Datasheet - Sitekit CMS and HTTPS

Document Control	
Registered Office	Sitekit Ltd Sitekit House Broom Place Portree Isle of Skye IV51 9HL
Business Unit	Sitekit.Solutions
Role	Support-Services
Document Type	Manual
Document Author	David Morgan
Document Checked by	Chris Reynolds
Date Checked	17/05/2013
Document Title	Sitekit CMS and HTTPS
Document ID	SKDOC-11-915
Document Version	2.4
Approved Document Version	2.0
Document Approver	David Morgan
Document Status	Approved
Creation Date	15/07/2013
Last Modified Date	20/02/2017
Next Review Date	14/02/2014
Audience	Client
Publisher Rights	© Sitekit Ltd 2013
This document is uncontrolled when printed	

Site visitors and administrators both require a degree of security when accessing a web site. Administrators obviously need to protect their passwords. Visitors often expect security when they submit information to a site – the more important the information, the more likely they are to expect HTTPS protection.

Sitekit CMS offers automatic protection for Administrators. Passwords are always entered via HTTPS.

HTTPS protection for site visitors is made available by a flexible system of options. This document describes those options.

Admin Login Security

When you sign on to Sitekit Admin, the connection is always secured via HTTPS admin sessions are HTTPS throughout (from 11.0 onward)

Visitor and Extranet Security

When front end visitors submit information to your site, the use of an HTTPS connection reassures them that the information they are entering is properly secure. The three main areas in which you might choose to use HTTPS to provide this extra security for your site are listed below.

1. Extranet login Screen. By default this is not protected by an HTTPS connection, but optionally HTTPS can be applied to the extranet login, again in a gatekeeper capacity, as with Admin login.

2. Any page on your site that you want to make secure – pages containing forms are obvious choices.

> Options 1 and 2 above require the use of an SSL Certificate. On a hosted site, you can do this in two ways. Firstly, you can share the Sitekit Admin Certificate. This is free of charge. But visitors to your site will see an address similar to **https://secure.sitekit.net** in their address bar, which they may find off-putting.
>
> Alternatively, a hosted site can share the Sitekit EV (Extended Validation) SSL Certificate. This is available as an optional extra from Sitekit. In this case visitors to your site will only see your site name – there's no mention of Sitekit.
>
> On a deployed site, the client can either share the FOC Sitekit Admin SSL Certificate (which has the disadvantage of displaying something like **https://secure.sitekit.net** in a visitor's address bar), or they may purchase their own SSL Certificate, which will display only their own site name. Sitekit have considerable experience with SSL certificates, and can purchase an SSL certificate on the client's behalf, if desired.

3. Sitekit Secure Forms. These are doubly secure. First they employ HTTPS between the visitor's browser and your website form. Secondly they encrypt the submitted data, preventing anyone – even Sitekit Administrators – from seeing the data, unless they hold the decryption key. See the Sitekit Secure Forms Datasheet for more information.

Extranet Login Screen

If you have a SSL Certificate – either your own, or a shared Sitekit certificate - it is advisable protect this screen using an HTTPS connection, to prevent hackers from using a sniffer to read your Extranet login details. Sitekit configure this on request.

Secure Pages

When visitors submit information to your site, the use of an HTTPS connection reassures them that the information they are entering is properly secure. It is essential that you check your organization's Information Security Policy, to see if HTTPS is required for submitted data.

If you have a SSL Certificate, then you can protect any page on your site, including forms, forums, guest books, resources – anything you want, via the HTTPS protocol. If you wished, you could make the entire site HTTPS.

The two tables below summarise the availability of HTTPS security options for your site. The first table is for Shared Hosting sites, and the second is for Deployed Hosting sites.

	Shared Hosting			
	SSL enabled by default	Sitekit shared EV SSL option available	Ability to use own SSL Certificate	Use shared Sitekit Admin SSL Certificate (FOC)
Admin Login	Yes	Not needed	Not needed	Automatic
Extranet Login	No	Yes	No	Yes
Secure Pages (including forms)	No	Yes	No	Yes
Sitekit Secure Forms	No	Yes	No	Yes

	Deployed Hosting		
	SSL enabled by default	Option to use deployed Sitekit.net admin certificate	Ability to use own SSL Certificate
Admin Login	Yes	Automatic	N/A
Extranet Login	No	Yes	Yes
Secure Pages (including forms)	No	Yes	Yes
Sitekit Secure Forms	No	Yes	Yes

Definition of Terms used in the Tables

SSL means Secure Socket Layer. Transmissions using SSL are encrypted meaning the data is not readable if it is intercepted. The protocol used is https.

Sitekit SSL shared EV SSL Option Available: This means that Sitekit's own EV SSL certificate can be configured to include the client's Domain.

Sitekit Admin shared SSL Certificate (FOC): You can use the shared Sitekit Admin Certificate to provide security. This has the advantage that it's FOC. It has the disadvantage that the HTTPS address will feature **Sitekit.net** as part of the address. Some visitors to your site might be put off by having an HTTPS address different from your site name.

SSL Enabled by default: This means the corresponding feature automatically uses SSL "out of the box". For both Hosted and Deployed sites, Sitekit automatically apply an SSL certificate to Admin logins to ensure these transmissions are secure.

Ability to use own SSL certificate: If this option is available a client can purchase and install their own third party certificate for a corresponding domain. You can purchase your own, or ask Sitekit to obtain a certificate on your behalf. There are a range of certificates available.

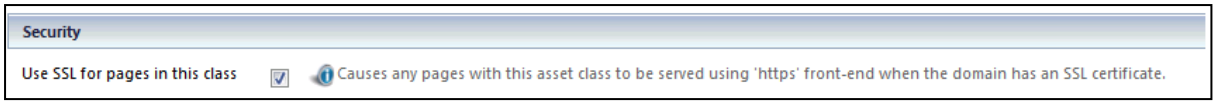
The default Cypher Strength is 256 bit for certificates purchased by Sitekit solutions, although in a deployed scenario the cypher strength used depends on web server configuration and the type of certificate purchased.

It is ***not*** possible for Sitekit to install a third party certificate on any of our shared hosting environments. Instead, you ask Sitekit to add your domain to the Sitekit EV SSL Certificate. This option is chargeable.

Using Secure Pages with an SSL Certificate

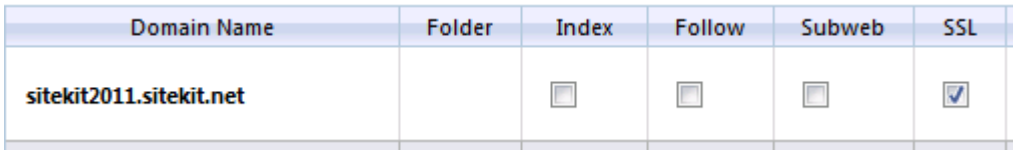
Once you have SSL active on your site, you can add HTTPS to any page you desire. The process is straightforward – you simply turn on SSL Security in the Asset Class which owns the page(s) you wish to make secure.

Right click on the Asset Class and select **Permissions>>Edit Permissions**, then tick the box labelled **Use SSL for Pages in this class**.



Applying SSL Security to Asset Classes is the easiest and quickest way to apply security. You could, for example, make all the Forms on your site belong to a single secure Asset Class, so that any new form created would automatically inherit SSL protection.

Note: You must have SSL turned on in the Configure Domain screen to use your SSL Certificate, as shown in the graphic below.



HTTPS encryption only applies between the browser and the web site, so the data stored in forms on your website can be read by your admin staff as plain text.