Liferay Kerberos SSO

by

SMC Treviso srl

Index

1. INTRODUCTION

This guide will describe the actors and actions taken by SMC to allow a Liferay portal to manage user access in Single SignOn through the Integrated Windows Authentication.

In order to create this guide, virtual machines have been set up containing the necessary operating systems and software.

The systems involved are:

- a virtual machine with Microsoft Windows Server 2008 R2 with the role of Domain Controller. In detail:
  - the Realm is "SMC.LOCAL"
  - the server name is "pdc.smc.local"
  - the NT domain is "SMC"
- a virtual machine with Microsoft Windows 10 joined to SMC domain
- a virtual machine with CentOS 7
  - there is a Liferay 7 CE GA7 bundle
  - Liferay exposes the portal on "http: //portal.smc.local"
  - our Kerberos SSO plugin is installed in Liferay
- name resolution uses the domain controller's DNS whenever possible, otherwise it takes advantage of the hosts file

2. INTEGRATED WINDOWS AUTHENTICATION

The term Integrated Windows Authentication (IWA) is used by Microsoft to identify authentication mechanisms through the SPNEGO, Kerberos and NTLMSSP protocols.

IWA is not a standard. It identifies an approach to authentication that the parties involved in the flow must agree and use. It is an approach with the use of different standards.

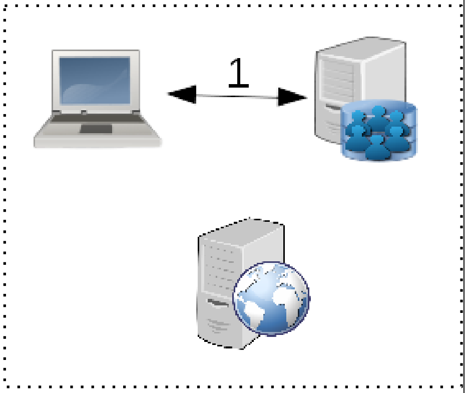
For example, if the context contains the prerequisites for using a Kerberos ticket this will be used; otherwise the systems will opt for NTLMSSP. The latter can also be chosen when a first attempt with Kerberos has failed.

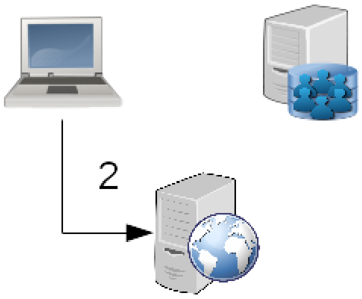
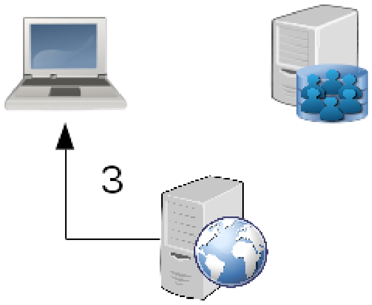
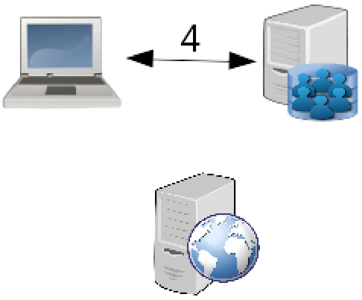
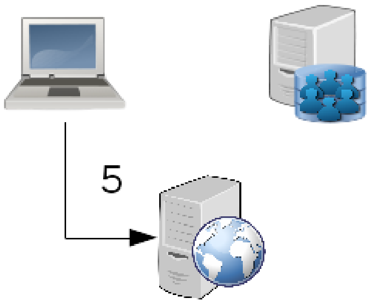
The IWA involves three actors:

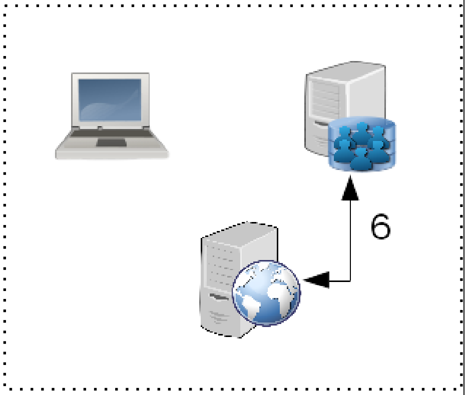
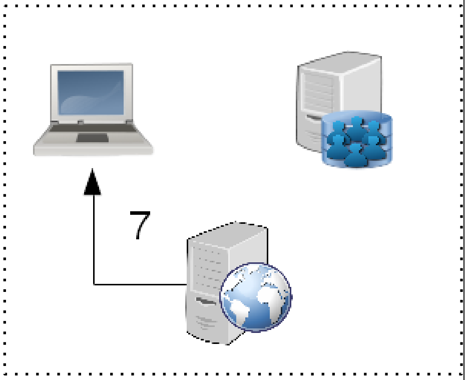
	The system that provides the web service. It can be a Windows server with IIS. Or, as in our scenario, a Linux system with a Tomcat with Liferay.
	The client workstation, typically a Microsoft Windows system joined to Active Directory domain, to which the user has accessed with his / her domain credentials
	The system that acts as an Active Directory domain controller. The same domain on which the client workstation and the user belong to.

2.1. OPERATIONAL FLOW

Let's see in detail the workflow of the authentication phase

1) the user accesses a Windows workstation connected to an Active Directory domain by providing his Active Directory credentials	

2) the user, using a browser configured to manage the IWA (ex: Internet Explorer), requests a protected web resource provided by WebServer (eg: http://www.test.net/stuff)	
3) at this moment the Web server does not know the user and therefore responds to the request with the result "401 Unauthorized". The response contains the header "WWW-Authenticate: Negotiate" which informs the browser about the need to provide an authorization token	
4) the browser receives the response 401 and the header, then contacts the KDC (domain controller) to request a token: • the KDC is asked if there is a service account to access the service. The account is in "HTTP/fqdn-web-server@REALM" format • if the service account exists, the credentials of the active user are used to obtain a token from the KDC	
5) the browser tries again to access the protected resource providing the token received from the KDC in the Negotiate header	

6) the WebServer receives the token and communicates with the KDC to validate it. Once validated, it has the username that identifies the user connected to the client workstation	
7) once the user is identified, the WebServer provides the requested web page. Obviously, if the user does not have the application authorizations to access the page, the WebServer will respond accordingly.	

In phase 2) the requested resource is always identified by a url like "http://fqdn-server-web/path/of/the/resource". It is important that the url contains a Full Qualified Domain Name to allow subsequent activities; it is not recommended to use the IP address.

The KDC server must be able to resolve, or obtain the IP address, of "fqdn-web-server" via DNS or hosts file (C:\Windows\System32\drivers\etc\hosts).

