FAQs About nsProtect™ Secure Extended Validation (EV) SSL Certificates

Q: What is an Extended Validation SSL Certificate?

A: Extended Validation is a level of high-assurance security authentication for SSL Certificates that was introduced in early 2007. It takes advantage of advanced features in next-generation browsers such as Microsoft® Internet Explorer® v7, and also benefits from being the first truly standardized authentication protocol ever developed for SSL Certificates.

Q: How was Extended Validation developed?

A: Awareness of the need to increase the level of security and consumer confidence in online transactions led a group of leading Web browser vendors and SSL Certificate issuers (called Certification Authorities) to form the Certification Authority/Browser (CA/B) Forum. Network Solutions® and the rest of the CA/B Forum members assembled and agreed upon both technical and procedural specifications for the new class of "high assurance" certificates.

Q: How do the certificate validation procedures for Extended Validation differ from those of existing certificates?

A: The application process for receiving an Extended Validation Certificate from one of the recognized Certification Authorities, such as Network Solutions, is both deeper and more thorough than existing certificate-issuance procedures. Companies applying for Extended Validation SSL Certificates will be required to provide far more detailed information about their business, their Articles of Incorporation, and so on. Validation and confirmation of this additional data is expected to both enhance the authority of and consumer confidence in the certificates and also, crucially, to make it all but impossible for fraudulent or criminal applicants to receive a certificate.

Q: How does the Extended Validation SSL Certificates' appearance differ from that of existing types of SSL Certificates?

A: The most obvious difference to consumers will appear in the navigation window of next-generation Web browsers, such as Microsoft Internet Explorer® v7. In addition to displaying a closed padlock image and "https" Web address prefix, the navigation window will turn green to signify a Web site secured by an authentic, Extended Validation SSL Certificate. Web sites secured by other types of legitimate SSL Certificates will continue to display both the closed padlock image and "https" prefix, but they will not display a green navigation window in next-generation Web browsers.

Q: Will it take longer for me to apply for and receive an Extended Validation SSL Certificate for my business than it does for existing certificates?

A: Yes. Because of the amount of information that applicants must supply to Certification Authorities and the amount of time required to verify that information, the application process will probably take 4 to 5 business days.

Q: Who can apply for an Extended Validation certificate?

A: EV SSL certificates are now available to corporations, business entities (such as sole proprietors, general partnerships, unincorporated associations, etc.) and government entities.

Q: Why do Extended Validation SSL Certificates cost more than other certificates?

A: Extended Validation SSL Certificates cost more than other types of SSL Certificates because of the extensive amount of additional verification activity that must be conducted before issuing the Certificate.

Q: Will my current Network Solutions SSL Certificates remain "good" after Extended Validation SSL Certificates are introduced?

A: Yes. Network Solutions will continue to offer, support, and authenticate its current Basic, Advanced, and Wildcard SSL Certificates. If your business is not eligible for an EV SSL Certificate because it is a non-corporate entity, then your existing Network Solutions SSL Certificate will continue to meet your needs and those of your customers for some time to come. If your business is incorporated and you choose to upgrade from your existing Network Solutions SSL Certificate to our EV SSL Certificate, contact Customer Support to learn about promotional offers available to our existing customers designed to preserve your investment in Network Solutions SSL Certificate services.

Q: Will my customers using Microsoft® Internet Explorer® 7 and other next-generation browsers still be able to view my current SSL Certificates?

A: Yes. Next-generation browsers support, recognize, and adhere to existing SSL Certificate standards.

Q: What information will I need to provide to Network Solutions in order to receive my EV SSL Certificate?

A: Before your EV SSL Certificate can be issued, Network Solutions must verify your legal, operational and physical existence. We must also confirm that you are authorized to apply for an EV SSL Certificate on behalf of your organization and that your organization is the registrant of the domain to which you are applying the EV SSL Certificate. When verifying the information that you supply to us, we will use such sources as government registries for your jurisdiction of incorporation, corporate registry systems like Dun & Bradstreet, letters from your Attorney or Certified Public Accountant, bank account information, and information from other directory sources like WHOIS and the Yellow Pages. On occasion, a site visit may be required to verify the information that you have supplied.

Q: Why can't I get a Wildcard EV SSL Certificate?

A: EV SSL Certificates provide a higher level of assurance than older and existing types of SSL Certificates. In order to ensure that EV SSL Certificates are not issued fraudulently or misused after issuance, the CA/B Forum decided to require that issuing CAs validate the legitimacy of each and every Web address to which an EV SSL Certificate is assigned. Therefore, the Forum's EV guidelines prohibit the issuance of "Wildcard" EV SSL Certificates for Web addresses such as "*.networksolutions.com.

Q: Why are EV Certificates limited to one- and two-year terms only?

A: In an effort to ensure that EV SSL Certificates provide the highest level of security, the CA/B Forum, which is responsible for establishing the guidelines for issuing EV SSL Certificates, decided that the information provided by EV recipients should be validated more frequently than that supplied by recipients of other types of SSL Certificates. Therefore, they limited the maximum lifetime of an EV SSL Certificate to no more than twenty-seven (27) months.

Q: I have installed Microsoft® Internet Explorer® 7. Why doesn't my browser address window turn green when I visit Web sites protected by EV SSL Certificates?

A: The Microsoft® Internet Explorer® v7 browser was launched before EV SSL Certificates became available, so you may need to update your browser's list of Trusted Root Certification Authorities. If you are using Internet Explorer® v7 on the Microsoft Windows Vista® operating system, your Trusted Roots will be updated automatically. If you are using Internet Explorer® v7 on the Microsoft Windows XP® operating system, you will need to update your Trusted Root Certification Authorities list manually.

For other questions about Network Solutions' nsProtect™ Extended Validation SSL Certificates, please contact us at premiersupport@networksolutions.com or 1-877-228-1023.