FAQs About nsProtect™ Secure SSL Certificates

GENERAL QUESTIONS

What is SSL?

SSL stands for **S**ecure **S**ockets **L**ayer, which is the standard security technology for creating an encrypted link between a web server and a browser. This link ensures that all data passed between the Web server and browser remains private and secure. All nsProtect™ Secure SSL certificates from Network Solutions are encrypted up to 256 bits, which is the highest encryption level available. Your site visitors will know they have created an SSL link with your Web server by seeing the "https://" at the beginning of the URL, as well as seeing the padlock icon in the frame in their Web browser.

What are the steps in being issued an SSL certificate from Network Solutions®?

There are four steps to being issued an SSL Certificate from Network Solutions®:

1. Create your CSR
2. Select your SSL Certificate
3. Validation of your organization
4. Install your certificate

Do all nsProtect™ Secure SSL certificates support 256-bit encryption?

Yes, all nsProtect Secure SSL certificates from Network Solutions are encrypted up to 256 bits. Additionally, nsProtect Secure SSL certificates also support lesser encryption levels as determined by the Web server or browser, in other words, if the Web server or browser is configured to only support 40 or 56-bit encryption, then a secure session can still be established at that encryption level.

Why is 256-bit encryption important?

256-bit encryption means that the data cryptographically encoded during an SSL session is at the strongest level available, and nearly impossible to break. Compared to a 40-bit encrypted SSL certificate, a 256-bit is more than 300 septillion (300,000,000,000,000,000,000,000,000) times stronger.

What is the browser recognition for nsProtect™ Secure SSL certificates?

Making sure your SSL certificate is recognized by almost all browsers is a key element when choosing an SSL provider.

Network Solutions® nsProtect Secure SSL certificates are trusted by over 99% of the browsers used on the Internet today, including:

- Microsoft Internet Explorer® 5.01+
- Mozilla Firefox® 1.0+
- Mozilla 0.6+
- Google™ Chrome
- KDE® Konqueror
- Netscape® 4.77 +
- Opera 7.0+
- Apple® Safari 1.2 +
- Camino® 1.0+
- AOL® 5+

What is the validation process for Network Solutions® security services?

Network Solutions follows a comprehensive validation process to ensure that your certificate is properly issued. It's a 4-step process that is expedited within 1 business day with the purchase of an nsProtect Secure Advanced or Wildcard certificate, and 2-4 business days with the purchase of the nsProtect Secure Basic certificate and Assured Site Seal.

How is nsProtect Secure Wildcard different from the other nsProtect Secure SSL certificates?

The nsProtect Secure Wildcard is ideal for anyone that needs an unlimited number of SSL certificates from a single domain name (such as secure.networksolutions.com, www.networksolutions.com, etc.), whereas nsProtect Secure Basic and nsProtect Secure Advanced certificates are issued to one single host name (such as secure.networksolutions.com).

My company is not incorporated, can I still apply for an SSL certificate?

Yes, you may still apply for an SSL certificate if you are not an incorporated company. You will need to provide Network Solutions different documentation during your validation process than an incorporated organization.

APPLICATION IN PROGRESS

How do I generate my CSR?

If you are using shared web hosting services with another provider, you must contact their technical support to have them generate a CSR for you. If you are using your own server, please see our instructions for generating a CSR.

How long will it take to receive my nsProtect Secure SSL certificate?

Upon receipt of all applicable documentation, your SSL certificate is issued within 1 business day with the purchase of an nsProtect Secure Advanced or Wildcard certificate, and 2-4 business days with the purchase of the nsProtect Secure Basic certificate or Assured Site Seal.

How can I check the status of my order?

You can e-mail us 24 hours a day, 7 days a week at **premiersupport@networksolutions.com**. Be sure to include your order number in your e-mail and our support team can assist you. Or, you can call us at **1-877-228-1023.**

What should I do if I have made a mistake in my application?

Due to the high level of security required for the issuance of SSL certificates, you will likely need to create a new order, which includes creating a new CSR. Please contact SSL Support at **premiersupport@networksolutions.com** or **1-877-228-1023** to discuss your order.

What do I put in the Common Name field when I generate my CSR?

Use the domain name you wish to have the SSL certificate issued to in the Common Name field when generating your CSR. Do not include the "http://" when entering the domain name, nor any slashes with subfolders after the domain name.

I selected the wrong web server on the order form when I ordered my SSL certificate, do I need to cancel my order and re-apply?

No. The web server field on the order form is stored in your account so that we may better serve you if you have any support questions. It is important, however, that you select the correct web server when generating your CSR and for installation instructions.

If I change my server or move to a different hosting provider, can I move the certificate?

For security reasons, you will need to have your SSL certificate reissued in these instances. You will need to create a new CSR, and then go to your SSL Manager and follow the instructions to re-issue an SSL certificate. Please contact SSL Support at **premiersupport@networksolutions.com** or **1-877-228-1023** for assistance.

Some details have changed since my last order, how do I get these updated?

All account changes should be sent to **premiersupport@networksolutions.com**.

If I renew my SSL certificate within 60 days of my certificate expiring, do I "carry over" my unused term?

Yes. The expiration date of your renewed certificate will reflect the unused days from your previous term if you renew within 60 days of your renewal. Please note that during the renewal process you will require a new CSR.

If I have accidentally deleted my "private key", what should I do now?

First check your backups and see if you can re-install the "private key". If you don't know how to re-install the key from your backups, then contact your system administrator or your web server software vendor for technical support. Another course of action is to have the certificate reissued. You will need to create a new CSR, and then go to your SSL Account Manager. Look up the certificate information under Manager Customer and follow the instructions to reissue an SSL certificate. Please contact SSL Support at **premiersupport@networksolutions.com** or **1-877-228-1023** if you need assistance.

Why does the web site say the SSL certificate is 'Untrusted'?

The likely cause is the Network Solutions® intermediate certificate has not been loaded. Please visit our SSL certificate installation instructions section to confirm that your certificate has been properly installed.

Why does the secure part of the web site say the name on the security certificate is invalid or does not match the name of the site?

In most cases, this is caused by the SSL certificate having a Common Name that is different from the web site's SSL configuration. For example, the SSL certificate's Common Name is secure.netsolssl.com and the web site has been configured so the secure section of the web site is using a Common Name of www.netsolssl.com.

When trying to go to my site using https in my URL, it displays the message "The page cannot be displayed." What causes this?

This is usually caused by port 443 not allowed through firewall or by the SSL certificate not having a corresponding key file.