In phase 4) it is the browser that talks directly with the KDC to get the token. It is necessary that in the domain there is a "Service Principal Name" aka a user connected to the service. Its configuration will be explained later.

The browser directly uses the credentials of the logged in user only if "http://fqdn-server-web", or "http://fqdn-server-web/path", or "*.part-fqdn-server-web", is present in the browser configuration as part of the"Local Intranet".

If the website is not present in the list, the user will see a modal window asking them to enter their credentials. And the user can provide credentials different from those used to connect to the PC.

This will result in the production of a Kerberos or NTLMSSP token.

As indicated above, in phase 4) the browser receives a Kerberos token only if a Service Principal Name (SPN) has been created and configured in Active Directory.

The Service Principal Name must also be known to ServerWeb and will be used in phase 6) to decode the token and obtain the name of the user in the format "username@REALM".

2.2. NEGOTIATION AND TOKEN

The Integrated Windows Authentication involves several actors each of which can apply their own rules to decide if they can use a Kerberos token.

Windows Operating System

- the Windows workstation must be joined to the same domain of the Service Principal Name
- also the user who has accessed the workstation must be present in the domain of the Service Principal Name
- the time difference between the workstation and the Domain Controller must be less than 5 minutes

Internet Explorer

- the resource to which the user is accessing is a UNC path (eg: \\portal), or it is a site that can be reached without exploiting a proxy and its VirtualHost is a unique word without dots (eg: http://portalsmclocal/)
- the resource, or rather its VirtualHost, is manually registered in the list of sites of the "Local Intranet"

For Internet Explorer there are rules that were applied in the past and/or applied in a non-deterministic way:

- the resource, or rather its VirtualHost, is manually registered in the list of sites on the "Trusted Sites" tab and in the "Local Intranet" tab, both the "Automatic detection" and the child entries are checked.
  This should make the "Trusted Sites" part of the "Local Intranet"; but often this does not happen, perhaps due to the presence or absence of Microsoft fixes

Again on Internet Explorer, as anticipated at the beginning of the chapter, in all those scenarios where it believes it cannot use the Kerberos token the browser will automatically fall back to NTLM.

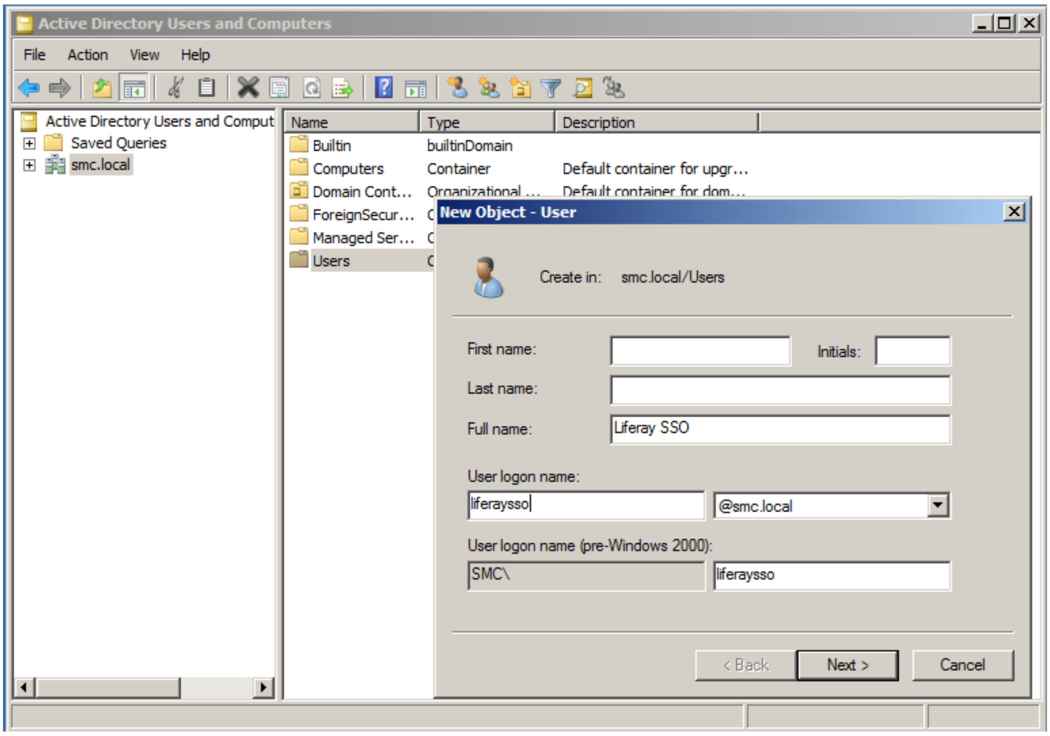
In this case Internet Explorer will use the credentials of the user connected to the workstation to generate an NTLMSSP token; or Internet Explorer will pop-up a client-side dialog asking the credentials in order to produce an NTLMSSP token.

3. SERVICE PRINCIPAL NAME

The Service Principal Name (or SPN) is a particular user registered in the Active Directory domain linked to a resource.

Let's look at the steps taken in the Windows Server 2008 R2 used for this guide.

Through the tool "Active Directory Users and Computers" we have created the user "liferaysso", having a fixed password that does not expire and must not be changed at the first login.



New Object - User

Create in: smc.local/Users

First name:

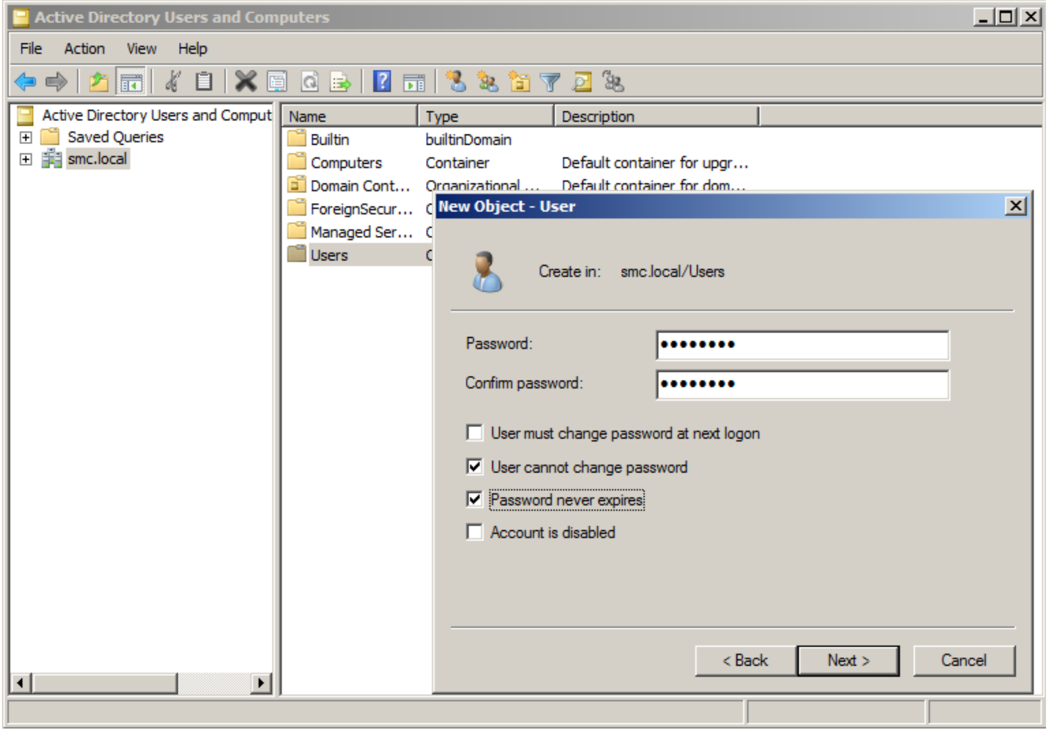
Initials:

