange Servers. The task of protecting and forwarding requests to the Enterprise Vault server is now left to appropriate applications, such as Microsoft ISA Server. As a result, the OWA 2007 and later extensions are simpler to install and reduce load and attack surfaces on the Exchange Servers.

The initial implementation of the Enterprise Vault OWA 2007 Extensions did not support the configuration of a different URL for Enterprise Vault access from an external network. This meant that the Enterprise Vault server names had to be published by the external DNS servers in order to enable Search Archives or Archive Explorer in external OWA clients. This document describes how to set up your OWA environment so that a different Enterprise Vault server name is published to external OWA users.

If you want to configure the functionality described in this document for an Exchange 2003-only environment, you must set the Enterprise Vault Exchange mailbox policy setting "Client Connection" to "Direct", in order to turn off the `EnterpriseVaultProxy` mechanism. If an Exchange 2003 mailbox is accessed through an Exchange CAS, this happens automatically.

The following terms are used throughout this document:

- "External URL" is a URL that is used outside the corporate network to access the Enterprise Vault server through a firewall.
- "Internal URL" is a URL that is used inside the corporate network to access the Enterprise Vault server directly.

How to define the external URL for Enterprise Vault

You define an external URL for Enterprise Vault in the Exchange mailbox policy setting "External Web Application URL", which is in the advanced OWA list of settings. The policy can then be assigned to Provisioning Groups to enable groups of users to access Enterprise Vault servers from their OWA clients using the external URLs.

The value of the external URL setting can be either a fully qualified URL to the Web Access application virtual directory, or a relative URL. An example of a fully qualified URL is:

http://evserver1.external.name/enterprisevault

An example of a relative URL is:

/enterprisevault

If a relative URL is specified, the fully qualified URL is constructed using the external host name of the Exchange Server used for OWA. This name is configured on the Exchange Server. An optional <https> component can be specified at the start of the relative URL to indicate that the HTTPS protocol should be used. If it is not present, then the HTTP protocol is used.

Table 1-1 gives examples of the URL that is used.

Table 1-1 Defining the external URL that will be used to access Enterprise Vault

URL used for OWA	Value set for External Web Application URL	External URL used for Enterprise Vault
https://owa.company.com/owa	http://ev.company.com/ enterprisevault	http://ev.company.com/ enterprisevault
https://owa.company.com/owa	/enterprisevault	http://owa.company.com/ enterprisevault
https://owa.company.com/owa	<https>/enterprisevault	https://owa.company.com/ enterprisevault
https://owa.company.com/owa	:8080/enterprisevault	http://owa.company.com:8080/ enterprisevault

The default value of the "External Web Application URL" policy setting is:

<https>/EnterpriseVault

The Enterprise Vault policy setting can be overridden by a configuration setting on the Exchange Server. See Table 1-2. This allows for load balancing, such that different Exchange CAS servers can use different URLs, and therefore access different Enterprise Vault servers.

On Exchange Server 2003, the setting is added to the `EVBackEnd.ini` file on the back-end Exchange Server 2003 computer. On Exchange Server 2007 and later, it is added to the `Web.Config` file on the Exchange CAS. In `Web.Config`, "<https>/EnterpriseVault" should be added as "&lt;https&gt;/EnterpriseVault".

The setting is read when the user logs into OWA, so a change to the value takes effect when the user next logs into OWA.

Table 1-2 URL setting on Exchange Server

Setting name in Exchange Server 2007 and later	Setting name in Exchange Server 2003	Description
EnterpriseVault_ ExternalWebAppUrl	ExternalWebAppUrl	Defines the external URL for Enterprise Vault access, and follows the same rules as the policy setting described above.

The Exchange Server 2003 setting is configured at virtual directory level, so that it is possible to use different settings for different OWA virtual directories. In `EVBackEnd.ini` the setting can be qualified as follows:

*server name.website ID.exchange virt dir name.*ExternalWebAppUrl=*value*

For example:

Exch01.1.exchange.ExternalWebAppUrl=/enterprisevault

Determining when to use the external URL for Enterprise Vault

The table, Table 1-3, describes three settings available to refine which users access Enterprise Vault using the external Web access URL.

The UseExternalWebAppUrl setting forces all connections to use the configured external URL. If you want to configure some connections to use the external URL and others to use the internal URL, use the ExternalHostNames and/or ExternalIPAddresses settings instead.

Add the required settings to the configuration file on the Exchange Servers. On Exchange Server 2003, these settings are added to the `EVBackEnd.ini` file. On Exchange Server 2007 and later, they are added to the `Web.Config` file.

The settings are read when the user logs into OWA, so changes to the values take effect when the user next logs into OWA.

