

# Secure Outlook Web Access using SSL

Outlook Web Access (OWA) has become a very important component of Exchange. Many companies deploy OWA to allow users the ability to access email almost anywhere. The content in this article is how to deploy OWA to make it more secure with Secure Socket

**In this article we will look at how to secure OWA access using Secure Socket Layers (SSL) .**

## Secure Outlook Web Access 2000 using SSL

Outlook Web Access (OWA) has become a very important component of Exchange. Many companies deploy OWA to allow users the ability to access email almost anywhere.

The content in this article is how to deploy OWA to make it safer with Secure Socket Layers (SSL). We will use Instant SSL (<http://www.instantssl.com/>) as a trusted third-party organization. You can create your own certificate using Microsoft Certificate Server.

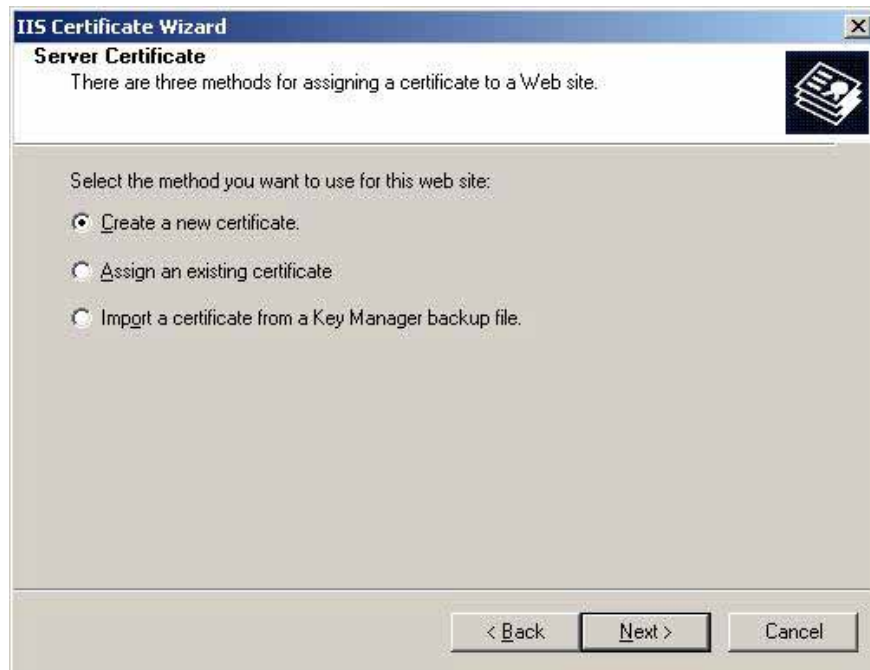
InstantSSL offers many different packages depending on price and aggregate level. You should check their website for the latest price and which version to use.

1. Use Internet Services Manager.
2. Right-click on the website that has your OWA component (written by default as "Default Web Site") and open its properties (Properties).