Last name:

Full name: Liferay SSO

User logon name: liferaysso @smc.local

User logon name (pre-Windows 2000): SMC\ liferaysso



New Object - User

Create in: smc.local/Users

Password: ••••••••

Confirm password: ••••••••

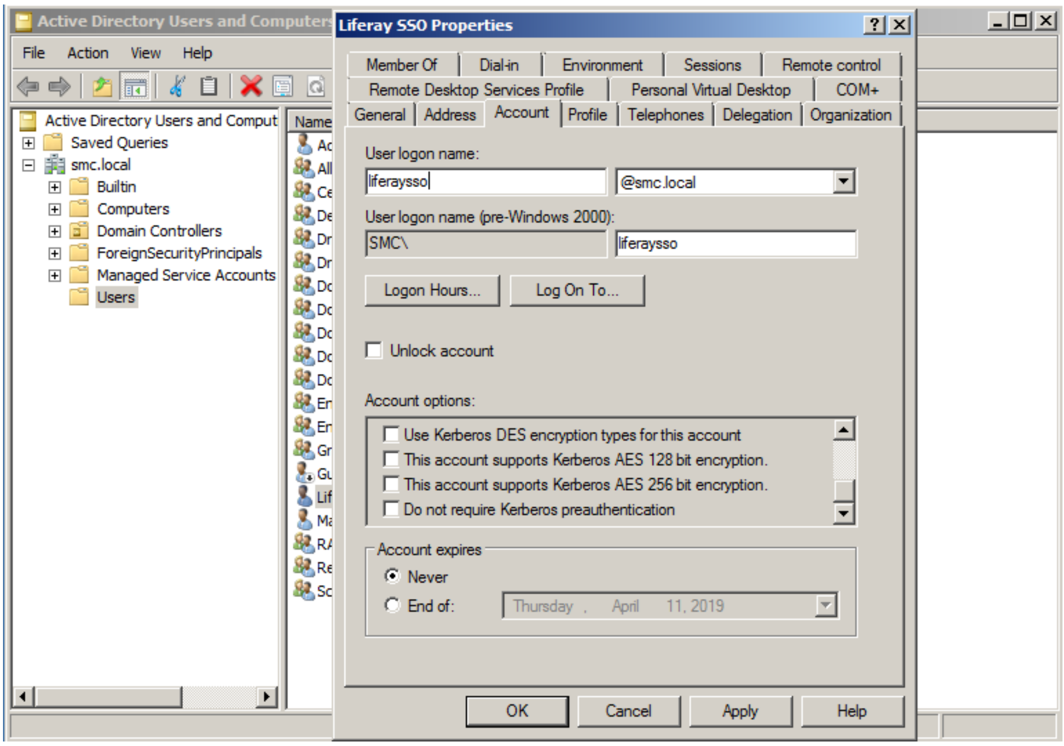
□ User must change password at next logon

☑ User cannot change password

☑ Password never expires

□ Account is disabled

Again through "Active Directory Users and Computers" it must be verified that the newly created user, in the Account tab, does not have variations on the cryptographic aspects



User logon name: liferaysso @smc.local

User logon name (pre-Windows 2000): SMC\ liferaysso

☐ Unlock account

Account options:

☐ Use Kerberos DES encryption types for this account
☐ This account supports Kerberos AES 128 bit encryption.
☐ This account supports Kerberos AES 256 bit encryption.
☐ Do not require Kerberos preauthentication

Account expires

● Never
○ End of: Thursday , April 11, 2019

We use the "ktpass.exe" command to make the user just created a Service Principal Name.

From a command prompt (cmd.exe) we execute the command (here divided on several lines only for editorial reasons)

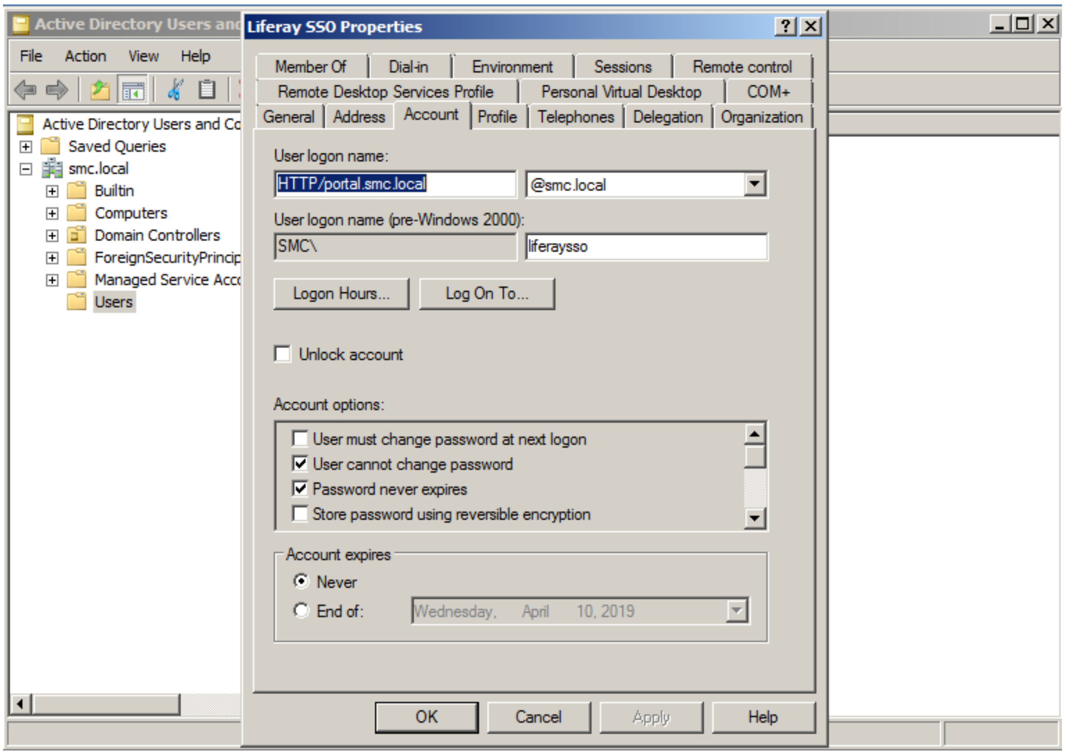
```
ktpass.exe /out liferaysso.keytab
  /princ HTTP/portal.smc.local@SMC.LOCAL /pass Welcome1
  /mapuser liferaysso@SMC.LOCAL /ptype KRB5_NT_PRINCIPAL
  /crypto RC4-HMAC-NT
```

