



Enable single sign on with Active Directory with MindTouch installed on Linux

This method uses [Winbind](#), the Samba method for allowing NT groups to show up as if they were local. It's very easy.

Another possible solution is to just use Kerberos, which does not require Samba at all. Since Mindtouch handles group membership lookups separate (via LDAP) from authentication, Kerberos is potentially the better choice. There are also some issues with NTLMv2 and Samba, depending on your version, which are not present when using straight Kerberos. See [Mod_Auth_Kerb](#) for more info.

Note: this guide assumes your wiki is installed in `/var/www/dekiwiki`: it might be in `/var/www/deki-hayes` if you have upgraded an older VM. [Here's how you can move it.](#)

Upgrade your wiki to 8.05.1 or greater

Start by ensuring you're at the latest code level (8.08.2 at time of writing). Update your wiki with:

```
/usr/bin/updateWiki.sh
```

Install Winbind and the Apache module

Attached to this page is a version of the NTLM authentication module built for Debian Etch. There are versions available for [Ubuntu](#) also.

```
# Install winbind and libapache2-mod-auth-ntlm-winbind
apt-get install winbind
wget http://wiki.developer.mindtouch.com/@api/deki/files/2921/
=libapache2-mod-auth-ntlm-winbind_0.1%252bgit20080610-0.1_i386.deb \
    -O libapache2-mod-auth-ntlm-winbind_0.1+git20080610-0.1_i386.deb
dpkg -i libapache2-mod-auth-ntlm-winbind_0.1+git20080610-0.1_i386.deb

# Enable the module
a2enmod auth_ntlm_winbind

# Allow Apache to connect to Winbind
usermod -a -G winbindd_priv www-data
```

Configuring Winbind

Change, uncomment or add the following six options in the [global] section of `/etc/samba/smb.conf`:

```
workgroup = SHORTDOMAINNAME
security = domain
password server = *
idmap uid = 10000-20000
idmap gid = 10000-20000
winbind use default domain = yes
```

Note: Samba does not need to be running for Winbind to work. Replace SHORTDOMAINNAME with the domain name (as in DOMAIN\user), but the * gets entered as-is.

Now, you must join this machine to your domain, and restart Winbind:

Note: If using a Windows Server 2008 Domain Controller, you must follow this kb article (<http://support.microsoft.com/kb/942564>). This setting must be enabled every time the Wiki starts.

```
# you will be prompted for a password after this:
net join DOMAINNAME -U username
```

```
/etc/init.d/winbind restart
wbinfo -u
```

If you see a list of users (without a DOMAINNAME\ prefix), then congratulations, you have successfully configured Winbind.

Configuring the LDAP service

Service management

Log into your wiki. You first need to set up your LDAP service. (under Control Panel, Service Management). You can edit an existing one if you have one, or create a new LDAP service. NOTE: If you've already had an LDAP service setup with users already existing, be sure to edit the service rather than creating a new one.

- **Type:** Authentication
- **SID:** [sid://mindtouch.com/2007/05/ldap-authentication](http://mindtouch.com/2007/05/ldap-authentication)
- **Config:**
 - userquery sAMAccountName=\$1
 - hostname myADserver
 - bindingdn ldapuser@domain.com
 - searchbase DC=domain,DC=com
 - bindingpw ldappassword
- **Status:** enabled

Save this service. Note the number it is allocated, as you will use this below. (On a new VM, it will probably be '10').

If you were previously using [Active Directory integration](#). please note in particular that *bindingdn* and *bindingpw* change from variables to a single hardcoded username and password, and that the *SID* changes too.

Configuration

Under Control Panel/Configuration, add two new values:

- security/allow-trusted-auth: true

- security/trusted-auth-provider-id: (the number of your LDAP service)

Log out of the wiki, and restart Dekihost again:

```
/etc/init.d/dekiwiki restart
```

(At this point it might be a good idea to log into your wiki and grant your LDAP user 'admin' rights, as it is difficult to log in as a local user once your browser is automatically authenticating you.)

Configuring Apache

In `/var/www/dekiwiki`, create a file named `.htaccess`. Add this content:

```
AuthName "NTLM Authentication"  
NTLMAuth on  
NTLMAuthHelper "/usr/bin/ntlm_auth --helper-protocol=squid-2.5-ntlmssp"  
NTLMBasicAuthoritative on  
AuthType NTLM  
require valid-user
```

You can set `AuthName` to anything you want.

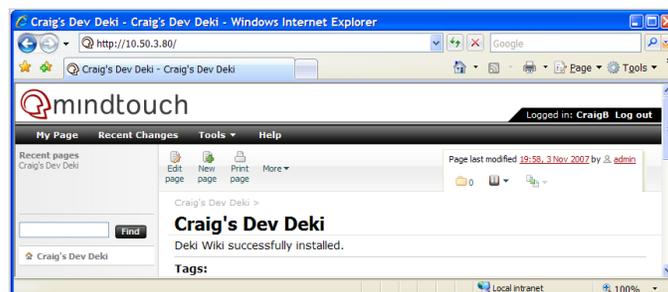
This will force Apache to ask require NTLM credentials before serving any content, and also pass the username to Deki for single sign on.

Restart Apache:

```
/etc/init.d/apache2 force-reload
```

You are now good to go!

Hit <http://mywiki/>, and as long as your browser is set up for NTLM, you will automatically be logged in.



Feels good!

Configuring your web browser

If your URL is in the Local Intranet site in IE, then the browser will present your credentials automatically. You can add the site manually if it doesn't automatically get detected.

Firefox users can set the property `network.automatic-ntlm.trusted-uris` in `about.config`.

Troubleshooting

Try browsing to `http://mywiki/@api/deki/services/def...users/username` (where 10 is the number of your LDAP service) to see if the LDAP service is returning correct results.

