Enterprise Vault™ Requesting and Applying an SSL Certificate

12.3 and later

VERITAS™

Enterprise Vault™: Requesting and Applying an SSL Certificate

Last updated: 2023-07-27.

Legal Notice

Veritas Technologies LLC, 2625 Augustine Drive, Santa Clara, CA 95054

https://www.veritas.com

Technical Support

Technical Support maintains support centers globally. All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policies. For information about our support offerings and how to contact Technical Support, visit our website:

https://www.veritas.com/support

You can manage your Veritas account information at the following URL:

https://my.veritas.com

If you have questions regarding an existing support agreement, please email the support agreement administration team for your region as follows:

Worldwide (except Japan)	CustomerCare@veritas.com
Japan	CustomerCare_Japan@veritas.com

Before you contact Technical Support, run the Veritas Quick Assist (VQA) tool to make sure that you have satisfied the system requirements that are listed in your product documentation. You can download VQA from the following article on the Veritas Support website:

https://www.veritas.com/support/en_US/vqa

Documentation

Make sure that you have the current version of the documentation. Each document displays the date of the last update on page 2. The latest documentation is available on the Veritas website:

https://www.veritas.com/docs/100040095

Documentation feedback

Your feedback is important to us. Suggest improvements or report errors or omissions to the documentation. Include the document title, document version, chapter title, and section title of the text on which you are reporting. Send feedback to:

evdocs@veritas.com

You can also see documentation information or ask a question on the Veritas community site:

https://www.veritas.com/community

Requesting and Applying an SSL Certificate

This document includes the following topics:

Introduction

From Enterprise Vault 12.3, Enterprise Vault web applications in new installations are configured to use HTTPS with Secure Sockets Layer (SSL) on port 443 by default. If a certificate does not already exist, the Enterprise Vault configuration wizard generates and installs a self-signed certificate, and enables SSL on all Enterprise Vault virtual directories in Internet Information Services (IIS). The self-signed certificate should be regarded as temporary. We strongly recommend that you replace this certificate as soon as possible with one obtained from a trusted certificate authority.

In earlier releases of Enterprise Vault, the default configuration for the Enterprise Vault web applications was HTTP over TCP port 80. If you upgrade to Enterprise Vault 12.3 or later, the existing protocol configured for Enterprise Vault web applications is not changed. To ensure the security of client connections to Enterprise

Vault, we strongly recommend that you configure SSL in IIS, and enable it on all Enterprise Vault virtual directories.

Some Enterprise Vault features, such as the Enterprise Vault Office Mail App, require secure connections. Although the information in this document is primarily about securing Enterprise Vault Office Mail App connections, the general procedure is applicable to securing web connections to other Enterprise Vault features.

This document describes how to create an SSL certificate request file and obtain a certificate, and how to apply the certificate using Internet Information Services (IIS) Manager. The document also describes a further optional procedure that is required only if you want to secure all new archive and restore actions, and all archive search requests.

In Enterprise Vault 10.0.3 and later, the Enterprise Vault Office Mail App is the only option for Enterprise Vault functionality in Outlook Web Access (OWA) with Microsoft Exchange Server 2013. With Exchange Server 2013, the Office Mail App replaces the Enterprise Vault OWA Extensions on the Client Access Server, which are required for older versions of Exchange Server.

Microsoft Office Mail Apps must be secured using SSL. Therefore the Enterprise Vault virtual directory on each Enterprise Vault server that services and loads the Enterprise Vault Office Mail App must be secured using SSL. The setup of the Office Mail App determines which servers service requests from Office Mail App users. For information about Office Mail App setup, see the Enterprise Vault *Setting up Exchange Server Archiving* guide. Additional factors, such as a Microsoft Threat Management Gateway farm or a third-party load balancing device, may affect which Enterprise Vault servers service requests.

The Enterprise Vault virtual directory may need to be secured using different names; for example, **EV.*domain*.com** and **EV1.*domain*.local** for HTTPS requests. In addition, you may want to request a certificate that contains all your internal server names, such as **EV1.*domain*.local** and **EV2.*domain*.local**, so the same certificate can be used on different Enterprise Vault servers. In these cases, you may require a Subject Alternative Name (SAN) certificate. These decisions depend on your Office Mail App requirements, and possibly on your requirements for securing Enterprise Vault web-based communication in general.

