



WHITE PAPER

---

# EV Upgrader: Enabling Windows XP Clients for Extended Validation



Where it all comes together.™



**CONTENTS**

+ The Windows XP Functionality Gap	3
+ What EV Upgrader Does to Trigger Root Installation	4
+ How Best to Use EV Upgrader	5



Extended Validation SSL Certificates offer online businesses the opportunity to demonstrate their genuine identity to site visitors. By doing so they can maximize visitor confidence and increase the total amount of business on the site. In order to ensure that the most possible site visitors are able to observe that the site has passed Extended Validation (EV) authentication and enjoy the increased confidence that accompanies this knowledge, VeriSign has created VeriSign® EV Upgrader™—the first-ever solution to enable all visiting Windows® Internet Explorer® 7 (IE7) browsers to detect EV SSL Certificates and display them appropriately.

EV Upgrader is a server-side application that prompts visiting IE7 systems to update their VeriSign® SSL Certificate roots. Microsoft specifically engineered Internet Explorer to allow root updates of this nature, and therefore the update is virtually instantaneous and undetectable to the site visitor. The only change the user sees is the display of green address bars and other EV interface conventions when visiting sites that have VeriSign EV certificates.

To make using EV Upgrader as easy as possible for site administrators, VeriSign has built it right into the VeriSign Secured Seal™. That means all you have to do to maximize consumer confidence in your EV-authenticated site is install the VeriSign Secured Seal. Installation takes minutes, and no additional administration is required. The VeriSign Secured Seal even gains this functionality automatically on existing sites, so if your site already has the VeriSign Secured Seal, you don't need to do a thing.

VeriSign signs EV certificates with a non-EV intermediate root to ensure full coverage for your site on legacy browsers. In order to enable EV functionality and behavior, VeriSign signs EV certificates with a new EV root as well. This innovative design makes possible a single SSL Certificate that offers the same comprehensive browser ubiquity as traditional VeriSign SSL Certificates and still enables EV functionality on the broadest possible set of IE7 client systems.

This white paper details the behavior of EV Upgrader and how it triggers root installation in Windows XP operating systems. A companion white paper, *Maximizing Site Visitor Trust Using Extended Validation SSL*, details the basic behavior and interface conventions of EV SSL Certificates.

## The Windows XP Functionality Gap

---

Microsoft created the Windows Vista™ operating system with the intention that it would work in conjunction with IE7 to automatically and seamlessly provide root updates. In the case of your EV SSL Certificate, that's exactly what the operating system does. Whether or not you install the VeriSign Secured Seal with EV Upgrader on your site, all clients using Windows Vista will have the ability to recognize EV certificates on your site. However, Microsoft engineered and released the Windows XP operating system long before the existence of EV SSL, so Windows XP lacks the ability to undergo this root installation in the absence of a specific event that will trigger update. Therefore, IE7 running on the Windows XP operating system requires prompting to download and add a new EV root. This prompt occurs when the browser attempts to connect with a Web site protected by an SSL Certificate that uses a root it does not recognize. At that point

the IE7 browser contacts a separate root store service maintained by Microsoft and downloads the root in question. It does not download all roots in the store but only the requested root. This functionality is a deliberate operating system behavior added specifically to enable scenarios such as this one.

## What EV Upgrader Does to Trigger Root Installation

EV Upgrader operates on a very simple principle. The site containing an EV SSL Certificate from VeriSign adds an invisible JavaScript™ link to one or more of its pages. This link initiates a connection with a specific Web site that VeriSign has set up explicitly for this purpose. The address of that domain is <https://extended-validation-ssl.verisign.com>, and if you access it by typing that address into any Web browser, you'll simply see explanatory information on EV SSL Certificates.

What you don't see is that this site contains an SSL Certificate that chains up only to the new VeriSign EV root. This fact is exhibited in the behavior of pre-EV browsers, which will warn the user of the presence of an untrusted root should they access the site. When an IE7 browser connects with this page, it automatically downloads and installs this new root from the Microsoft® Root Store. The browser installs only the root required by the site to which it's connecting and no other roots.

We can't, however, rely on every IE7 user to visit a Web page that VeriSign has set up unbeknownst to them. Instead, your own Web site can cause this access to happen in the background, invisibly to the user. This functionality once again is a standard part of browser behavior, and in fact a great many sites use a variant of it whereby they assemble the components for display on the site from a variety of different sources. This technique is particularly popular with graphic content (like the photograph of a product on a retail site) and online advertisements. In the case of EV authentication, the site does not need to retrieve any content; however, it still accesses a page protected with what may be a new root for the visiting client, and if this root is indeed new, the client automatically performs an update.