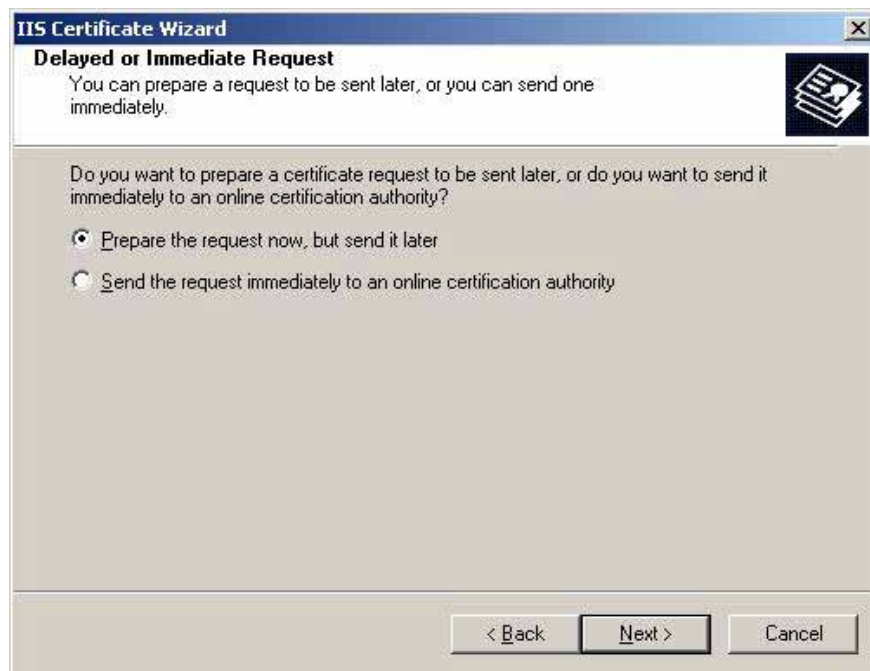


3. Select " *Directory Security* " and click on " *Server Certificates* ". "The *Certificates Wizard Web Server* " appears, click Next.

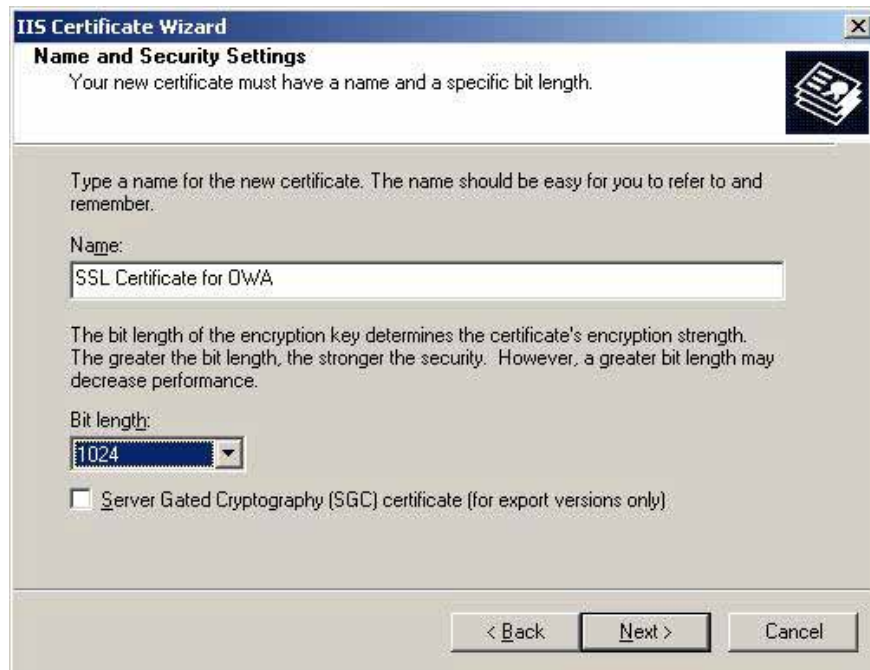
4. On the " *Server Certificate* " dialog box (below), we will select " *Create new certificate* ", click Next.



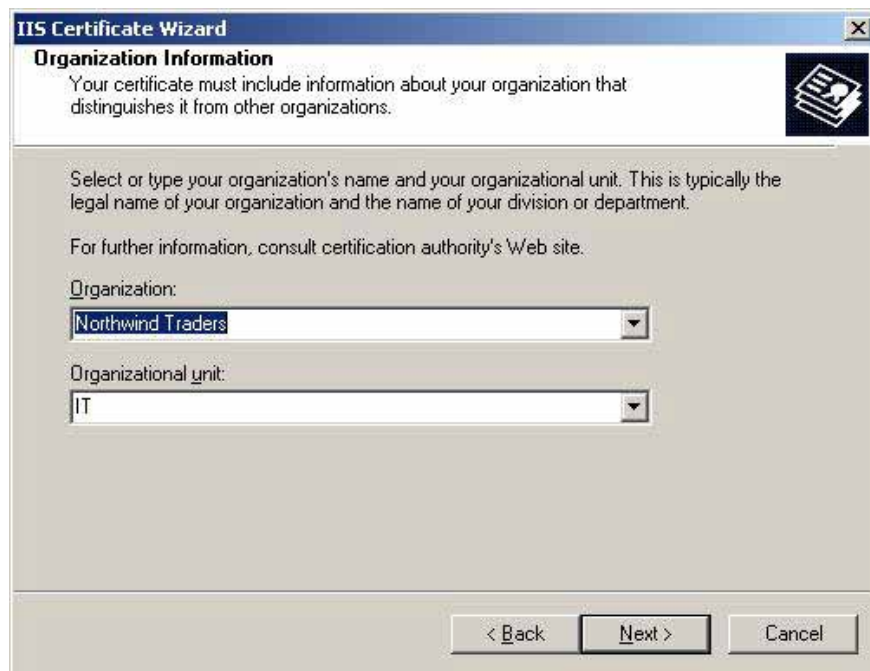
5. In the " *Delayed or Immediate Request* " dialog box (below), select " *Prepare the request now, but send it later* ". We will send a certificate request to a third group, in this case InstanSSL. Click Next.



