

Outlook Web Access 2003 Forms-based Authentication and the default domain dilemma

Date Launched: Aug 10, 2004
 Last Updated: Aug 10, 2004
 Section: **Tutorials :: Exchange 2003**
 Author: **Henrik Walther**

Okay so you have enabled Forms-based Authentication (FBA) and your users can now logon to Outlook Web Access (OWA) 2003 either by typing domain\username or username@domain.com. But ever since you enabled FBA your users have found it annoying they can't type username anymore, the other day even the CEO told you his opinion about it, and he definitely wasn't satisfied so you better come up with a solution.

You probably already tried to replace the backslash "\ " (which replaces the domain name when enabling FBA) with your Active Directory NetBIOS domain under the authentication settings of the Exchange virtual folder in the Internet Information Services (IIS) Manager, but only to find out that the changes you applied were being reset with a backslash "\" every 15 minutes or doing a reboot.

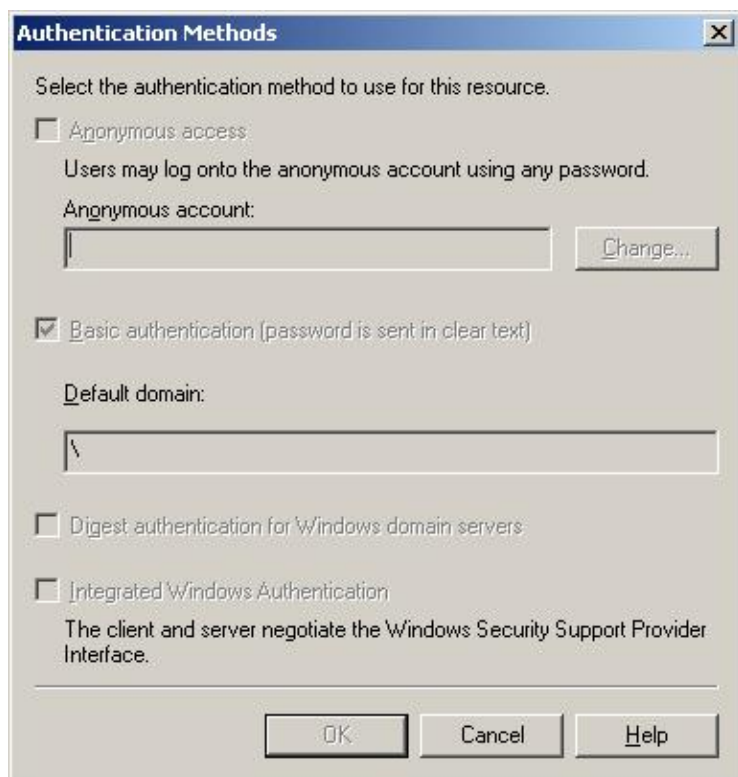


Figure 1: Authentication Method Settings in System Manager when FBA is enabled



Figure 2: Authentication Method Settings in IIS Manager when FBA is enabled

Well this is how Exchange 2000/2003 was designed; the behaviour is actually controlled by what is known as the Directory Service/Metabase Synchronization process (DS2MB process). In short the DS2MB process overwrites new configuration information in the local metabase (the metabase is kind of a registry for IIS) with configuration information that was last set in Active Directory by using the Exchange System Manager snap-in.

Note

For more information about the DS2MB process, see the [Relevant reading](#) section in the end of the article.

This means you should always strive to change any authentication related settings through the Exchange System Manager and not through the IIS Manager (even though it actually is possible to change them through the IIS Manager!)

Customizing the Logon.asp file

So how can we solve this problem? Well if some of your customers use SBS 2003, you may have noticed that you can logon to your mailbox by simply typing **username** instead of **domain\username** or **username@domain.com**. If you look carefully you can actually see OWA inserts your Active Directory NetBIOS domain name automatically when logging on. How does this magic occur? I hear you grumble. Well the magic lies within the Logon.asp, which is the file behind the FBA logon page, this file is located under:

C:\Program Files\Exchsrvr\exchweb\bin\auth\usa (or your language specific folder)

Note

In this article we will focus on the Logon.asp file for US English located in the USA folder (C:\Program Files\Exchsrvr\exchweb\bin\auth\usa.)