Table 1-3 External URL settings on the Exchange Server

Setting name in Exchange Server 2007 and later	Setting name in Exchange Server 2003	Value
EnterpriseVault_ UseExternalWebAppUrl	UseExternalWebAppUrl	The value is a simple Boolean value which defines whether the external URL is to be used or not. If the value is set to "True", then all Enterprise Vault connections are forced to use the configured external URL. If this value is set, then it overrides the settings below.

Table 1-3 External URL settings on the Exchange Server *(continued)*

Setting name in Exchange Server 2007 and later	Setting name in Exchange Server 2003	Value
EnterpriseVault_ ExternalHostNames	ExternalHostNames	The value is a semi-colon delimited list of host names. If the host name used to access OWA is in the list, then the external URL will be used to access Enterprise Vault. For example, if a user accesses OWA outside the corporate network using **https://owa.company.com/owa**, then **owa.company.com** could be added to this list. Enterprise Vault connections from hosts that are not listed in this setting , or from IP addresses that are not listed in the ExternalIPAddresses setting, will use the configured internal URL.

Table 1-3 External URL settings on the Exchange Server *(continued)*

Setting name in Exchange Server 2007 and later	Setting name in Exchange Server 2003	Value
EnterpriseVault_ ExternalIPAddresses	ExternalIPAddresses	The value is a semi-colon delimited list of IP addresses. If the IP address of the originator of the request to OWA is on this list, then the external URL will be used to access Enterprise Vault. For example, the IP addresses of the firewall servers could be added to this list. Enterprise Vault connections from addresses that are not listed in this setting, or from hosts that are not listed in the ExternalHostNames setting, will use the configured internal URL. Note that when using an Exchange CAS proxy, the originator is the Exchange CAS acting as proxy, not the firewall. In this case, it may be better to specify the host names to trigger the use of the external URL.

The Exchange Server 2003 settings are configured at virtual directory level, so that it is possible to use different settings for different OWA virtual directories. In `EVBackEnd.ini` the setting can be qualified as follows:

server name.website ID.exchange virt dir name.setting name=value

For example:

Exc01.1.exchange.UseExternalWebAppUrl=true

The settings for Exchange Server 2007 and later are configured in the **appSettings** section of the `Web.Config` file. For example:

<add key="EnterpriseVault_UseExternalWebAppUrl" value="true"/>

Load balancing

The flexibility of Enterprise Vault architecture means that any user in the site can access the Enterprise Vault Web Access application using any Enterprise Vault server. For this reason, publishing only one Enterprise Vault server on a firewall or Exchange CAS proxy is feasible. However, the feature described in this document allows for load balancing. Load balancing can be implemented in the following ways:

- Use an external load-balancer or round-robin DNS on the given host name.
- Assign a different virtual directory name in different policies. This will allow the URL to be used by different firewall or Exchange CAS proxy rules, which would forward requests to different Enterprise Vault servers.

  For example, user A could be assigned a policy with "External Web Application URL" set to "/EV1", and user B could be assigned a policy with "External Web Application URL" set to "/EV2".

  Both users use the same OWA server, accessed using the URL:

  https://mail.company.com/owa

  For User A the external URL to access Enterprise Vault would be:

  https://mail.company.com/EV1

  For User B, the URL would be:

  https://mail.company.com/EV2

  These URLs would both be processed by the same firewall server. However, the firewall server would have different rules for the virtual directories, EV1 and EV2:

  - EV1 would map to http://evserver1/enterprisevault.
  - EV2 would map to http://evserver2/enterprisevault.
- Assign a different virtual directory name on different Exchange Servers using the "ExternalWebAppUrl" configuration setting.
- Assign a different, fully qualified URL in different Exchange Mailbox policies, and assign the policies appropriately. These could use different host names to access different firewall or proxy servers, or different virtual directory names to access different firewall rules.
- Assign a different fully qualified URL on different Exchange Servers using the "ExternalWebAppUrl" configuration setting.

Similar techniques can also be used to allow for mailboxes in different Enterprise Vault sites; each site’s policies would need to specify a different external URL to allow the firewall rules to be set to access an Enterprise Vault server in the correct site.

Fault tolerance

The configurations discussed in this document make no allowance for fault tolerance; they simply provide the OWA client with one URL for Enterprise Vault access. If the target Enterprise Vault server fails, then the client will not be able to access Enterprise Vault.

Clustered Enterprise Vault servers could be used to provide resilience.

Customized shortcut links

In the Enterprise Vault OWA 2003 Extensions, the links in customized shortcuts are translated by the OWA extensions to refer back to the Exchange Server. In the OWA 2007 and later extensions, the links are not translated by the extensions. They are, however, translated by OWA to refer back to the Exchange Server, and the original link is added as a parameter. For this reason, normal link translation by a firewall or proxy may not work. However, Microsoft ISA 2006 is capable of translating the links as described in the following article:

http://technet.microsoft.com/en-us/library/bb794742(TechNet.10).aspx

To ensure this works correctly:

- There must be a "Computer" Network Object for the Enterprise Vault server that is being published.
- The "This rule applies to this published site" value on the "To" page of the Enterprise Vault Web publishing rule properties dialog must be the host value in the customized shortcut link.