The syntax of the ktpass command:

- /princ, to indicate the service which we want to connect in the "HTTP/fqdn-server-web@REALM" format
- /crypto, to indicate the supported encryption algorithm. We will use the most portable and compatible RC4-HMAC-NT
- /pass, to reset the user's password in a manner consistent with the chosen encryption algorithm
- /mapuser, to indicate which user to connect the service to
- /out, to save on file a certificate that would allow us to use the service without specifying the password

The generated keytab file can be used by the WebServer to access the Service Principal Name.

If we come back to "Active Directory Users and Computers" we will see how the user data has changed in the "Account" tab to reflect its new role



User logon name:
HTTP/portal.smc.local @smc.local

User logon name (pre-Windows 2000):
SMC\ liferaysso

□ Unlock account

Account options:

- □ User must change password at next logon
- ☑ User cannot change password
- ☑ Password never expires
- □ Store password using reversible encryption

Account expires

- ● Never
- ○ End of: Wednesday, April 10, 2019

4. LINUX, TOMCAT AND LIFERAY

The web functionality to which the user must access in an authentic way is provided by Liferay Portal: a web application developed in Java and installable in Tomcat, JBoss and many other Application Servers. Typically Liferay is installed on Linux systems. In the scenario used for this guide we use a CentOS 7.

Liferay integrates natively with different Single SignOn mechanisms and allows the authentication logics to be managed in a timely and separate manner based on the different channels of resource use.

In the case of the "Integrated Windows Authentication" the integration was implemented by SMC as a hot-deployable plugin.

Before understanding the configuration aspects of the plugin, let's see the preparatory phase.

4.1. SERVER TIME

The time to the systems involved must be aligned. This aspect is especially important for the dialogue between the Domain Controller and the Linux server hosting Liferay.

It is advisable to connect the different systems to a public NTP (Network Time Protocol) service if no one is present in the company network.

4.2. LINUX CONFIGURATION

The Linux system hosting Liferay must be able to communicate with the Domain Controller.

Our first action consists in transferring the ".keytab" file with the Service Principal Name access key inside the Linux system and using the standard Kerberos libraries to verify that the file is read and the systems can talk to each other.

To carry out this check, the "k5start" command contained in the "kstart.x86_64.rpm" package is required.

Let's assume we have transferred the file "liferaysso.keytab" (created in 3 SERVICE PRINCIPAL NAME) to the "/root" folder.

Update file "/etc/krb5.conf" as follows:

```
# Configuration snippets may be placed in this directory as well
```

```
includedir /etc/krb5.conf.d/

[logging]
default = FILE:/var/log/krb5libs.log
kdc = FILE:/var/log/krb5kdc.log
admin_server = FILE:/var/log/kadmind.log

[libdefaults]
dns_lookup_realm = false
ticket_lifetime = 24h
renew_lifetime = 7d
forwardable = true
rdns = false
pkinit_anchors = /etc/pki/tls/certs/ca-bundle.crt
# default_realm = EXAMPLE.COM
default_ccache_name = KEYRING:persistent:%{uid}
default_tkt_enctypes = rc4-hmac
default_tgs_enctypes = rc4-hmac
permitted_enctypes = rc4-hmac

[realms]
# EXAMPLE.COM = {
#  kdc = kerberos.example.com
#  admin_server = kerberos.example.com
# }
 SMC.LOCAL = {
  kdc = pdc.smc.local
  admin_server = pdc.smc.local
 }

[domain_realm]
# .example.com = EXAMPLE.COM
# example.com = EXAMPLE.COM
 .smc.local = SMC.LOCAL
 smc.local = SMC.LOCAL
```

Where we set:

- that the crypt algorithm used for the keytabs is RC4-HMAC (as per command ktpass.exe)
- our Realm with the IP address of the Domain Controller server (kdc)
- a sequence of aliases so that the Realm is used independently of upper or lower case

We execute the command k5start as follows (the gray lines are an example of a positive outcome)

```
# k5start -f liferaysso.keytab -U -v
Kerberos initialization for HTTP/portal.smc.local@SMC.LOCAL
k5start: authenticating as HTTP/portal.smc.local@SMC.LOCAL
k5start: getting tickets for krbtgt/SMC.LOCAL@SMC.LOCAL
```

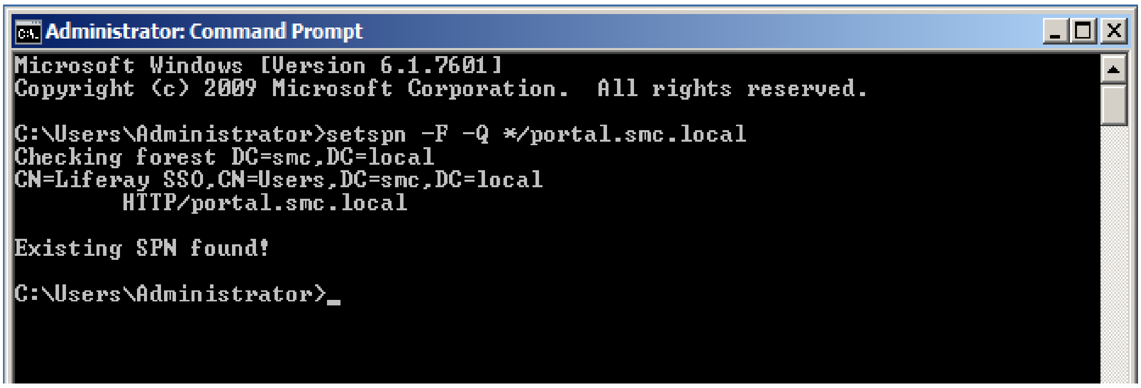
First possible connectivity error situation:

- if in the krb5.conf file the KDC is set by name it is possible that this is not registered in the DNS. Verify that it is resolved by eventually adding it to the /etc/hosts file
- the two servers (CentOS and KDC) must be able to communicate. Make sure any intermediate firewalls allow communication. Eventually use the nmap command to understand the status of the ports

The message "`k5start: error getting credentials: Client 'HTTP/portal.smc.local@SMC.LOCAL' not found in Kerberos database`" usually happens when there are multiple ServicePrincipals connected to the same resource.