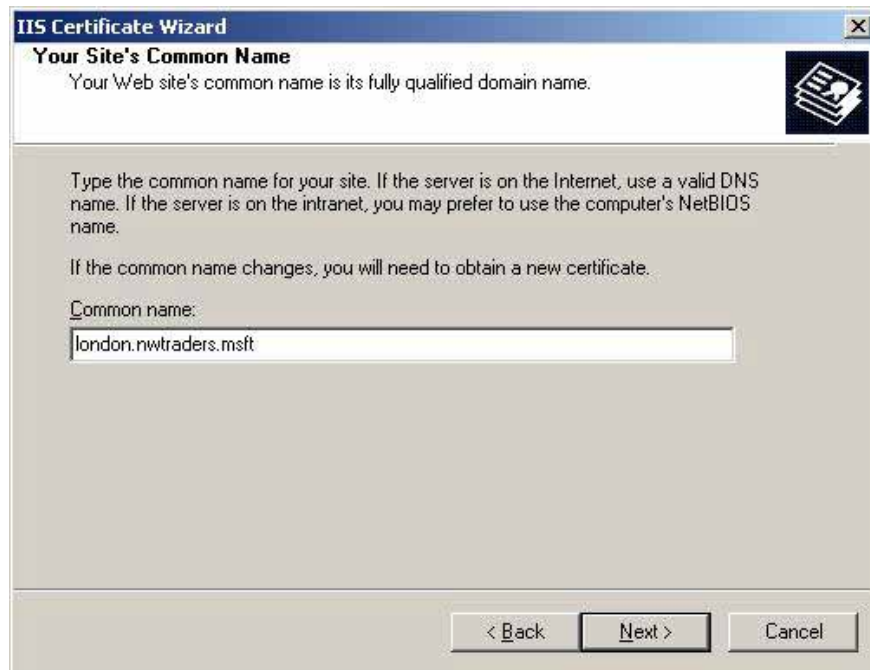
6. The " *Name and Security Settings* " dialog box appears (below). Provide a name for our new certificate and select the level of security to use (you should not choose to exceed 1024 because it will cause a harmful effect on your server). Click Next.



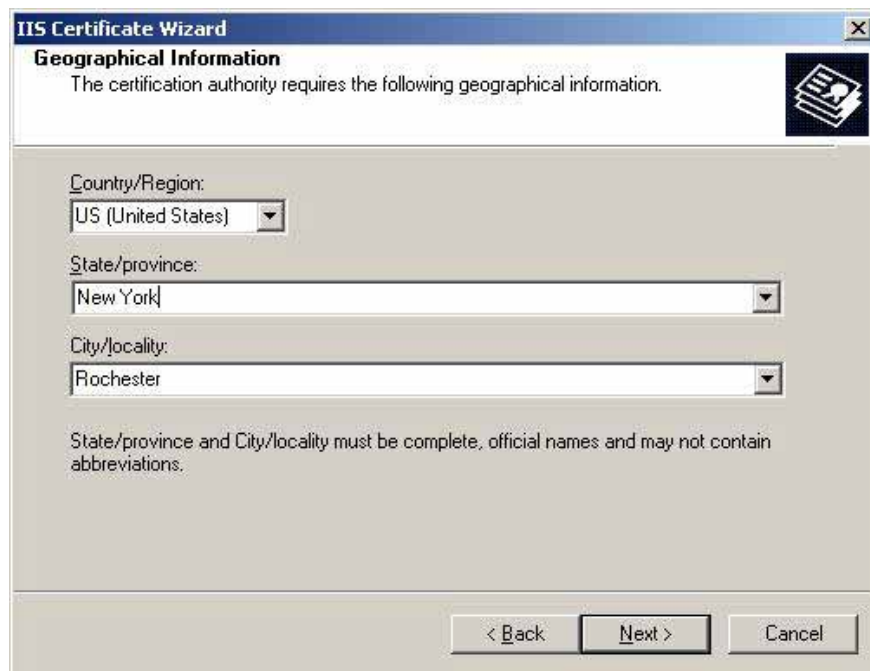
7. The " *Organization Information* " dialog box (below) requires entering an organization name. This is the name that will appear in the legal documents because it is also the name that appears in your certificate. This organizational unit can be an area, office or business unit in your company.