Certainly it would be possible for sites to install this JavaScript prompt directly onto their own pages. However, VeriSign makes it as easy as possible for online businesses to gain the full benefit of their EV certificates by building the functionality directly into the VeriSign Secured Seal. That means by simply installing the VeriSign Secured Seal on your Web site, you automatically add EV Upgrader and subsequently trigger root installation on all eligible client systems. Even if your site had the VeriSign Secured Seal before the creation of EV certificates, it is still enabled with EV Upgrader. Therefore, you won't have to update to a new version of the seal to realize the full potential of your EV SSL Certificates.



*The VeriSign Secured Seal initiates root update through a background connection to a designated root update site.*

The VeriSign Secured Seal itself works on the principle described above. When a site installs the VeriSign Secured Seal, it is actually installing a JavaScript file. With every site visit, this file requests a seal image or animated graphic from a service maintained by VeriSign, which then serves up the requested file to the client system for display. This architecture has several advantages, the most significant of which is it enables VeriSign to monitor and control the use of the VeriSign Secured Seal and to limit its use to legitimate sites. A second advantage is that VeriSign is able to create improvements to the seal such as the addition of EV Upgrader and make those improvements available to all seal-posting sites without requiring any additional effort on the part of site administrators.

When the site requests the image of the VeriSign Secured Seal from VeriSign's seal service, it also makes a request to <https://extended-validation-ssl.verisign.com>. As described above, this request triggers the browser to download and install the new root. From this moment forward, the client system in question is populated with this new EV root and can use that root for any site employing a VeriSign EV SSL certificate. EV Upgrader does not install any other roots into the browser apart from the EV root for that particular certificate.

## How Best to Use EV Upgrader

Companies that use EV SSL Certificates on their Web sites have the potential to improve a visitor's confidence and increase that visitor's propensity to do business online. These companies are therefore well motivated to trigger an update in advance of the first appearance of the EV root. Because the browser reads the SSL Certificate on any given page before it displays the page's contents, the first time a client receives the prompt to download the VeriSign EV root, the green address bar will not display for that specific page on that specific occasion. The next time this client visits a page with this same EV root (including on the same site as soon as one click later), the browser displays the SSL Certificate as an EV certificate.

Fortunately, sites are not limited to displaying the VeriSign Secured Seal only on the pages for which they have implemented SSL Certificates. In fact, you can display this seal on pages earlier in the visitor's path than those on which the SSL Certificate page appears. So if your site has an EV certificate at [secure.\[sitename\].com](https://secure.[sitename].com), and you'd like to ensure root availability on Windows XP systems before accessing this page, it's quite practical to add the VeriSign Secured Seal to [www.\[sitename\].com](https://www.[sitename].com). In this scenario the Windows XP user will receive a root installation upon visiting the site's home page. It doesn't matter that the site does not have an SSL Certificate enabled on the home page. All it needs is the VeriSign Secured Seal. In this case the VeriSign Secured Seal prompts a background root installation on [www.\[sitename\].com](https://www.[sitename].com), and by the time the user actually clicks through to [secure.\[sitename\].com](https://secure.[sitename].com), the browser already is able to view EV certificates correctly.

One particular advantage of this technology architecture is that the pages on which a site should display the VeriSign Secured Seal for root update are the best places to include it for increasing overall site visitor confidence as well. In a typical online retail scenario, the

page with the most abandonment is the home page, followed second by the page immediately preceding the checkout process. Therefore, these are the two pages from which a site will derive the most benefit by posting the VeriSign Secured Seal. They're also the two most useful places to initiate a root update. The home page is the most-visited page for most sites, so it's an ideal place to display a seal and cause most site visitors to have their roots updated. By installing the VeriSign Secured Seal on the home page and all pages that provide access to the SSL-enabled pages, most sites can rely on enabling the overwhelming majority of their Windows XP-using visitors before they ever display an EV certificate.

Research indicates that displaying the VeriSign Secured Seal can be expected to positively affect a site visitor's likelihood to perform transactions on your site. Leading European travel company Opodo tested a set of identical online order pages with and without the VeriSign Secured Seal and found that the pages with the seal received a 10 percent uplift in sales over those without it. Said Warren Jonas, Opodo's head of service management, "We immediately realized the impact that the trust factor can have on shopping basket abandonment rates and we have since published the VeriSign seal on all the payment pages across our network of European sites." Furthermore, in the summer of 2006, prominent market research firm TNS studied online shoppers' reactions to a variety of online security seals and determined that the VeriSign Secured Seal is far and away the world's most recognized online trust mark. The research indicates that 56 percent of worldwide online shoppers recognize the VeriSign Secured Seal—a percentage eight times greater than the next most-recognized SSL trust mark.

To learn more about VeriSign EV certificates or to purchase them for your site, see <http://www.verisign.com/ssl/index.html>. VeriSign also has provided a white paper on EV general functionality, titled *Maximizing Site Visitor Trust Using Extended Validation SSL*. To learn more about the VeriSign Secured Seal or to download the seal for installation on your site, see <http://www.verisign.com/ssl/secured-seal/index.html>.