On the Domino Controller run "`setspn -F -Q */portal.smc.local`" to view the SPN users and eventually remove the incorrect ones.

The image shows a scenario without errors.



```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\Administrator>setspn -F -Q */portal.smc.local
Checking forest DC=smc,DC=local
CN=Liferay SSO,CN=Users,DC=smc,DC=local
        HTTP/portal.smc.local

Existing SPN found!

C:\Users\Administrator>_
```

4.3. FILE LOGIN.CONF

Kerberos ticket validation is performed by the standard Java Security component present in the JRE or JDK used by the Tomcat with Liferay. This component must be instructed to use the keytab of Service Principal Name.

Unfortunately it is possible to set only one keytab for JVM, and this is a problem with Liferay which is multi-tennant. So:

- if only one instance of Company is managed in Liferay, the keytab can be used to indicate the Service Principal password
- if you have to manage multiple instances of Company in Liferay, the password must be provided in the Liferay Control Panel
- if you have only one Company instance you are free to set password in Control Panel, you are not forced to use keytab

The SMC plugin uses the "jcifs.spnego.accept" security context to validate the Kerberos ticket.

4.3.1. TOMCAT

Only if you can and want to use the keytab file you need to create the "login.conf" file with a content similar to the following

```
jcifs.spnego.accept {
  com.sun.security.auth.module.Krb5LoginModule required
  doNotPrompt=true
  principal=”HTTP/portal.smc.local@SMC.LOCAL”
  useKeyTab=true
  keytab=”/path/to/liferaysso.keytab”
  storeKey=true;
};
```

And set the full path of that file in the Kerberos SSO configuration as described in “5 PLUGIN KERBEROS SSO”.

4.3.2. JBOSS

Only if you can and want to use the keytab file it is necessary to modify the standalone.xml file by adding a similar content

```
<subsystem xmlns="urn:jboss:domain:security:1.2">
  <security-domains>
    <security-domain name="PortalRealm">
      <authentication>
        <login-module
code="com.liferay.portal.kernel.security.jaas.PortalLoginModule" flag="required"/>
      </authentication>
    </security-domain>
    <security-domain name="jcifs.spnego.accept">
      <authentication>
        <login-module code="com.sun.security.auth.module.Krb5LoginModule"
flag="required">
          <module-option name="refreshKrb5Config" value="true"/>
          <module-option name="storeKey" value="true"/>
          <module-option name="principal"
value="HTTP/portal.smc.local@SMC.LOCAL"/>
          <module-option name="keyTab" value="/path/to/liferaysso.keytab"/>
          <module-option name="useKeyTab" value="true"/>
        </login-module>
      </authentication>
    </security-domain>
  <security-domain name="other" cache-type="default">
    <authentication>
```

4.4. LIFERAY

The Kerberos SSO plugin can be hot-deployed and configured through the Liferay Control Panel as shown in “5 PLUGIN KERBEROS SSO”.

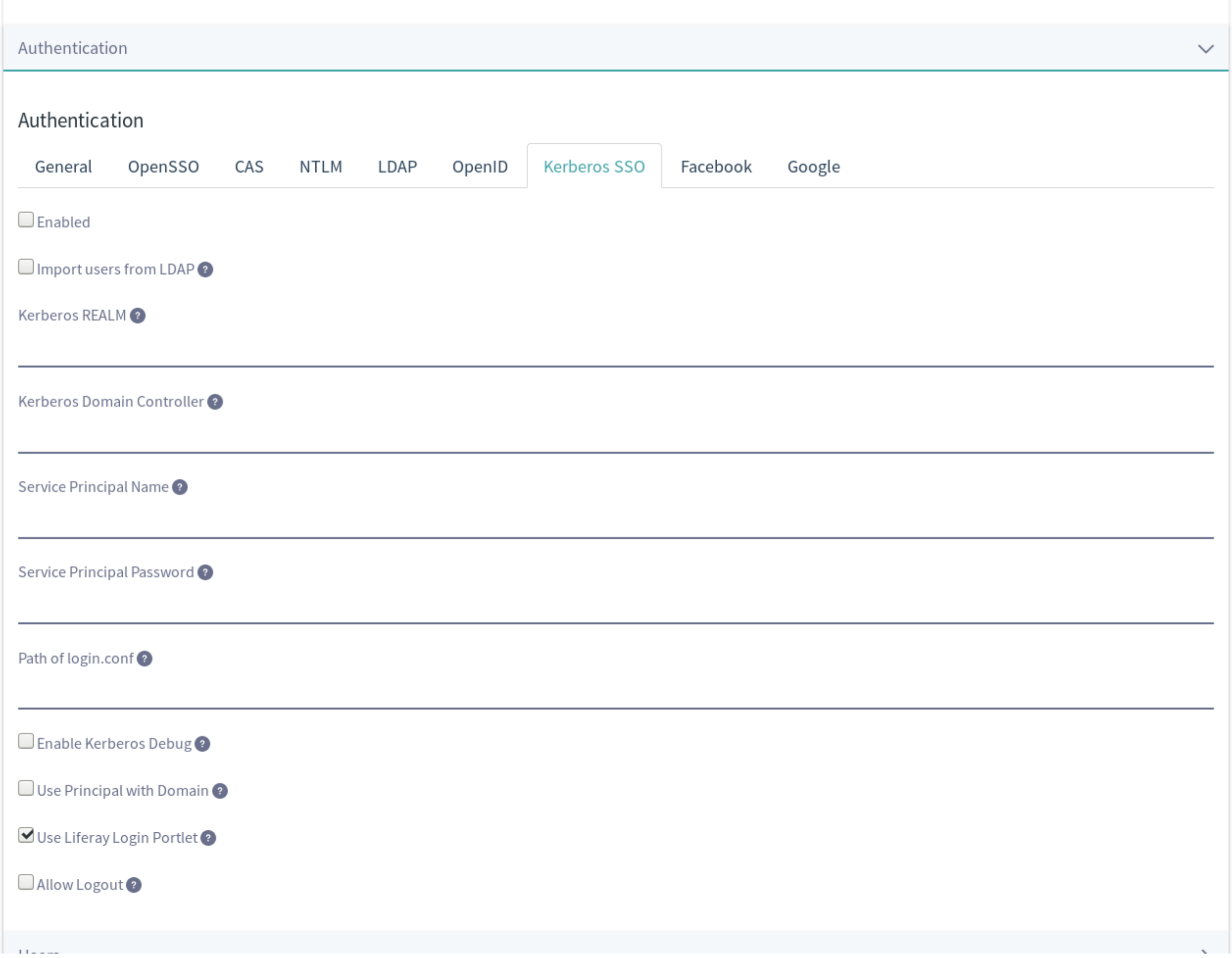
5. PLUGIN KERBEROS SSO

Liferay integrate different authentication solutions or Single SignOn. In compliance with the Liferay authentication infrastructure, SMC has created a plugin to manage the Single SignOn based on the Integrated Windows Authentication. The plugin complies with the specifications stated in RFC 7235.