Other firewall or proxy solutions may also be able to handle this translation.

Translating customized shortcut links is not discussed further in this document, as the links are intended for clients that are not integrated with Enterprise Vault, such as Outlook Express. In OWA clients, double-clicking the item will open the item, even if the customized shortcut link has not been translated correctly.

OWA configuration examples

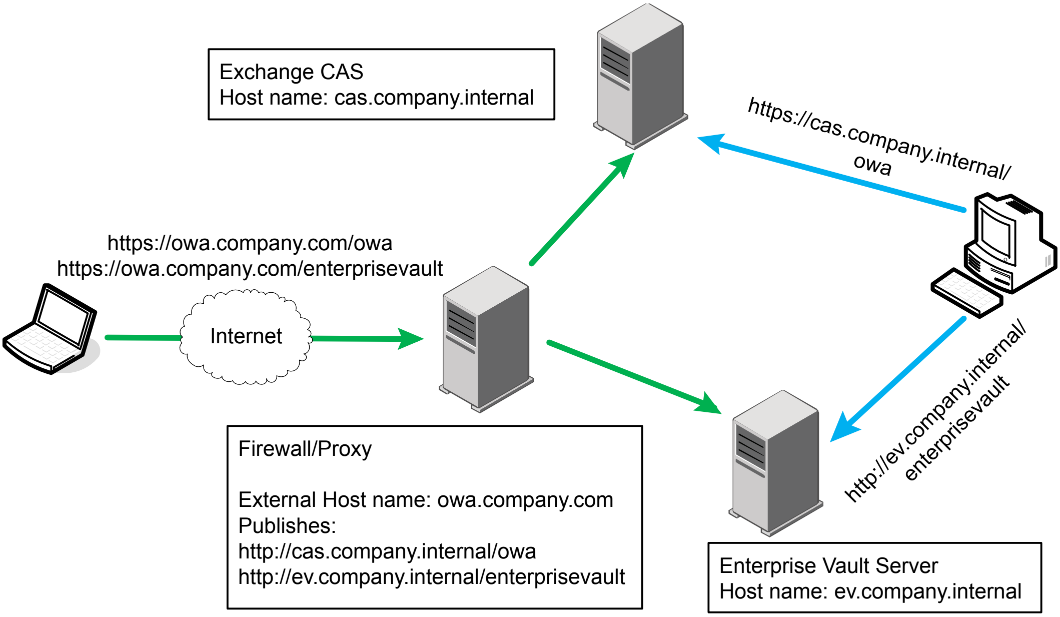
This section illustrates different OWA configurations in which the functionality described in this document can be used.

In the examples, Exchange CAS servers can be Exchange Server 2007 or later.

Note that additional configuration is required if OWA 2007 clients access the Exchange 2007 CAS through an Exchange Server 2010 CAS. The additional steps are documented in the following technical note on the Symantec Enterprise Support Web site:

http://www.symantec.com/docs/TECH125053

Different host names


Exchange CAS
Host name: cas.company.internal
https://cas.company.internal/owa
https://owa.company.com/owa
https://owa.company.com/enterprisevault
Internet
Firewall/Proxy
External Host name: owa.company.com
Publishes:
http://cas.company.internal/owa
http://ev.company.internal/enterprisevault
http://ev.company.internal/enterprisevault
Enterprise Vault Server
Host name: ev.company.internal

In this case, external clients access OWA using the following URL: .

https://owa.company.com/owa

Whereas internal clients use a different URL:

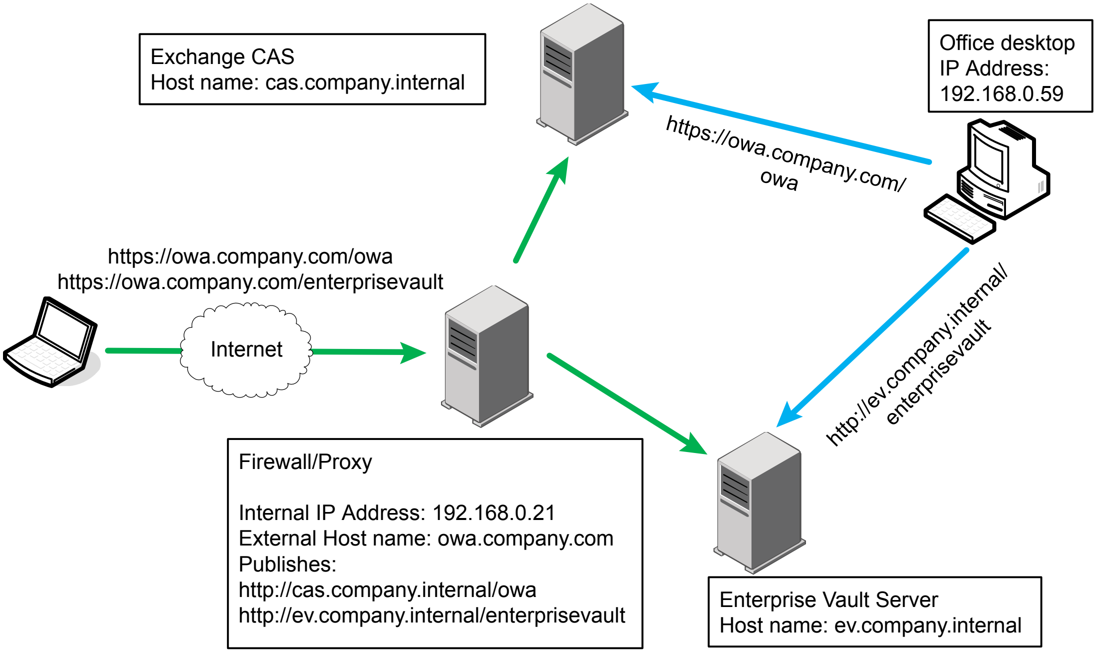
https://cas.company.internal/owa

The following settings should be used to allow the OWA extensions to use the correct URL:

External Web Application URL: <https>/enterprisevault

EnterpriseVault_ExternalHostNames: owa.company.com

Different IP addresses


Exchange CAS
Host name: cas.company.internal
Office desktop
IP Address:
192.168.0.59
https://owa.company.com/
owa
https://owa.company.com/owa
https://owa.company.com/enterprisevault
Internet
http://ev.company.internal/
enterprisevault
Firewall/Proxy
Internal IP Address: 192.168.0.21
External Host name: owa.company.com
Publishes:
http://cas.company.internal/owa
http://ev.company.internal/enterprisevault
Enterprise Vault Server
Host name: ev.company.internal

In this case, both external and internal clients use the same URL to access OWA:

https://owa.company.com/owa

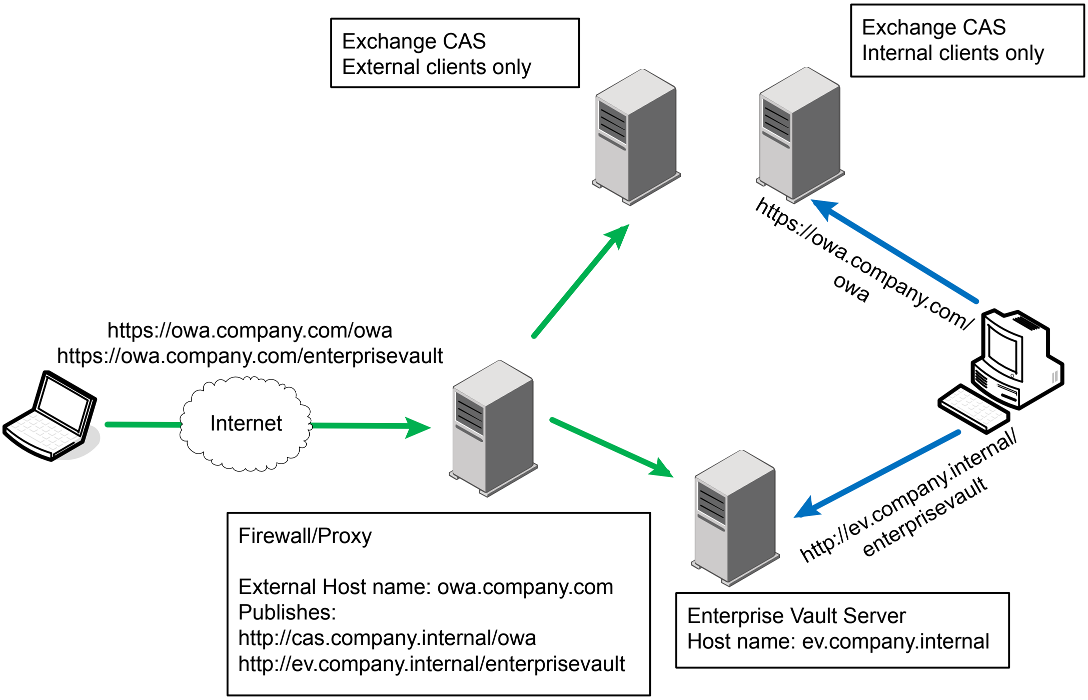
The internal DNS maps the name directly to the Exchange CAS. The OWA extensions cannot use the host name to differentiate, and so they use the IP address of the originator of the request instead. For internal clients, this will be the IP address of the client, but for external clients it will be the IP address of the firewall or proxy server.