When dealing with ordinary Exchange 2003 Servers, we can make a similar trick. In order to accomplish our goal we need to edit the Logon.asp file, therefore browse to and open the Logon.asp file in notepad (remember to make a backup of the file before editing it!). Find below code by pressing **CTRL+F** then search for **<% If g_flMSIE5Rich Then %>** (Now press **Find** or **F3** twice!):

```
<% If g_flMSIE5Rich Then %>
<BODY scroll="AUTO" bgColor="#3D5FA3" text="#000000" leftMargin=0 topMargin=0>
<FORM action="/exchweb/bin/auth/owaauth.dll" method="POST" name="logonForm" autocomplete="off">
<% Else %>
<BODY scroll="AUTO" bgColor="#FFFFFF" text="#000000" onload="window.document.logonForm.username.focus()">
<FORM action="/exchweb/bin/auth/owaauth.dll" method="POST" name="logonForm">
<% End If %>
```

In above code you should replace both instances of:

```
<FORM action="/exchweb/bin/auth/owaauth.dll" method="POST" name="logonForm" autocomplete="off">
```

With below piece of code:

```
<script Language=javascript>
  <!--
  function logonForm_onsubmit()
  {
  if (logonForm.username.value.indexOf("@") !=-1)
  {
  return true;
  }
  logonForm.username.value = "NetBIOS domain here\\" + logonForm.username.value;
  return false;
  }
  //-->
</script>
<FORM action="/exchweb/bin/auth/owaauth.dll" method="POST" name="logonForm" autocomplete="off"
onsubmit="logonForm_onsubmit()">
```

Remember to replace **NetBIOS domain here** in above code with your own NetBIOS domain name (if your DNS name were Testdomain.com your NetBIOS name would be Testdomain.)

Testing the modified Logon.asp File

When you have made the proper changes to the Logon.asp file you should save it, then logon to your mailbox using OWA to verify it works. If it does then congratulations! If not, you should either try to go through the above steps again (to pinpoint any errors) or if you're the lazy kind of guy download a modified version of the Logon.asp file [here](#) (you only need to replace **NetBIOS domain here** with your own NetBIOS domain name then save the file).

Note

The downloadable Logon.asp file is the one contained in the USA folder, so if you're using another language, you need to modify your language specific version.

Changing the appearance of the FBA Logon Page

When implementing this behaviour bear in mind your users no longer can logon using **domain\username**, it's therefore a very good idea to both warn your users before making this change, as well as make a few minor modification to the visual appearance of the FBA logon page. As you can see in **figure 3** it still informs the user to type **Domain\user name**, which by now is quite misleading, you should therefore also modify line 20 of your language specific Logon.asp file, which looks identical to below line of code (simply remove the **Domain** part which will have it look like **figure 4**):

```
CONST L_UserName_Text = "Domain\username:"
```

You should also consider removing the **Domain** part from line 24, 25 and 26, so that the FBA page is kept in a consistent state.

Note

These modifications are as well included in the downloadable version of the **Logon.asp** file; I referred to earlier in the article.

