VITRIUM.COM

Vitrium Security

Customized Domain Names
&
SSL Certificates

Updated: January 20, 2020

1.604.677.1500 (direct)
1.866.403.1500 (toll-free)

www.vitrium.com

Table of Contents

Document Revisions

Date	Reason
2019-10-28	Created revision table
2010-01-30	Added external link to Wikipedia for the CSR definition

Introduction

Vitrium Security provides two (2) content delivery options for secured content: Protected PDF files and secured HTML5 web services. Each type of content in managed by two different web applications in Microsoft Internet Information Services (IIS).

Enterprise customers have the option of using customized domain names for one or both the protected PDF files and/or the Webviewer URLs. An enterprise customer would need to purchase either a single multi-domain (SAN) SSL certificate that encompasses 2 domains (Vitrium preference) or 2 individual certificates, one for each service.

SAN (Subject Alternate Name) certificates are digital security certificates that allow multiple hostnames to be protected by a single certificate.

Examples of registered domain names

Sample company name: Company XYZ:

For Protected PDF's:
Common Name: docs.xyzcompany.com
Organization: XYZ Company Ltd.
Organizational unit: IT
City: Vancouver
State: British Columbia
Country: CA

For Secured Webviewer:
Common Name: view.xyzcompany.com
Organization: XYZ Company Ltd.
Organizational unit: IT
City: Vancouver
State: British Columbia
Country: CA

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

In order to minimize ongoing maintenance, a minimum of a 1-year expiry is required.

NOTE: Vitrium does not support Lets Encrypt certificates.

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

DNS Name: docs.xyzcompany.com
DNS Name: view.xyzcompany.com

What needs to be done

- Vitrium will generate a Certificate Signing Request (CSR) and send to you
- SSL certificate must be purchased and then the certificate request from the step above needs to be applied
- Usually the SSL provider will have a guide as to what you must do to get the certificate completed, if not then Vitrium should be able to help
- You will create CNAME DNS entries for the domains:

  Example CNAME: docs.xyzcompany.com -> xyzcompany-docs.vitrium.com
  Example CNAME: view.xyzcompany.com -> xyzcompany-view.vitrium.com

If you are able to send SSL cert(s) in Microsoft IIS PFX format that would be perfect. If not, 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 in the first step 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 exported as a .pfx file which will include both certificate and private key. If you created the request in Linux then determine where the key is stored and send it along.

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

When you receive the certificate you may upload it to us by using the following secured link: https://spaces.hightail.com/uplink/VitriumSystems

Please contact Vitrium Support (support@vitrium.com) with any questions or concerns that you may have.

The Subject Alternative Name Field Explained

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 a 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.