If only one namespace is required, then the procedures in this document still apply, but you need to add only one name to the certificate. Later on, there may be a requirement to add additional namespaces for expansion of the Enterprise Vault environment. In this case, the procedures are still valid, and a new SAN certificate with the additional namespaces is required from your certificate authority.

In most cases, obtaining a trusted certificate from a certificate authority is recommended and is considered industry best practice. This document assumes that this method is the one in use. However, you can produce a certificate using

your own certification of authority. The details of this method are not covered in this document.

The procedures assume that Internet Information Services (IIS) 7.0/7.5 is in use on the Enterprise Vault servers.

Creating a certificate request file

Before you follow the procedure to create a certificate request (`.req`) file:

- Identify the DNS namespaces required. For example, if you want to secure internal communication and external web requests for the Enterprise Vault Office Mail App or Enterprise Vault access, the names might be **evserver.*domain*.local** and **ev.*domain*.com**, where ***domain*** is the domain name.
- Decide which Enterprise Vault servers need a certificate. The following factors determine this requirement:
  - The configuration of the Enterprise Vault Office Mail App and Enterprise Vault itself.
  - Whether the load is balanced, and if so the load-balancing method.

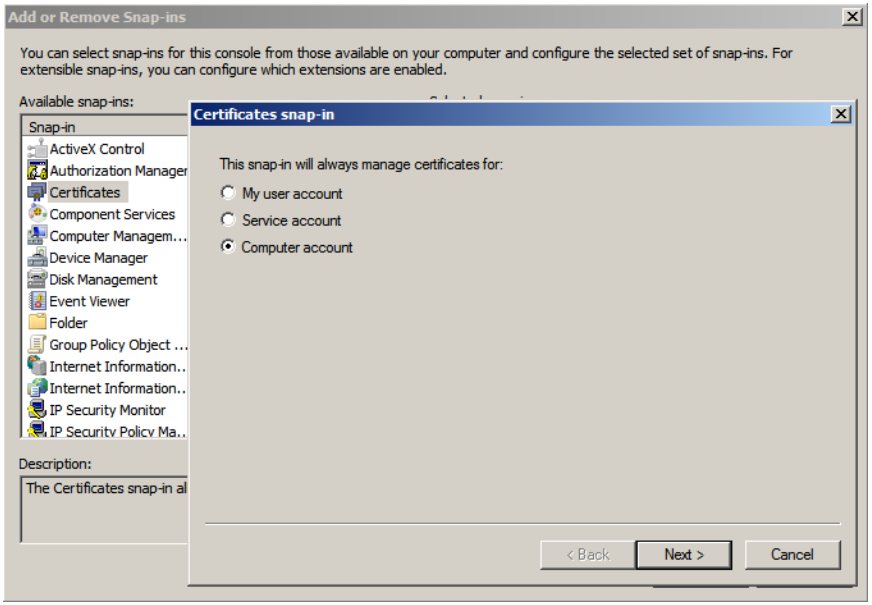
  You may then need to create a Subject Alternative Name (SAN) certificate for multiple server names, for example **EVserver1.*domain*.local** and **EVserver2.*domain*.local**.

To create the certificate request file, follow this procedure on one Enterprise Vault server.

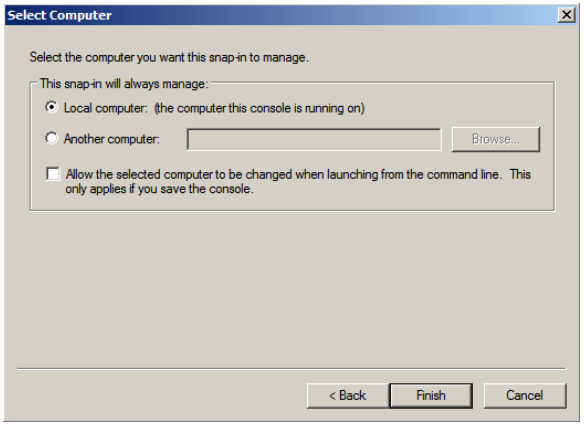
To create a certificate request file

1. On an Enterprise Vault server, open the **Start** menu, type **mmc** in the Search box, and press Enter to run `mmc.exe`.
2. On the **File** menu, click **Add/Remove Snap-in**.