As stated in chapter "2 INTEGRATED WINDOWS AUTHENTICATION", when the user requests a protected resource through a browser the plugin created by SMC provides a response with status 401 and the header "WWW-Authenticate: Negotiate".

In these scenarios, it is common practice to provide a page with content, typically a login form, to allow access even to those using a non-configured browser.

The plugin is configurable from the Liferay in "Control Panel - Configuration - Instance Settings" as shown in the figure



Authentication

Authentication

General | OpenSSO | CAS | NTLM | LDAP | OpenID | Kerberos SSO | Facebook | Google

□ Enabled

□ Import users from LDAP

Kerberos REALM

Kerberos Domain Controller

Service Principal Name

Service Principal Password

Path of login.conf

□ Enable Kerberos Debug

□ Use Principal with Domain

☑ Use Liferay Login Portlet

□ Allow Logout

Let's see in detail the different configuration options:

- "Enabled"
  Check to enable this authentication mechanism for the Company instance

- “Import users from LDAP”
  After the authentication phase the user must be registered in Liferay. If this option is checked the user details will be searched in the LDAPs previously configured in Liferay. The data (name, surname, email, groups, ...) are updated at each login.

- “Kerberos REALM”
  Set the Realm of the Kerberos Domain that you intend to use for the Single SignOn.
  This property is mandatory

- “Kerberos Domain Controller”
  Set the network name, or rather the IP address, of the domain controller server. It is the server that manages the Active Directory.
  This property is mandatory

- “Service Principal Name”
  Set the Service Principal Name connected to the VirtualHost of the portal. In our scenario it will be "HTTP/portal.smc.local@SMC.LOCAL".
  This property is mandatory

- “Service Principal Password”
  The Service Principal Name password can be explicitly declared in this property. The absence of value indicates that the password will be provided through the ".keytab" file in the manner and restrictions explained below.

- “Path of login.conf”
  Token validation is performed by elements of the "Java Security" framework that are activated by a configuration that depends on the application server used. For Tomcat the configuration provided by our plugin is sufficient (see 4.3 FILE LOGIN.CONF)

- “Enable Kerberos Debug”
  When checked Kerberos components of the JVM will produce debug messages within the log file

- “Use Principal with Domain”
  Kerberos token provides to Liferay the Windows username which is generally in the format "username@domain". Leave unchecked if you want to use only the "username" part to search the user within LDAP.

- “Use Liferay Login Portlet”
  Check if you want to use the Liferay standard Login portlet as a "fallback" mechanism for non-configured browsers. The alternative is a blank page with a minimal form

- “Allow Logout”
  The specifications of the Integrated Windows Authentication declares that the user cannot log out, and the only way to "logout" is to close the browser. The plugin created by SMC allows you to derogate this constraint

For the purposes of this guide the configuration will be:

- "Enabled" = checked
- "Import users from LDAP" = unchecked
- "Kerberos REALM" = "SMC.LOCAL"
- "Kerberos Domain Controller" = "192.168.85.191"
- "Service Principal Name" = "HTTP/portal.smc.local@SMC.LOCAL"
- "Service Principal Password" = "Welcome1"
- "Path of the login.conf file" = empty
- "Enable Kerberos debug" = checked
- "Use the Principal with Domain" = unchecked
- "Use Liferay login portlet" = checked
- "Allow Logout" = unchecked

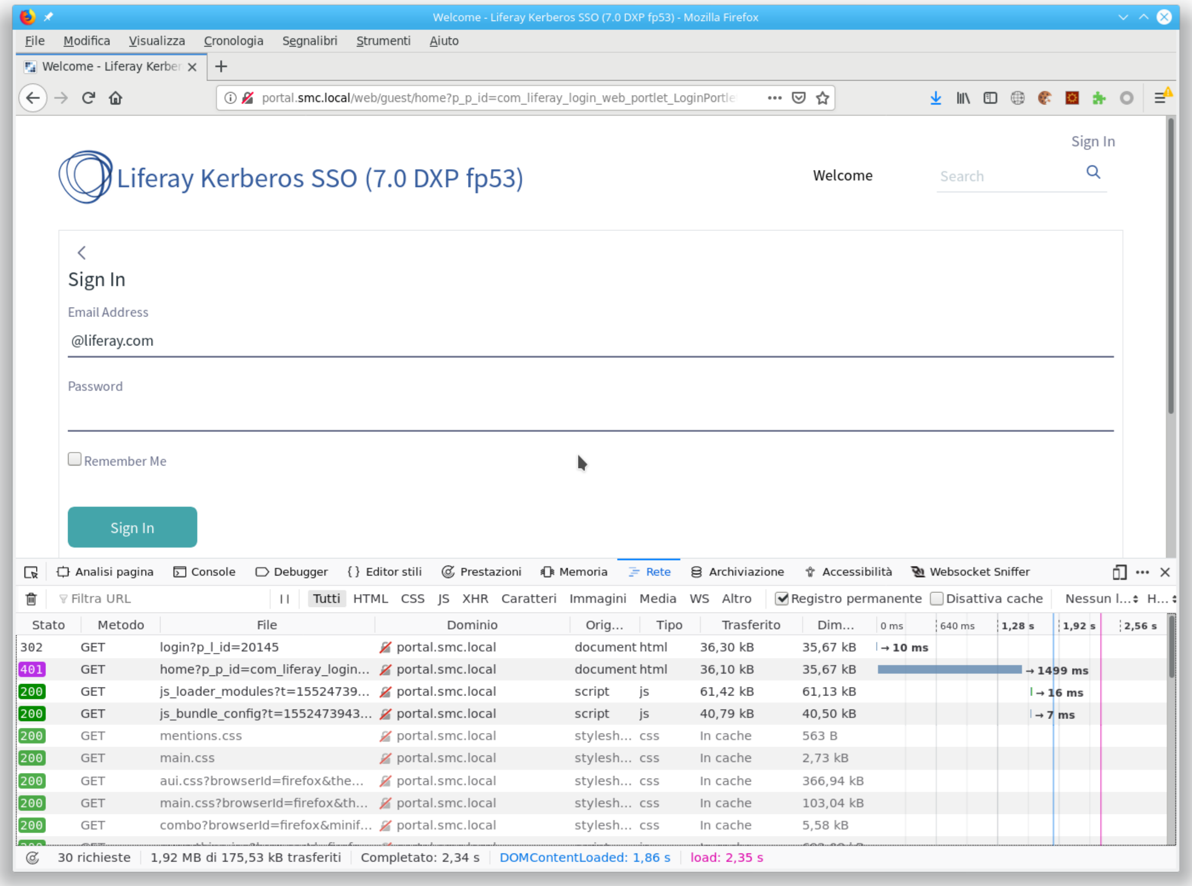
5.1. FIRST TRY

In the scenario used for this guide, users will be pre-registered within Liferay. In a real situation users will probably be recovered from LDAP.

