

## Re: ISAPI Authentication

**Source:** <http://www.derkeiler.com/Newsgroups/microsoft.public.inetserver.iis.security/2003-12/0371.html>

---

**From:** Wade A. Hilmo [MS] ([wadeh\\_at\\_microsoft.com](mailto:wadeh_at_microsoft.com))

**Date:** 12/13/03

Date: Fri, 12 Dec 2003 20:38:29 -0800

Hi Kevin,

I've made some comments inline.

Thank you,  
-Wade A. Hilmo,  
-Microsoft

"Kevin" <[anonymous@discussions.microsoft.com](mailto:anonymous@discussions.microsoft.com)> wrote in message  
news:12b3001c3c0be\$889b8a80\$a601280a@phx.gbl...

> *Thanks for the reply Wade.*

>

> *A little background will help explain what I am trying to*

> *do. We develop and sell a third party software product*

> *that is written in MFC. We are going to use a .NET*

> *webapp to mimic the MFC GUI interface and provide a web*

> *interface. The login information for the interface will*

> *come from an existing database, not from Windows accounts.*

>

When IIS processes the request, it will require a token that corresponds to Windows account. The job of your authentication filter is to accept non-Windows credentials from the client and then map them to a Windows account. After this mapping takes place, the REMOTE\_USER variable will reflect what the client sent, and the mapped credentials are used to generate the token.

> *One requirement that I am trying to stick to is to*

> *provide a reasonable level of security. That means not*

> *sending passwords in plain text and not storing them in*

> *plain text in the database. In order to simplify our*

> *security issues, we are willing to have our interface*

> *installed as an intranet web app and recommend that they*

> *either use VPN to connect remotely or configure extra*

> *security measures such as SSL before allowing access over*

> *the internet.*

>

> *Two other requirements that I am trying to stick to are*

- > *to not incur extra costs to implement our solution and to*
- > *keep the installation seamless (meaning the customer*
- > *won't have to do any special configuration). This seems*
- > *to rule out using SSL. If we used a third party*
- > *Certificate Authority like Verisign, we would be*
- > *incurring an extra cost or forcing the customer to. If*
- > *we implemented our own certificates, we would create*
- > *extra work for the customer, as he would have to create*
- > *the certificate and install a root certificate on each of*
- > *the clients in order for the users to be able to access*
- > *the site without receiving a warning message.*
- >

For password security, I would recommend storing either MD5 or SHA1 hashes of the password in the database. Then, you'll need some way to convert the user credentials from the client into the equivalent hash at authentication time. If you can hash the password on the client, then sending it in the clear will provide that reasonable level of security that you are looking for. To do this, you need to run code on the client. If you are able and willing to do this with client side scripting, then this is your answer. I usually prefer SSL over doing this because lots of clients disable scripting.

- > *I have been going back and forth between Forms*
- > *Authentication and an ISAPI filter. After what you have*
- > *told me, it seems that my best bet may be to use Forms*
- > *Authentication with an anonymous user, use JavaScript to*
- > *encrypt the credentials before the client returns the*
- > *login form, and encrypting the credentials stored in the*
- > *cookie.*
- >
- > *Do you have any thoughts or suggestions? I appreciate*
- > *advice from someone with more experience in these matters.*
- >

> >-----Original Message-----

> >Hi Kevin,

> >

> >There are lots of ways to implement authentication  
> filters on ISAPI. The

> >"common" way is to write a filter that registers for the

> >SF\_NOTIFY\_AUTHENTICATION event. When the event fires,  
> you are given the

> >username and password from the client (they are blank in  
> the case of an

> >anonymous request.) Your filter can then change them to  
> whatever username

> >and password you like (or blank to use the anonymous  
> user account – the IUSR

> >account.) When your filter then returns

> SF\_STATUS\_REQ\_NEXT\_NOTIFICATION,

> >any other authentication filters will get a chance to do

> *the same thing.*  
> > *After all of the authentication filters have had a  
> chance at it, then IIS  
> will use the filter supplied credentials to get the user  
> token. Note that  
> IIS does not ship with any authentication filters  
> installed.*  
> >  
> > *It is important to understand that the authentication  
> notification will only  
> fire for anonymous or basic authenticated requests, so  
> any password from the  
> client will be sent in the clear. Acutally, unless you  
> have code running on  
> the client to somehow encrypt or hash the user's  
> password, it's impossible  
> to prevent it from being sent in the clear at least  
> once. You should  
> consider this when you say that you will not use SSL,  
> even for an intranet.*  
> >  
> > *Other filter authentication schemes typically use a  
> login form on the server  
> and a cookie to get the client to resubmit  
> authentication information. The  
> typical logic for such a filter is more complex than I  
> can go into in this  
> reply.*  
> >  
> > *If you'd like more information about this (or any other)  
> ISAPI issue, please  
> feel free to post to  
> microsoft.public.platformsdk.internet.server.isapi-dev,  
> which exists for this purpose.*  
> >  
> > *Thank you,*  
> > *-Wade A. Hilmo,*  
> > *-Microsoft*  
> >  
> >  
> >  
> > *"Kevin" <anonymous@discussions.microsoft.com> wrote in  
> message  
> news:1243c01c3c029\$db795560\$a601280a@phx.gbl...  
> > I'm considering writing an ISAPI filter to handle  
> > authentication.  
> >>  
> >> Will it completely replace the configured windows  
> >> authentication or will it serve as an extra  
> >> authentication step before the windows authentication?  
> >> The documentation says that I can return*

microsoft.public.inetsrvr.iis.security: Re: ISAPI Authentication

> >> *SF\_STATUS\_REQ\_NEXT\_NOTIFICATION* but only says that it  
> >> will cause the next filter to be called and says  
> nothing  
> >> about what will happen if IIS is configured to Basic,  
> >> Digest, etc.  
> >>  
> >> Also, is this considered a secure form of  
> authentication  
> >> when compared to other options? I am going to use the  
> >> filter to compare against userids and passwords in a  
> >> database. (The passwords won't be stored as plain  
> >> text.) From what I have read, I already know to watch  
> >> out for buffer overruns. It will run on an intranet  
> and  
> >> we don't plan on using SSL.  
> >  
> >  
> >  
> >.  
> >