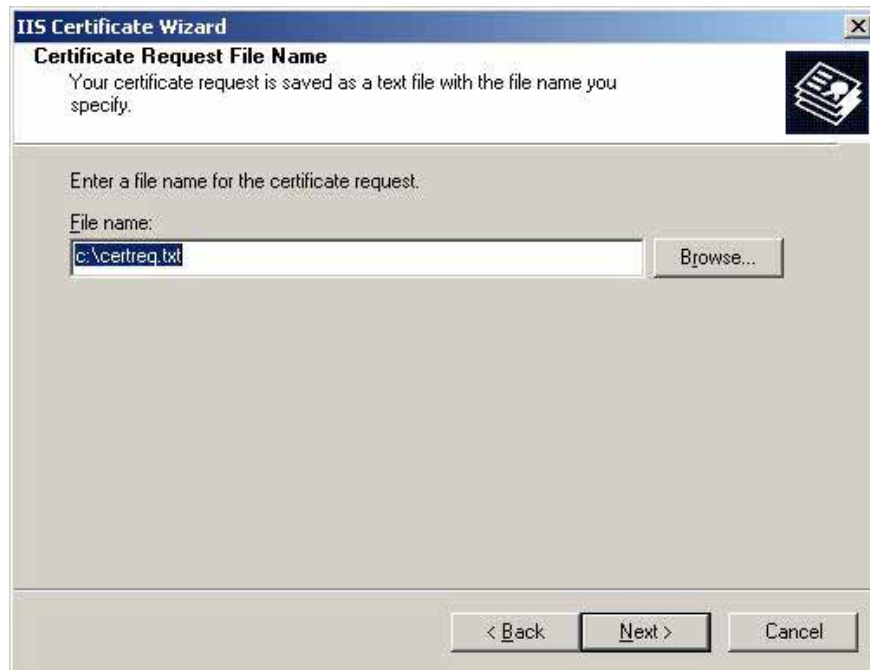
8. In the " *Your Site's Common Name* " dialog box (below), we must enter the FQDN of the web server.



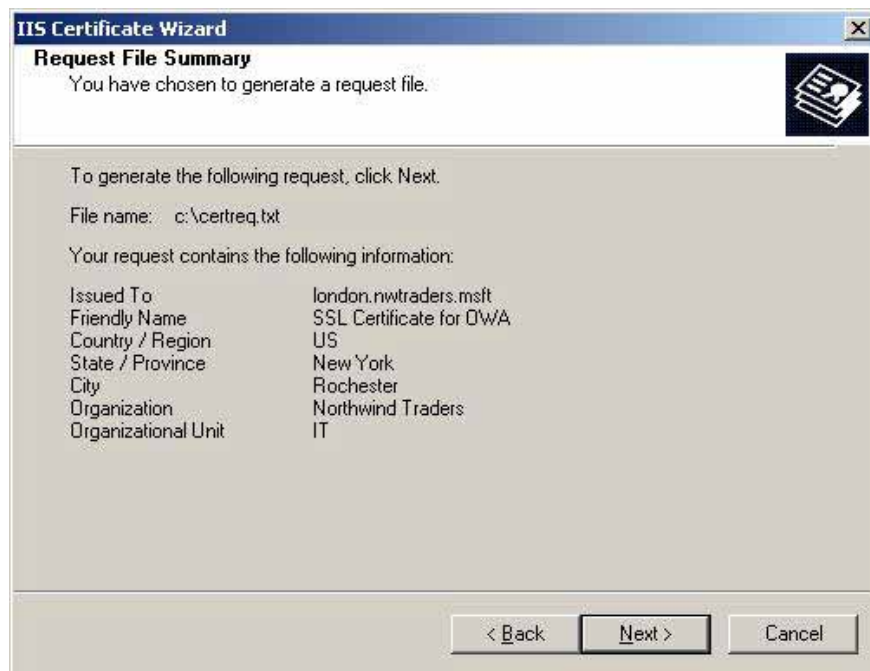
9. Then go to the " **Geographical Information** " dialog box (below). You need to enter the province or state name (in the US) in the State box completely. For example, enter "New York" instead of "NY". This is very important. The abbreviated name in the State box will be removed at the end of the Certificate Wizard.