3 Double-click **Certificates**, select **Computer Account**, and click **Next**.



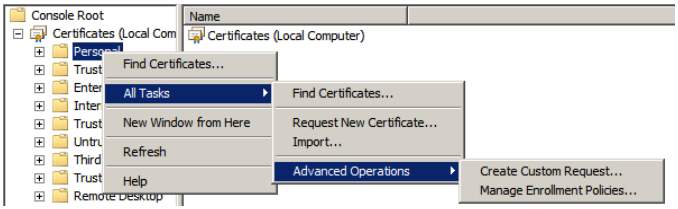
4 Select **Local Computer**, and click **Finish**.



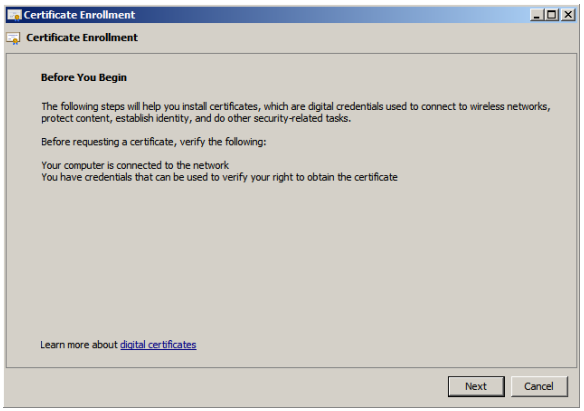
5 Click **OK**.

6 Expand the **Certificates** node.

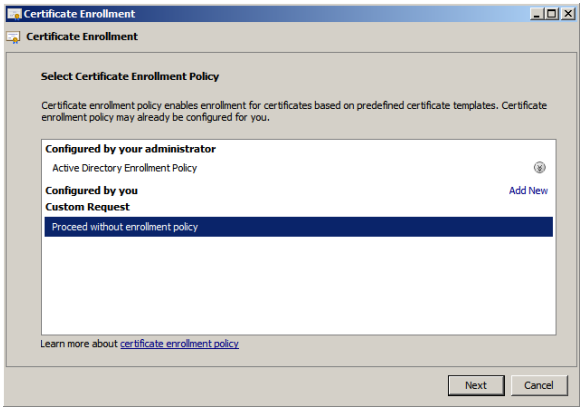
7 Right-click **Personal** and select **All Tasks** > **Advanced Operations** > **Create Custom Request**.



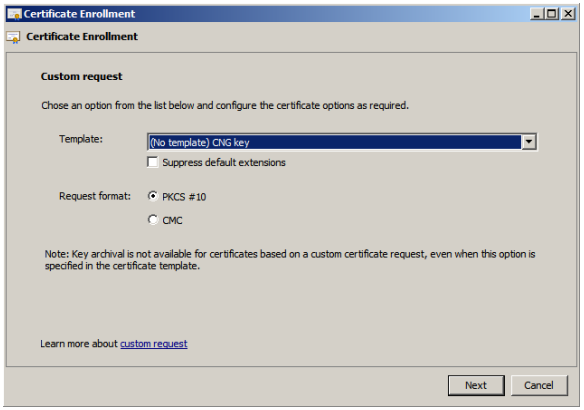
8 On the Certificate Enrollment Welcome page, click **Next**.



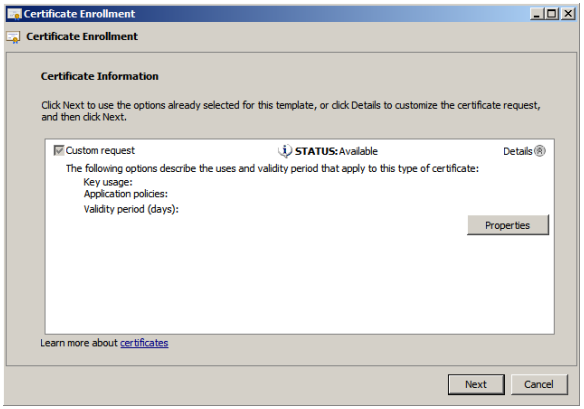
9 Select **Proceed without enrollment policy** and click **Next**.