We will use the user “SMC\mauro.mariuzzo” already created in Liferay with “mauro.mariuzzo” as screenName.

After activating the Kerberos SSO we try to access the portal with a Firefox browser not configured to manage the Integrated Windows Authentication: we get the public page "/web/guest/home".

Than we try to access



Welcome - Liferay Kerberos SSO (7.0 DXP fp53) - Mozilla Firefox

portal.smc.local/web/guest/home?p_p_id=com_liferay_login_web_portlet_LoginPortle

Liferay Kerberos SSO (7.0 DXP fp53)

Sign In

Email Address: @liferay.com

Password:

□ Remember Me

Stato	Metodo	File	Dominio	Orig...	Tipo	Trasferito	Dim...	
302	GET	login?p_l_id=20145	portal.smc.local	document	html	36,30 kB	35,67 kB	→ 10 ms
401	GET	home?p_p_id=com_liferay_login...	portal.smc.local	document	html	36,10 kB	35,67 kB	→ 1499 ms
200	GET	js_loader_modules?t=15524739...	portal.smc.local	script	js	61,42 kB	61,13 kB	→ 16 ms
200	GET	js_bundle_config?t=1552473943...	portal.smc.local	script	js	40,79 kB	40,50 kB	→ 7 ms
200	GET	mentions.css	portal.smc.local	stylesh...	css	In cache	563 B	
200	GET	main.css	portal.smc.local	stylesh...	css	In cache	2,73 kB	
200	GET	aui.css?browserId=firefox&the...	portal.smc.local	stylesh...	css	In cache	366,94 kB	
200	GET	main.css?browserId=firefox&th...	portal.smc.local	stylesh...	css	In cache	103,04 kB	
200	GET	combo?browserId=firefox&minif...	portal.smc.local	stylesh...	css	In cache	5,58 kB	

30 richieste | 1,92 MB di 175,53 kB trasferiti | Completato: 2,34 s | DOMContentLoaded: 1,86 s | load: 2,35 s

As you can see from the browser logs, Liferay responded with a 401. Because the browser is not configured to manage Integrated Windows Authentication, the standard login portlet is correctly shown.

6. MICROSOFT WINDOWS WORKSTATION

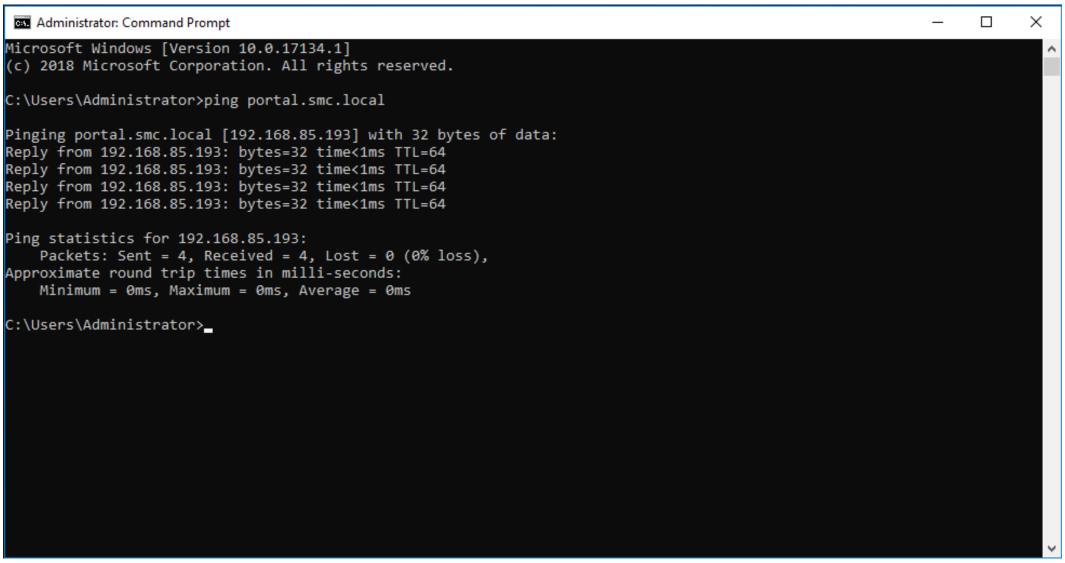
In Windows systems the Integrated Windows Authentication can be used from Internet Explorer, Microsoft Edge, Google Chrome and Mozilla Firefox.

From the configuration point of view it is important to know that:

- Microsoft Edge uses the same libraries and the same configuration as Internet Explorer
- Google Chrome uses the same libraries and the same configuration as Internet Explorer
- Mozilla Firefox uses its own internal component

As a first check, let's make sure that the Windows workstation is able to reach the Liferay server, that is, it is able to resolve the virtual host on which Liferay is exposed.

From a command prompt we execute the ping command

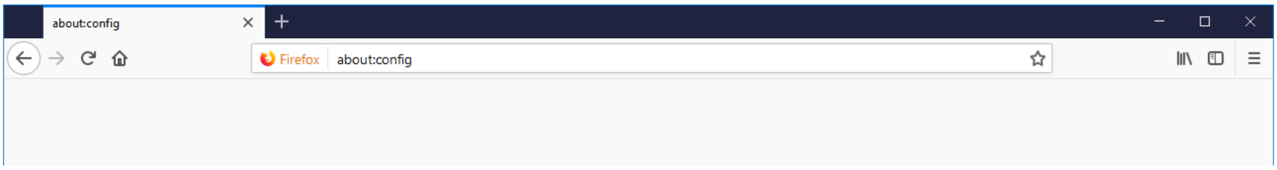


```
Microsoft Windows [Version 10.0.17134.1]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ping portal.smc.local

Pinging portal.smc.local [192.168.85.193] with 32 bytes of data:
Reply from 192.168.85.193: bytes=32 time<1ms TTL=64
Reply from 192.168.85.193: bytes=32 time<1ms TTL=64
Reply from 192.168.85.193: bytes=32 time<1ms TTL=64
Reply from 192.168.85.193: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.85.193:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Administrator>_
```