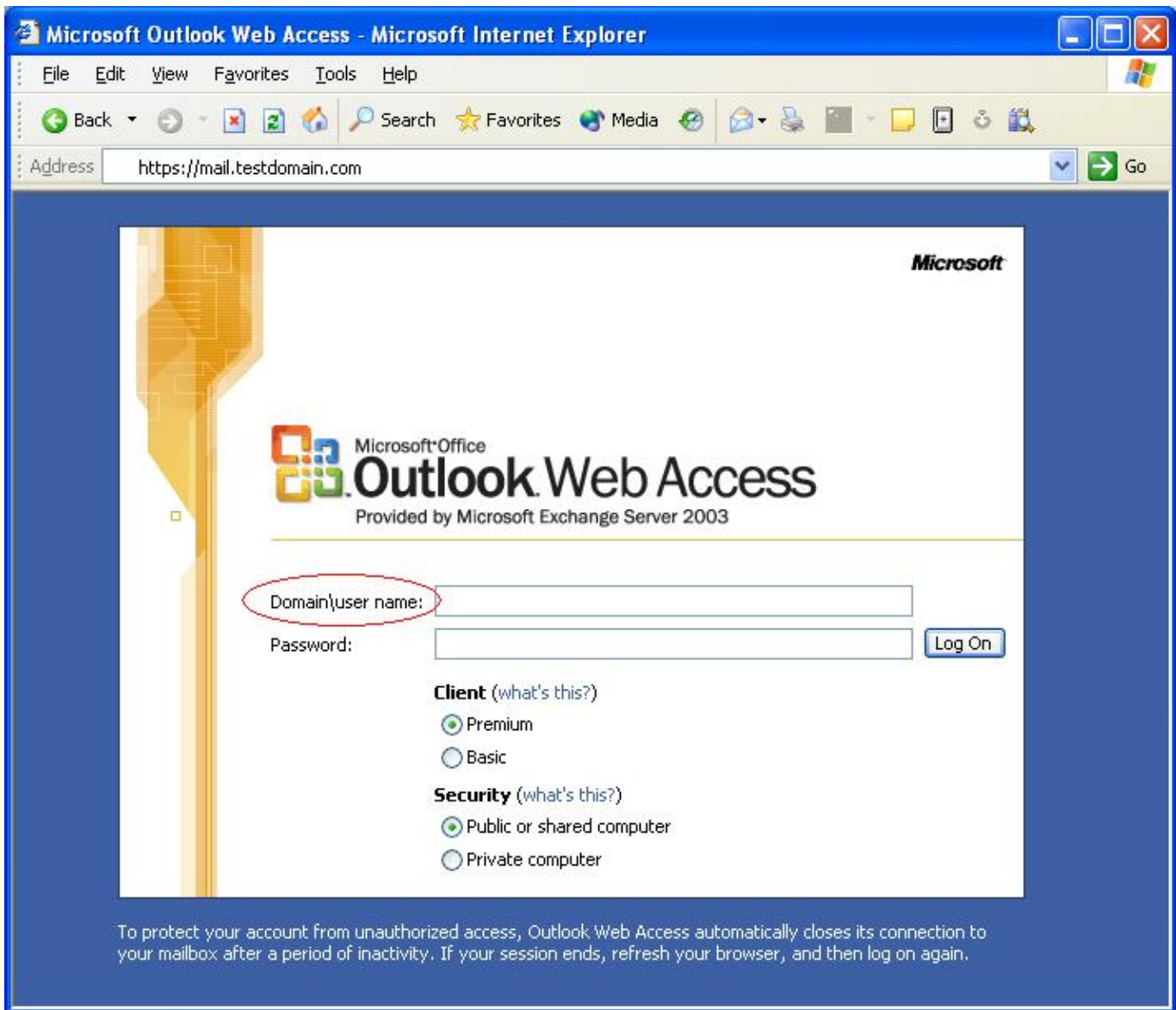


Figure 3: FBA logon page still informs user to enter Domain\user name

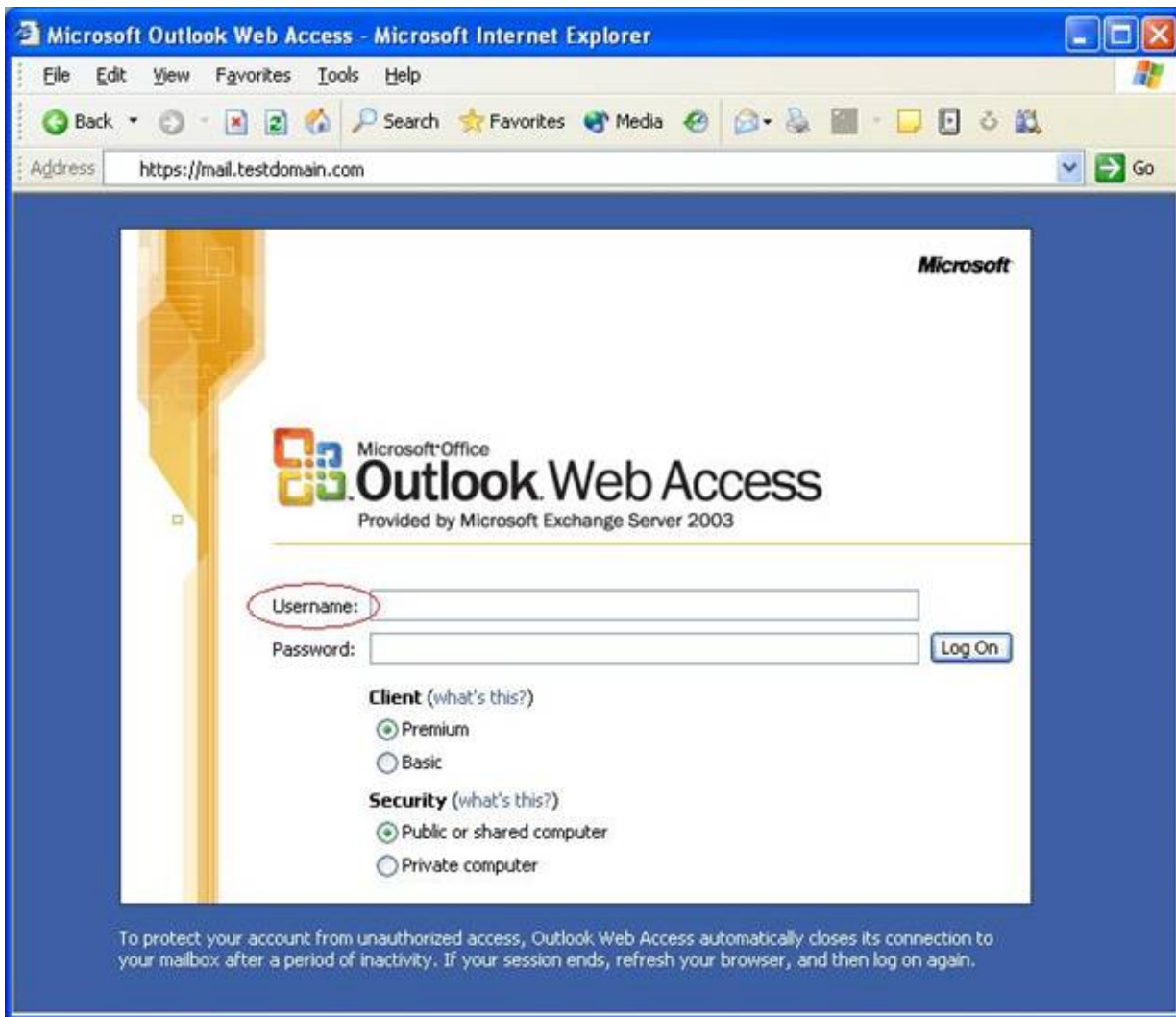


Figure 4: FBA logon page after the modification

That was all for this time, see you soon!

Relevant reading

[240105 - XGEN: General Information on Directory Service/Metabase Synchronization in Exchange 2000 Server](#)

[264941 - XCCC: Changes to Virtual Directory Settings Are Not Maintained](#)

[830827 - How to Use Forms Based Authentication with Outlook Web Access Clients in Exchange Server 2003](#)

[820378 - Outlook Web Access session unexpectedly quits when forms-based authentication is used](#)

Featured Links*

Copyright © 1995- 2004 MExchange.org All Rights Reserved.
Visit us at www.MExchange.org