10. The final step is to describe the location of the Certificate Request File. You must remember this information (what location and what to call) because you will need to copy data from this file to send it to a third party organization.



11. The " *Request File Summary* " dialog box appears (below). Check back to make sure everything is ok and click Next.



Now we have created a "Certificate Request" certificate request. It will be used in CSR sent to InstantSSL.

When you request a certificate from InstantSSL, they will ask you for a certificate request (Certificate Request). This is done by "pasting" the contents of the file we just created into a form when you apply for a certificate.

Each time you issue a certificate request, it takes a while for them to make the request, usually a few hours. But within 24 hours, the certificate provider will send their receipt notice via e-mail to the technical contact you

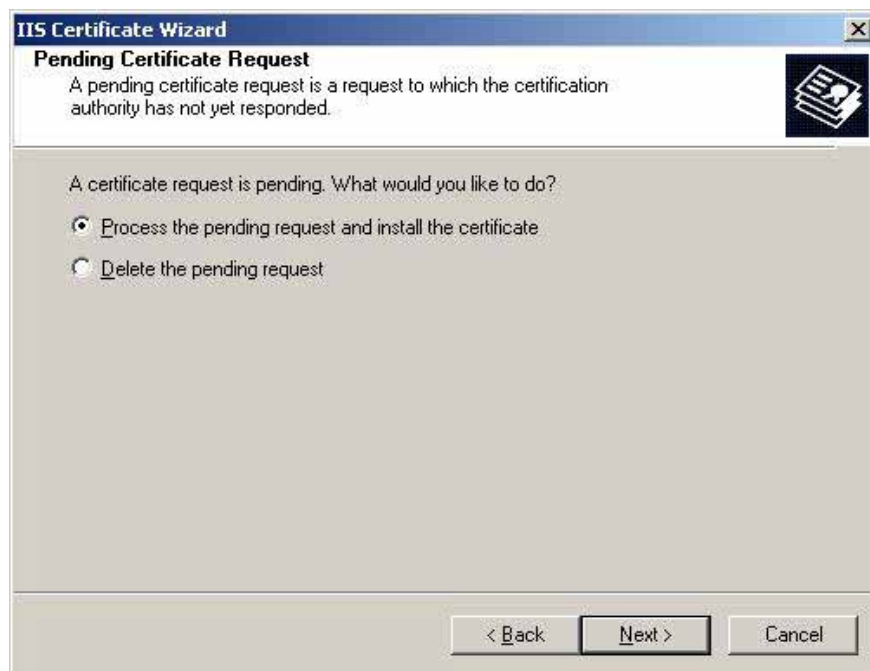
described in the submitted form.

When you receive a verification email from a third-party provider, they will also include instructions on how to install the certificate.

