DOMAIN NAMES & SSL CERTIFICATES

Overview

Vitrium uses 2 different domains depending on what encrypted formats you plan to use:

1. **Web Viewer** – secure web viewer for all content types: documents, images, video, & audio
   - Vitrium's default domain is: https://view.protectedpdf.com/
2. **Protected PDF** – downloadable protected PDF file for documents only (not currently available for VitriumOne customers)
   - Vitrium's default domain is: https://docs.protectedpdf.com

If you wish to customize these domains, you will need to purchase an SSL certificate for one domain or both domains since each type is managed by two different web applications in Microsoft IIS.

Steps Involved to Use Your Own Domain

STEP 1: You should inform Vitrium what domains you will use and fill in these details:

For Web Viewer:	**For Protected PDF:**
Common Name: view.yourdomain.com	Common Name: docs.yourdomain.com
Organization:	Organization:
Organizational unit:	Organizational unit:
City:	City:
State:	State:
Country:	Country:

STEP 2: Vitrium will generate a Certificate Signing Request (CSR) **and send this to you.** If you don't require a Certificate Signing Request (CSR) from Vitrium, skip to Step 3

STEP 3: You can apply the information from the CSR to purchase the SSL certificate. Usually, the SSL provider will have a guide to help you, but Vitrium can help if they don't. You will need to purchase:

- A single multi-domain (SAN) certificate that encompasses both domains (recommended), OR
- Two individual SSL certificates to cover each domain.

STEP 4: You will then need to create CNAME DNS entries for the domains:

For web viewer: CNAME view.yourdomain.com → yourdomain-view.vitrium.com
For PDF: CNAME: pdf.yourdomain.com → yourdomain-docs.vitrium.com

STEP 5: Send the SSL certificate(s) back to Vitrium* (ideally in Microsoft IIS PFX format) via this secure method: https://spaces.hightail.com/uplink/VitriumSystems

*In Step 5, please make sure to include both the certificate and the private key so the certificate chain can be completed on our end. Without the private key on our end, the certificate cannot be used in IIS.

If Vitrium supplied the CSR to you first, then we already have the private key.

If you created the certificate request from within IIS, then the private key only exists on your IIS server and the certificate must be completed there ('Complete Certificate Request' Action in IIS Server Certificates section) and then export it as a .pfx file which will include both certificate and private key.

If you created the request in Linux, then you need to find out where the key is stored and send it to us.

If you have an existing valid certificate in IIS, then it must be exported as a .pfx file as this will include both the certificate and private key.

SSL Certificates Need to be Renewed

Much like domain names registration, SSL certificates expire so they need to be purchased or renewed periodically. The lifespan depends on the certificate reseller (GoDaddy, Namecheap, RapidSSL, etc). Most resellers will have the option to purchase multi-year SSL certificates.

Vitrium recommends a minimum 1-year expiry.

Certificate Providers

Vitrium often recommends using **NameCheap** or **RapidSSL** as a certificate provider as they have a SAN certificate (multi-domain) that can be purchased. For example, the *PositiveSSL Multi-Domain* certificate from NameCheap would work: https://www.namecheap.com/security/ssl-certificates/

Vitrium does not support Lets Encrypt certificates.

About "Subject Alternative Name"

The **Subject Alternative Name** field lets you specify additional host names (sites, IP addresses, common names, etc.) to be protected by a single SSL Certificate, such as a Multi-Domain (SAN) or Extend Validation Multi-Domain Certificate.

Background

The **Subject Alternative Name** extension was part of the X509 certificate standard before 1999, but it wasn't until the launch of Microsoft Exchange Server 2007 that it was commonly used. This change makes good use of Subject Alternative Names by simplifying server configurations. Now Subject Alternative Names are widely used for environments or platforms that need to secure multiple sites (names) across different domains/subdomains.

What Can You Do with Subject Alternative Names?

Secure Host Names on Different Base Domains in One SSL Certificate: A Wildcard Certificate can protect all first-level subdomains on an entire domain, such as **.example.com*. However, a Wildcard Certificate **cannot** protect both www.example.com and www.example.net

Virtual Host Multiple SSL Sites on a Single IP Address: Hosting multiple SSL-enabled sites on a single server typically requires a unique IP address per site, but a Multi-Domain (SAN) Certificate with Subject Alternative Names can solve this problem. Microsoft IIS and Apache are both able to Virtual Host HTTPS sites using Multi-Domain (SAN) Certificates.

Greatly Simplify Your Server's SSL Configuration: Using a Multi-Domain (SAN) Certificate saves you the hassle and time involved in configuring multiple IP addresses on your server, binding each IP address to a different certificate, and trying to piece it all together.

Where Can You See Subject Alternative Names in Action?

To see an example of Subject Alternative Names, in the address bar for this page, click the padlock in your browser to examine our SSL Certificate. In the certificate details, you will find a **Subject Alternative Name** extension that lists both support.vitrium.com and www.support.vitrium.com

In our hosting environment, once your SAN certificate is installed, you will see *docs.xyzcompany.com* and *view.xyzcompany.com* secured by the certificate.