The following settings should be used:

External Web Application URL: <https>/enterprisevault

EnterpriseVault_ExternalIPAddresses: 192.168.0.21

Different Exchange CAS servers


Exchange CAS
External clients only
Exchange CAS
Internal clients only
https://owa.company.com/owa
https://owa.company.com/owa
https://owa.company.com/enterprisevault
Internet
Firewall/Proxy
External Host name: owa.company.com
Publishes:
http://cas.company.internal/owa
http://ev.company.internal/enterprisevault
http://ev.company.internal/enterprisevault
Enterprise Vault Server
Host name: ev.company.internal

In this case, dedicated Exchange CAS servers are used for internal and external access. Rather than using host names or IP addresses, the settings should be:

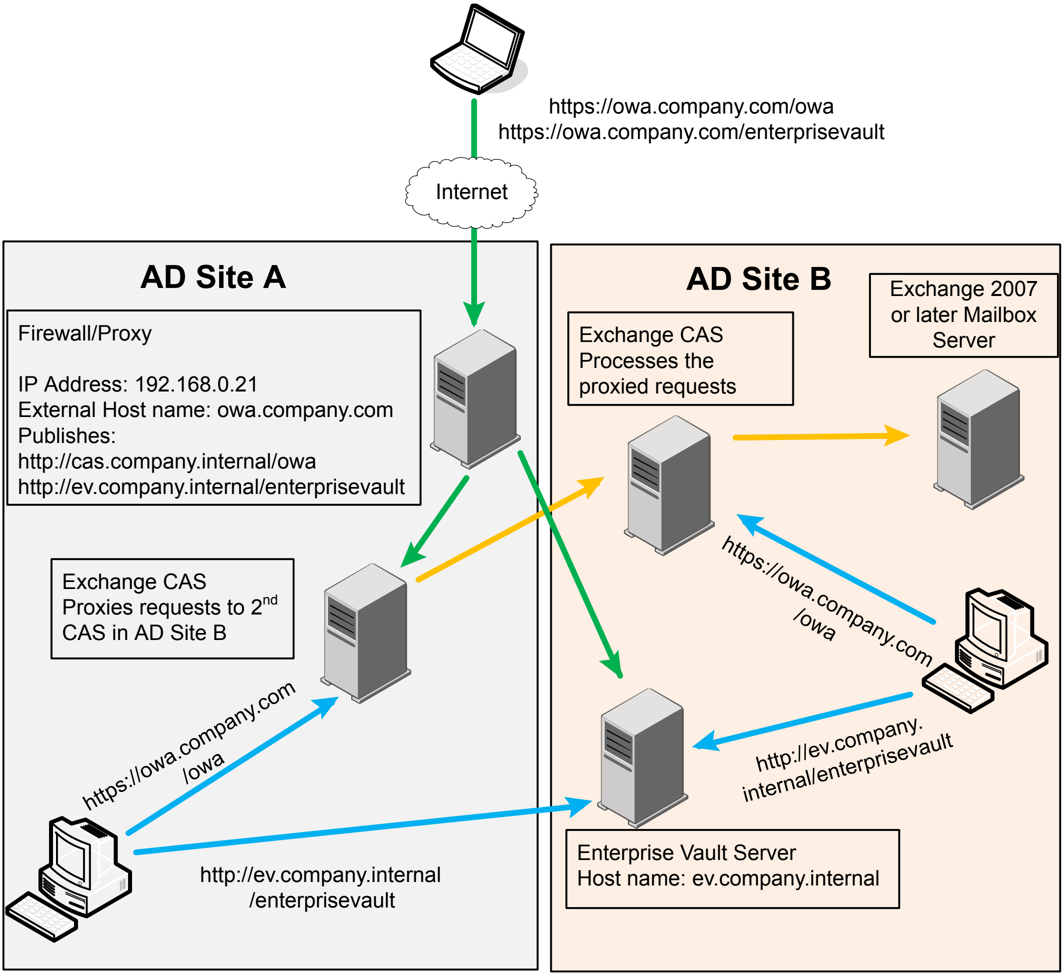
External Web Application URL: <https>/enterprisevault

EnterpriseVault_UseExternalWebAppUrl: true. Note that this is set on the external facing Exchange CAS only.

It would be possible to use the "EntepriseVault_ExternalIPAddresses" setting instead in this scenario. Also, no settings need to be added to the internal facing Exchange CAS, because the internal URL will be used by default.

Using an Exchange CAS proxy

The main difference with using an Exchange CAS proxy is that it is the proxy server which determines whether to use an external URL, and not the Exchange CAS actually processing the requests.


https://owa.company.com/owa
https://owa.company.com/enterprisevault
Internet
AD Site A
Firewall/Proxy
IP Address: 192.168.0.21
External Host name: owa.company.com
Publishes:
http://cas.company.internal/owa
http://ev.company.internal/enterprisevault
Exchange CAS
Proxies requests to 2nd CAS in AD Site B
https://owa.company.com /owa
http://ev.company.internal /enterprisevault
AD Site B
Exchange CAS Processes the proxied requests
Exchange 2007 or later Mailbox Server
https://owa.company.com /owa
http://ev.company. internal/enterprisevault
Enterprise Vault Server
Host name: ev.company.internal

In this example, the same URL, https://owa.company.com/owa, is used for both external and internal access to OWA. The Exchange CAS in site A acts as a proxy server and forwards requests to the Exchange CAS in site B. This means that to the Exchange CAS in site B the originator of the request appears to be the first Exchange CAS. For this reason it cannot determine whether the request has come from the Internet or from an internal client in site A.