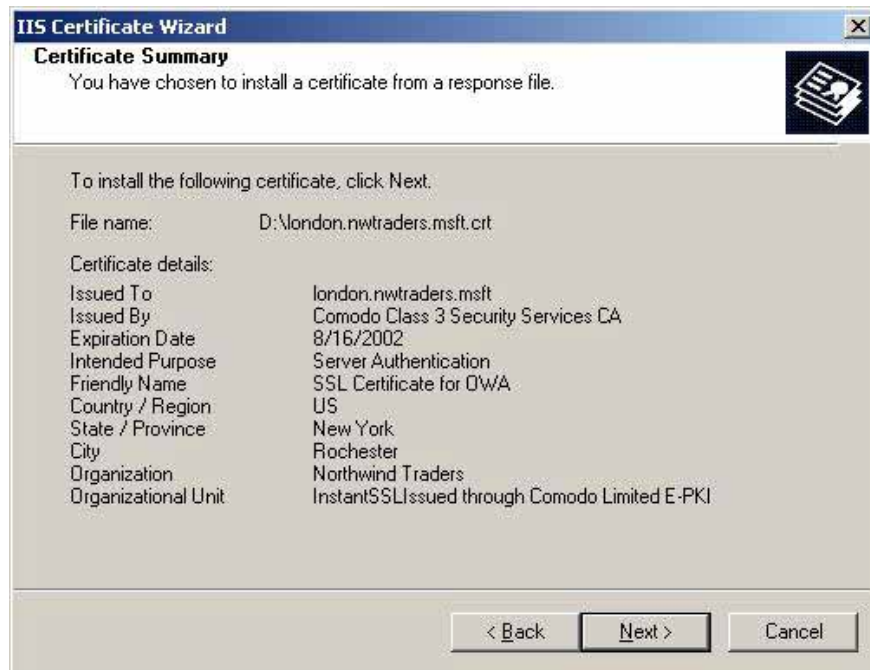
### **Add SSL to the OWA page**

Now you have received the certificate from InstantSSL. We will continue to install OWA and require SSL.

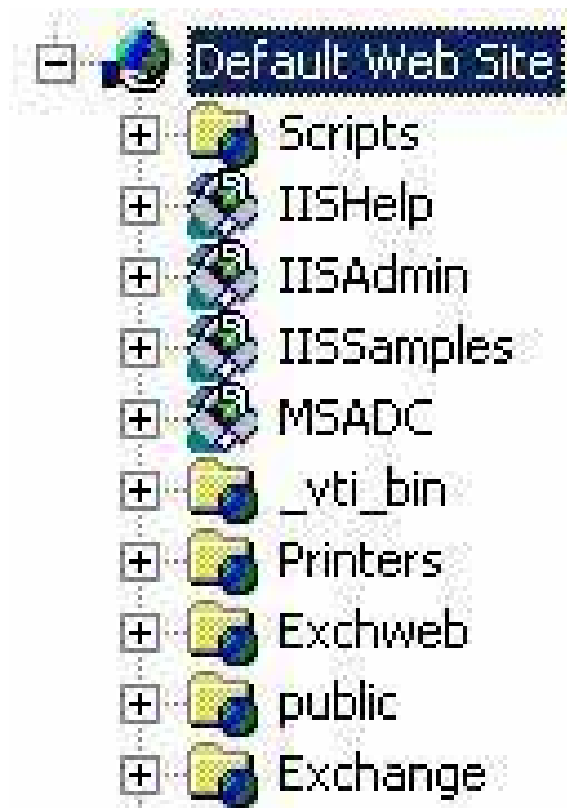
1. Open Internet Explorer Services Manager from the Administrative Tools component.
2. Open the Properties section of the website with OWA (usually the Default Web Site).
3. Select " *Directory Security* " and click on the " *Server Certificates* " button.
4. The " *Pending Certificate Request* " dialog box appears (below), select " *Process the pending request and install the certificate* ". Click Next.



5. The " *Process a Pending Request* " dialog box appears (below). Locate the certificate (Certificate) you receive from the third group. Click Next.



6. Next you will see the " *Certificate Summary* " dialog box appear (below). If everything is fine, click Next.



We have installed the SSL certificate on the website. The next step is to enable SSL in OWA, a fairly simple task.

1. Use Internet Services Manager, open the properties section (Properties) of the " *Exchange* " virtual directory.



2. Select " *Directory Security* " and click the " *Edit* " button in the Secure Communication section.

3. In the " *Secure Communication* " dialog box, check the box " *Require Secure Channel (SSL)* ". You can also check the box " *Require 128-bit encryption* ". If you mark a 128-bit box, any browser that does not support 128-bit encryption will not be connected to OWA.

Now, when users enter the URL `http://ahost.adomain.com/exchange` , they will receive an ' *HTTP 403.4 - Forbidden: SSL required Internet Information Services* ' error message because we have configured the owa required OWA. SSL is required. SSL uses HTTPS protocol, so users need to enter the url of the link: `https://ahost.adomain.com/exchange` . You can refer to the article on using SSL with Microsoft OWA.

Finally, you need to make sure that your firewall is configured to allow HTTPS to pass through (the default port 443).

Following all the steps above, OWA will be safe.

You finished reading the article "**Secure Outlook Web Access using SSL**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.