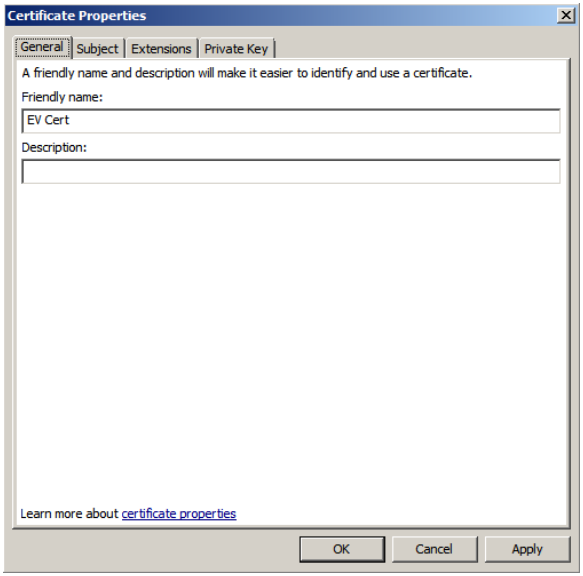
10 Accept the default options and click **Next**.



11 Expand **Details** and click **Properties**.

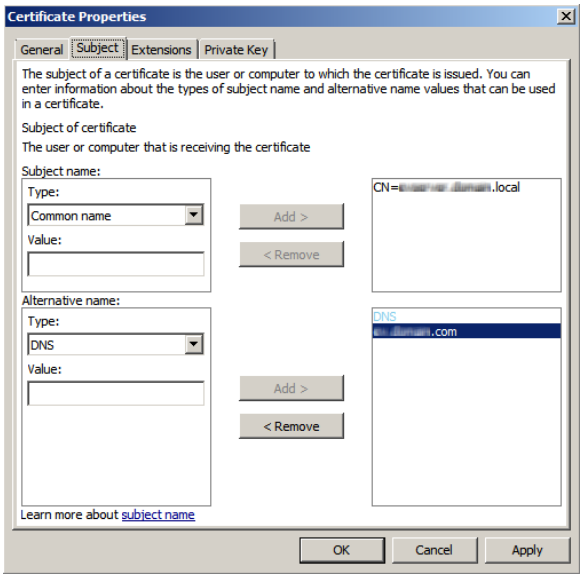


12 On the Certificate Properties General tab, enter a **Friendly name**, which can be anything you choose.



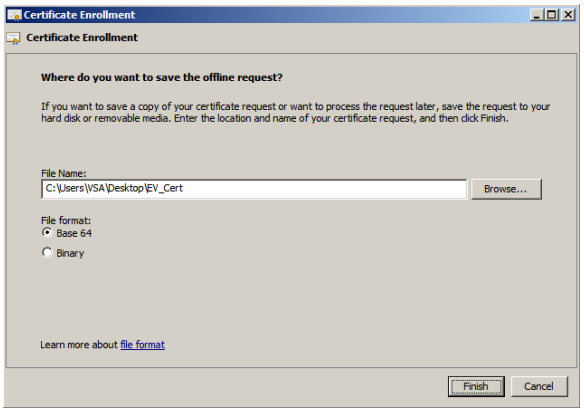
13 On the Certificate Properties Subject tab, under **Subject name**, select the type **Common name** and add a common name. In this case the common name is the internal namespace name for the Enterprise Vault server.

14 Still on the Certificate Properties Subject tab, under **Alternative name**, select the **DNS** type and add the external namespace for DNS. You can add as many alternative namespaces under DNS as you require. Then click **OK**.



15 On the Certificate Information page, click **Next**.

16 On the next page, enter a location and a name for the request file and click **Finish**. Note that there is no **Back** option here. If you make a mistake, click **Cancel** and repeat the steps as necessary.



17 Close the MMC.

Obtaining the certificate

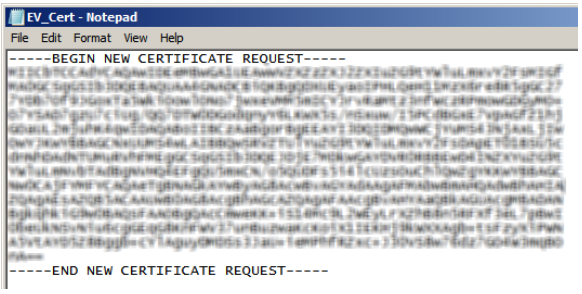
Next, you must use the certificate request file to obtain the certificate.

To obtain the certificate

- Open the request file in a text editor and supply the contents to your certification authority.

  You can get more information about obtaining the certificate from your SSL vendor. They will provide a certificate (`.cer`) file.

  Alternatively, you can obtain a certificate from your own certification authority, using (for example) Microsoft Certificate Services.

