

HOW-TO Enable NTLMv2 SSO for Unified Self Service 14.1 (OpenSpace 4.0)

Purpose:

Unified Self Service Out of the Box only allow authentication through EEM with NTLMv1 that is outdated or CA Site Minder that allow federation and SSO but with a higher costs.

As an alternative until a full modern SSO platform is implemented, this is possible to enable NTLMv2 SSO following the instruction in this document.

Note that the standard NTLM filter of LifeRay only process SSO for Internet Explorer as this is not possible to release the session in those browsers until the browser itself is completely close. This is an acceptable risk and this is how this was previously implemented with Jespa. Therefore we created a modified filter that remove that restriction.

Implementation:

Note that the path described below can vary depending of your installation and refer to the OSOP installation folder.

Step 1:

Copy the 2 modified class files **NtlmFilter.class**, **NtlmPostFilter.class** into:

...\OSOP\tomcat-7.0.40\webapps\ROOT\WEB-INF\classes\ext\com\liferay\portal\servlet\filters\sso\ntlm

(Basically, you can copy the ext folder to the ROOT\WEB-INF\classes folder)

Step 2:

Edit ...\\OSOP\tomcat-7.0.40\\webapps\\ROOT\\WEB-INF\\liferay-web.xml

Locate the filters below:

```
<filter-name>SSO Ntlm Filter</filter-name>
```

```
<filter-name>SSO Ntlm Post Filter</filter-name>
```

Change the filter-class entries to prepend ext. to the class as shown below:

```
<filter>
```

```
<filter-name>SSO Ntlm Filter</filter-name>
```

```
<filter-class>ext.com.liferay.portal.servlet.filters.sso.ntlm.NtlmFilter</filter-class>
```

```
</filter>
```

```
<filter>
```

```
<filter-name>SSO Ntlm Post Filter</filter-name>  
<filter-class>ext.com.liferay.portal.servlet.filters.sso.ntlm.NtlmPostFilter</filter-class>  
</filter>
```

Step 3:

Edit ...\\OSOP\\portal-ext.properties:

- Search and set all filters sso filters to false if any:

```
com.liferay.portal.servlet.filters.sso.cas.CASFilter=false  
com.liferay.portal.servlet.filters.sso.opensso.OpenSSOFilter=false  
com.liferay.portal.servlet.filters.sso.ntlm.NtlmFilter=false  
com.liferay.portal.servlet.filters.sso.ntlm.NtlmPostFilter=false
```

- Add new modified filters:

```
ext.com.liferay.portal.servlet.filters.sso.ntlm.NtlmFilter=true  
ext.com.liferay.portal.servlet.filters.sso.ntlm.NtlmPostFilter=true
```

- Add ntlm properties:

```
#adding SSO by Jmayer  
ntlm.auth.enabled=true <set to true to enable ntlm auth>  
ntlm.auth.domain=MYDOMAINL<set the domain that you need to connect to>  
ntlm.auth.domain.controller=XXX.XX.XX.XX<comma separated list of DC IP address for that domain>  
ntlm.auth.domain.controller.name=DC01<hostname of the domain controller>  
ntlm.auth.service.account=computeraccount$@mydomain.com<computer account for that domain>  
ntlm.auth.service.password= xxxxxxxx<password of the computer account>
```

Important Note: You need to create or request a computer account to you domain Administrator and set a password for this account (by default computer account are created without a password. You may also want to see JESPA documentation at www.ioplex.com on how to create a computer account and set password

- Set auto.login.hooks=com.liferay.portal.security.auth.NtlmAutoLogin

For SSO to work you need to access specific URL constructed as below to be the landing page of your users after your root:

<https://selfservice.mydomain.com/c/portal/login>

Testing:

Using Internet Explorer, Firefox and /or Chrome go to the USS portal using the link example provided above.

If your browser is configured for Windows integrated authentication, you will be automatically logged in Unified Self Service transparently.

If not the case (i.e. Chrome) you will be prompted with a netlogon window and be asked to enter your credential in the form of:

<domain name>\<username>

Note: that USS authentication login page is always available for any other URL than the **/c/portal/login** and will go through CA EEM authentication.

IMPORTANT:

This is a workaround for the current release of Life Ray used by CA. This solution may need to be reviewed if CA upgrade the Life Ray version used in Unified Self Service.

This is to be consider a temporary solution until better SSO platform is defined to be use.