The following settings should be used:

External Web Application URL: <https>/enterprisevault

EntepriseVault_ExternalIPAddresses: 192.168.0.21. Note that this is set on the Exchange CAS in Site A.

If the Exchange CAS in site A determines that an external URL should be used, then the first Exchange CAS appends an extra query string parameter to the request passed to the Exchange CAS in site B. This allows the OWA extensions doing the real work on the Exchange CAS in site B to use an external URL if necessary.

The Exchange CAS in site B has no additional configuration to determine whether to use external URLs, as it does not handle external requests directly. Hence requests from the internal client in site B will always use the internal URL.

Exchange Server 2003 mailboxes

This section describes how the functionality described in this document can be configured to provide access for OWA 2003 clients.

Using an Exchange 2003 Back-End server

This is similar to the configuration required for Exchange Server 2007 and later mailboxes without an Exchange CAS proxy server, and all the considerations mentioned remain valid.

See “Different host names” on page 15.

See “Different IP addresses” on page 16.

Note that in Exchange Server 2003, OWA requests are always redirected to the back-end server holding the mailbox, so the configuration described in Different Exchange CAS servers is not applicable.

Using an Exchange Server 2003 Front-End server

This is similar to accessing Exchange Server 2003 mailboxes through an Exchange Server CAS.

See “Using an Exchange CAS (internal and external)” on page 20.

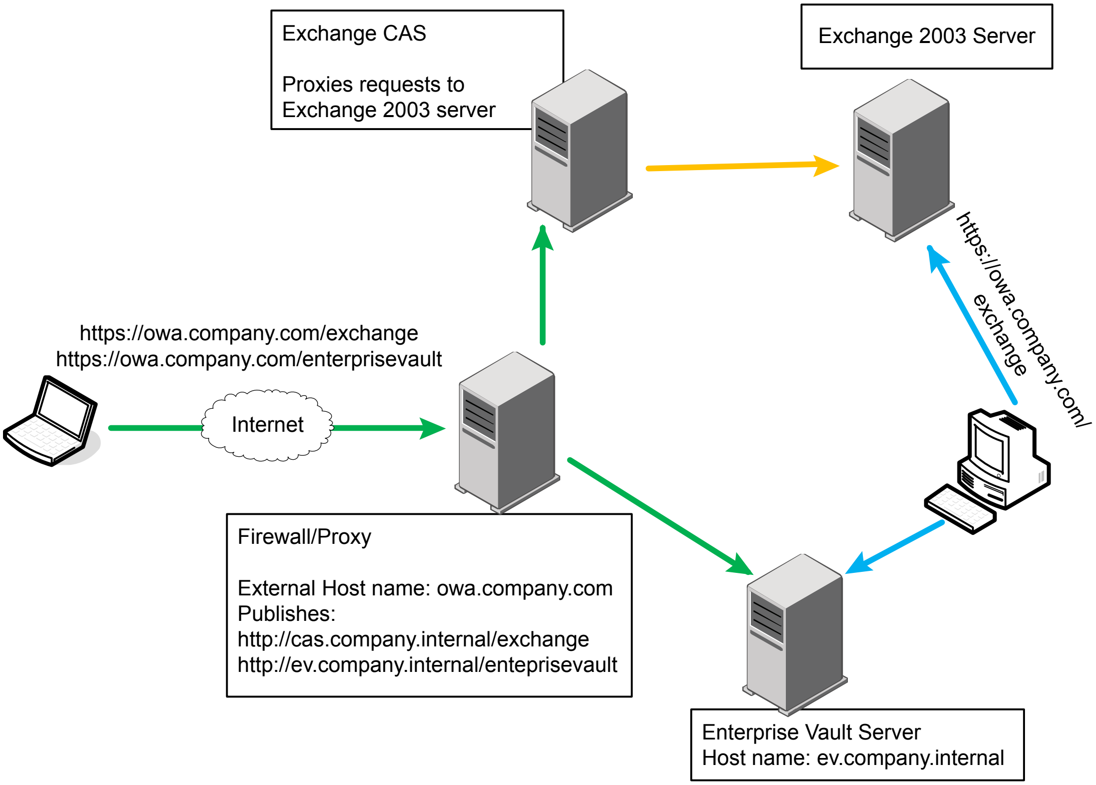
See “Using an Exchange CAS Server (external only)” on page 21.