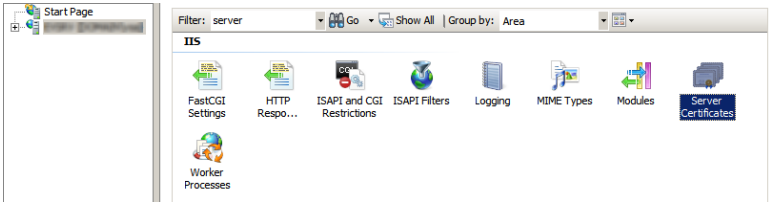


Applying the certificate

Note: When you have completed the procedure "To apply the certificate" in this section, you have installed the SSL certificate and fulfilled the SSL certificate requirements for use of the Enterprise Vault Office Mail App. The steps in the next section, Securing Enterprise Vault web-based communication, are required only if you want to secure all Enterprise Vault web-based communication from now on.

To apply the certificate

1 Open IIS Manager. In the **Connections** pane, select the Enterprise Vault server and then open the **Server Certificates** feature.



2 Click **Complete Certificate Request**.

If the certificate was supplied as a `.pfx` file rather than a `.cer` file, first click **Import** and follow the wizard.

3 Select the certificate (`.cer`) file and click **OK**.

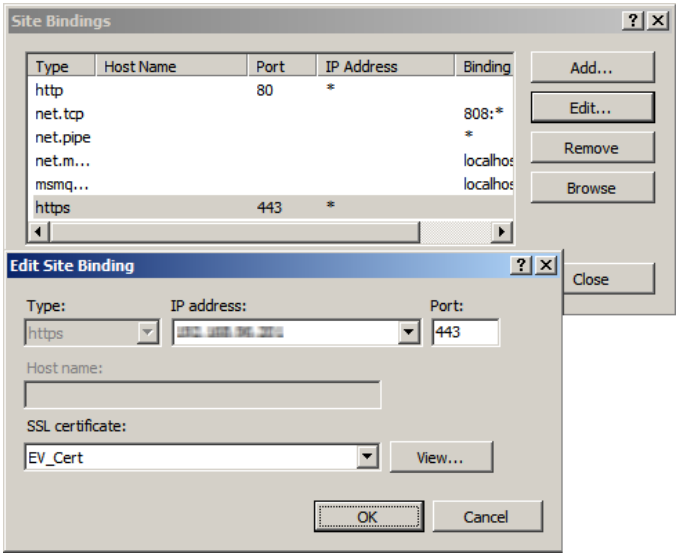
4 In the **Server Certificates** list, check that the certificate has been added.

5 This step assumes that the Default Web Site is in use for Enterprise Vault.

In the **Connections** pane, right-click **Default Web Site** and click **Edit Bindings**. Select **https** port 443 and click **Edit**. If **https** is not in the **Type** list, click **Add** and add **https** from the **Add Site Binding** dialog.

6 In the **Edit Site Binding** dialog, select the SSL certificate from the menu and add it to the required IP address and port.

If the certificate is the only certificate in IIS on this Enterprise Vault server, you can leave the IP address unassigned.



Note: If multiple websites are hosted on the Enterprise Vault server, further planning of IP addresses and port numbers is required. This planning is beyond the scope of this document.

7 Click **OK** on the **Edit Site Binding** dialog and **Close** on the **Site Bindings** dialog, and close IIS Manager.

Securing Enterprise Vault web-based communication

The procedure in this section is required only if you want to secure all connections to all Enterprise Vault web applications in IIS from now on. In particular, the procedure secures all new archive and restore actions, and all search requests. If you do not require this additional configuration, do not follow the procedure.

Effect on existing shortcuts

If you follow all the steps in the procedure, note that existing shortcuts of the following types are not updated with the HTTPS/SSL request path and will no longer work:

- Customized shortcuts
- File System Archiving (FSA) shortcuts
- SharePoint shortcuts

You may therefore want to follow the procedure in two stages when you change from HTTP to HTTPS, as follows:

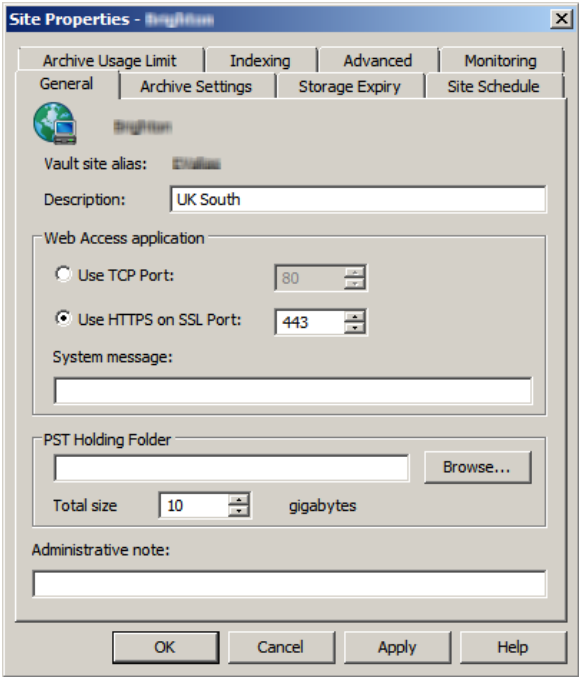
- Run steps 1 to 3 to change the Enterprise Vault site properties so that new shortcuts are created with an HTTPS URL. You must also run step 6 to synchronize mailboxes.
- When existing HTTP shortcuts have expired, run steps 4 and 5 to require SSL and turn off HTTP support. The policy settings for your Enterprise Vault site control the timing of shortcut expiry.

Additional steps for FSA Reporting

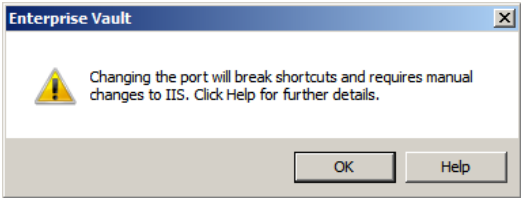
If the Enterprise Vault site uses FSA Reporting, you must perform some additional steps on each Enterprise Vault server and on each file server in the site. Otherwise the status of FSA Reporting is shown as Off in the Administration Console. For details of the additional steps, see "Customizing the port or protocol for the Enterprise Vault Web Access application" in the Enterprise Vault *Administrator's Guide*.

To secure web-based communication

1 Open the Enterprise Vault Administration Console on one Enterprise Vault server, and open the Site Properties.



2 On the General tab, select **Use HTTPS on SSL Port** and specify port 443. When you make the selection, the following warning appears:



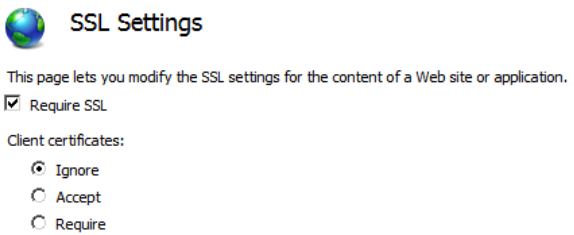
3 To continue with the change, click **OK** on the warning and then click **OK** on the Site Properties.

Note: Before you continue with steps 4 and 5, make sure you have read Effect on existing shortcuts and considered the option to follow this procedure in two stages.

---

4 Open IIS Manager on each Enterprise Vault server to which a certificate has been applied. Select **Default Web Site**. Then under **IIS**, open the **SSL Settings** feature.

5 Select **Require SSL**, then click **Apply** and **OK**.



6 Synchronize all mailboxes that are enabled for Enterprise Vault for these updates to take effect.

Note: Until you complete this step, existing Enterprise Vault users may not be able to access Enterprise Vault facilities.

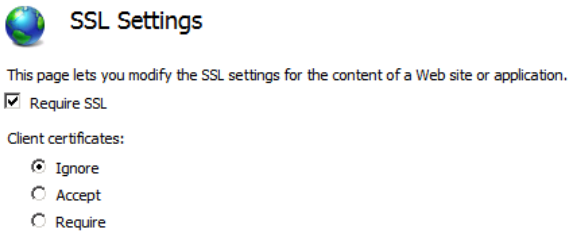
For information on synchronizing mailboxes, see the Enterprise Vault documentation.

Securing Compliance Accelerator and Discovery Accelerator web-based communication

The procedure in this section is required only if you want to secure all connections to all Compliance Accelerator and Discovery Accelerator web applications in IIS.

To secure web-based communication

1. Open IIS Manager and on each Compliance Accelerator and Discovery Accelerator related virtual directory open the **SSL Settings** feature.
2. Select **Require SSL**, then click **Apply** and **OK**.



3. Reset IIS for these updates to take effect.