See “Using separate Exchange CAS Servers” on page 22.

The front-end Exchange Server cannot pass any information to the back-end OWA extensions, and the details described in these sections remain valid.

Using an Exchange CAS (internal and external)

Although this appears similar to using an Exchange CAS as a proxy server, the Exchange CAS is unable to pass on any information to the OWA 2003 Extensions. This means that if both internal and external clients access the Exchange CAS using the same host name, then there is no way of determining if an internal or external URL should be used.


Exchange CAS
Proxies requests to Exchange 2003 server
Exchange 2003 Server
https://owa.company.com/exchange
https://owa.company.com/enterprisevault
Internet
https://owa.company.com/exchange
Firewall/Proxy
External Host name: owa.company.com
Publishes:
http://cas.company.internal/exchange
http://ev.company.internal/entepriseavault
Enterprise Vault Server
Host name: ev.company.internal

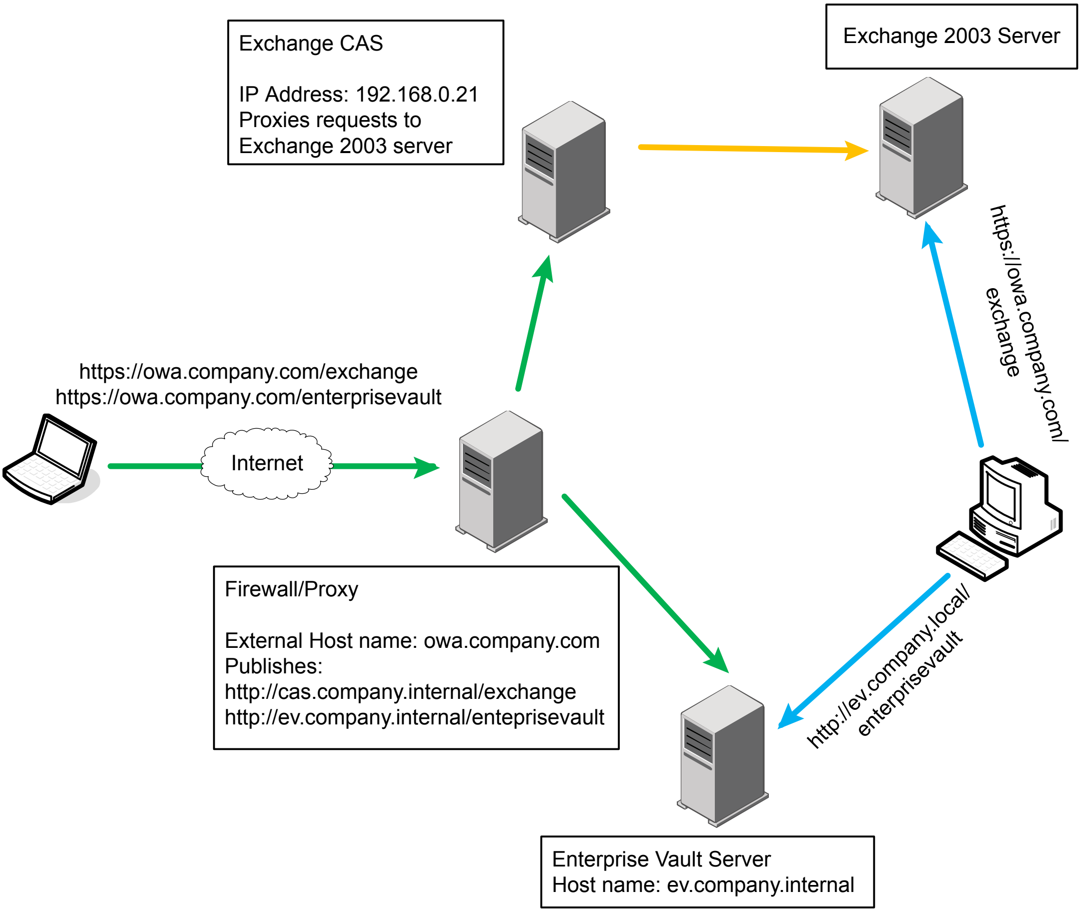
One possible workaround is to have the internal URL access an Exchange Server 2003 back-end server directly. Even if more than one Exchange Server 2003 is in use, the client will be redirected to the correct server, and the IP address can be used to distinguish internal and external clients. This is described in more detail in Using an Exchange CAS Server (external only).

A second workaround is to introduce a second Exchange CAS, so that internal clients and external clients use different Exchange CAS servers. This is described in Using separate Exchange CAS Servers.

A third workaround is to create an additional virtual directory on the Exchange CAS and back-end servers. The firewall or proxy could then be configured to pass requests to the new virtual directory on the Exchange CAS, which in turn would forward it to the new virtual directory on the back-end server. The new virtual directory could then be specified in the "UseExternalWebAppURL" setting, so that requests using that virtual directory would trigger the external URL for Enterprise Vault, and requests for the **exchange** virtual directory would trigger the internal URL for Enterprise Vault.

Using an Exchange CAS Server (external only)

If only external clients are coming through the Exchange CAS, as illustrated below, then the "ExternalIPAddresses" setting can be used to trigger external URLs.



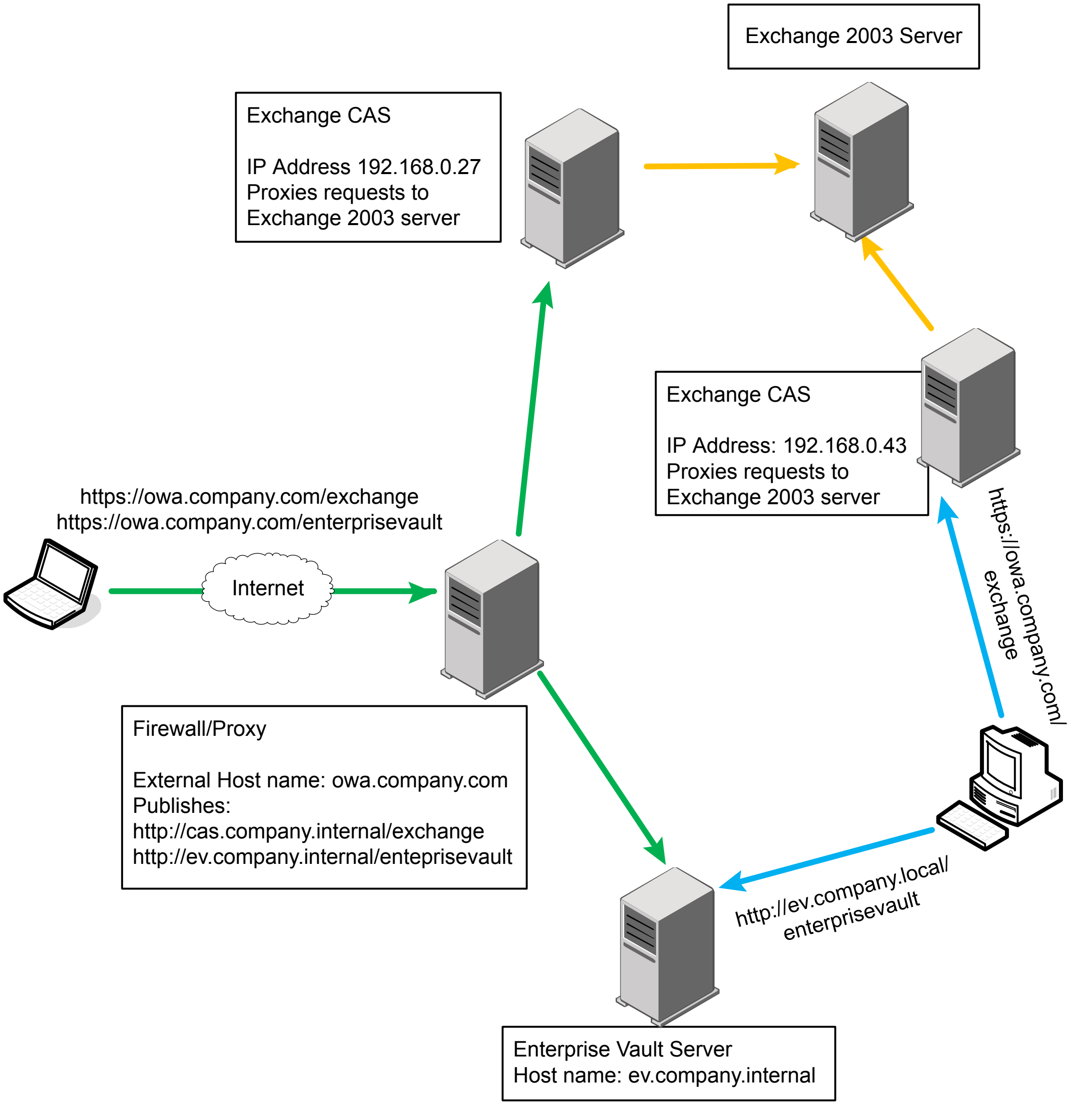
In this case the following settings could be used:

External Web Application URL: <https>/enterprisevault

ExternalIPAddresses: 192.168.0.21. Note that this is set on Exchange Server 2003.

Using separate Exchange CAS Servers

Although this configuration is similar to that illustrated in Different Exchange CAS servers, the configuration settings would be applied on the Exchange 2003 server, using the IP address of the Exchange CAS for the external clients.



In this example, the following settings should be used:

External Web Application URL: <https>/enterprisevault

ExternalIPAddresses: 192.168.0.27. Note that this is set on the Exchange 2003 server.