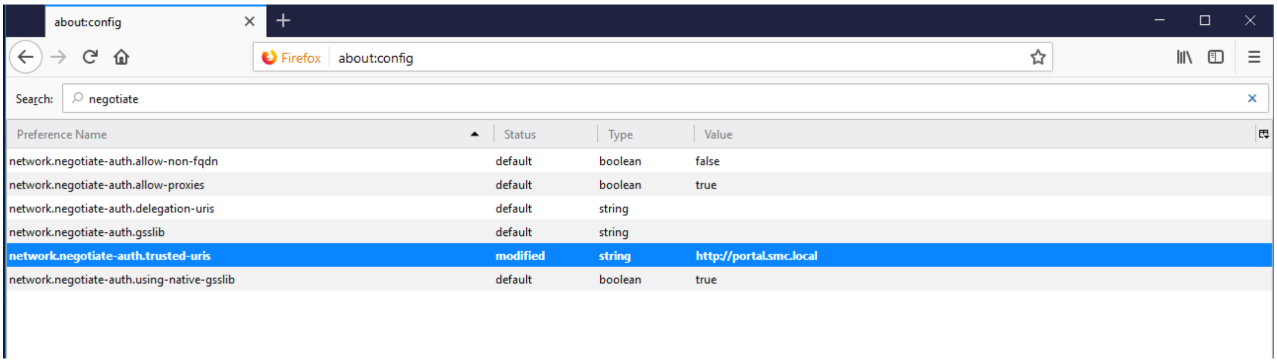
6.1. MOZILLA FIREFOX

Since Firefox uses its own components it is easier to do the first tests with this browser which, among other things, allows you to configure specifically if you want Integrated Windows Authentication using only Kerberos, or only NTLM, or both.

Within the Firefox browser we use the special url "about: config" to enter the configuration section of the special parameters



From this section, by typing "negotiate" on the search box, it is possible view and configure the IWA properties with Kerberos.



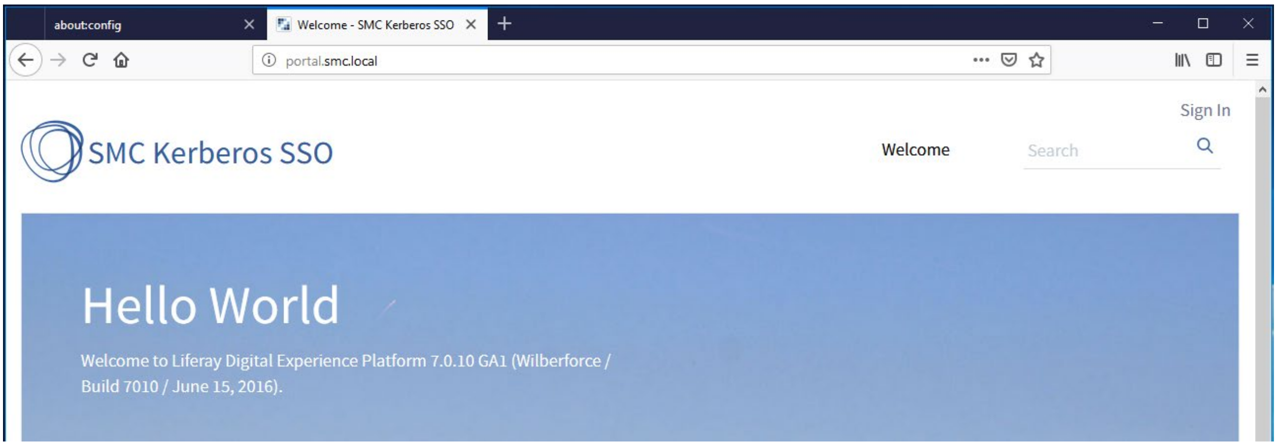
Search: negotiate

Preference Name	Status	Type	Value
network.negotiate-auth.allow-non-fqdn	default	boolean	false
network.negotiate-auth.allow-proxies	default	boolean	true
network.negotiate-auth.delegation-uris	default	string	
network.negotiate-auth.gsslib	default	string	
network.negotiate-auth.trusted-uris	modified	string	http://portal.smc.local
network.negotiate-auth.using-native-gsslib	default	boolean	true

It is enough to modify the property "network.negotiate-auth.trusted-uris" indicating the Virtual Host connected to Liferay; or the Virtual Host used in the definition of the Service Principal Name.

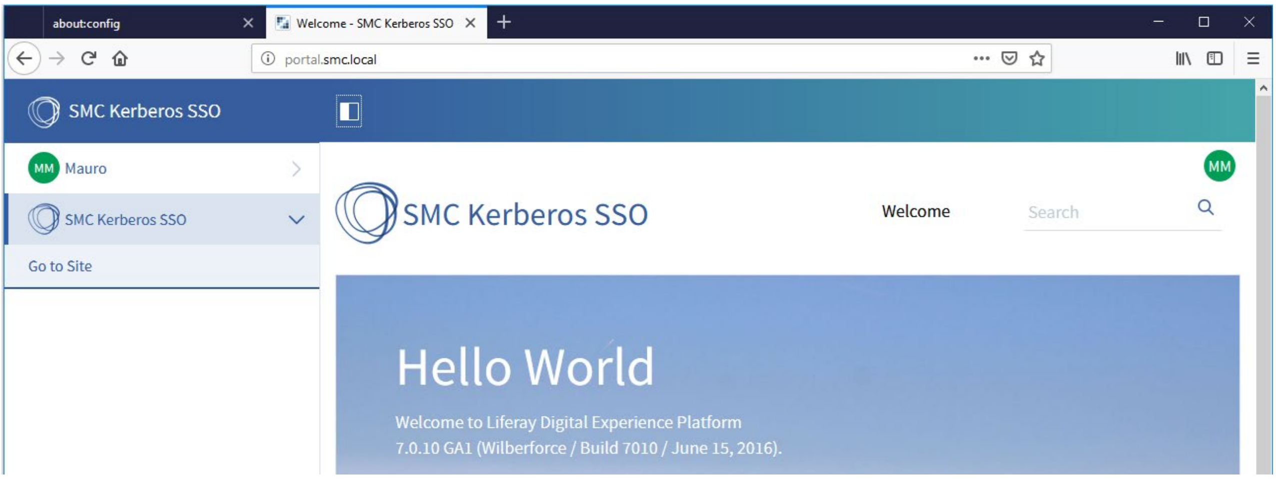
The changes are automatically saved.

From a new tab, or from the same one, we access the public page of the portal.



Welcome to Liferay Digital Experience Platform 7.0.10 GA1 (Wilberforce / Build 7010 / June 15, 2016).

With "Sign In" the authentication mechanism is activated at the end of which we find ourselves again in the "Welcome" page (because it is the default login landing page); but authenticated.



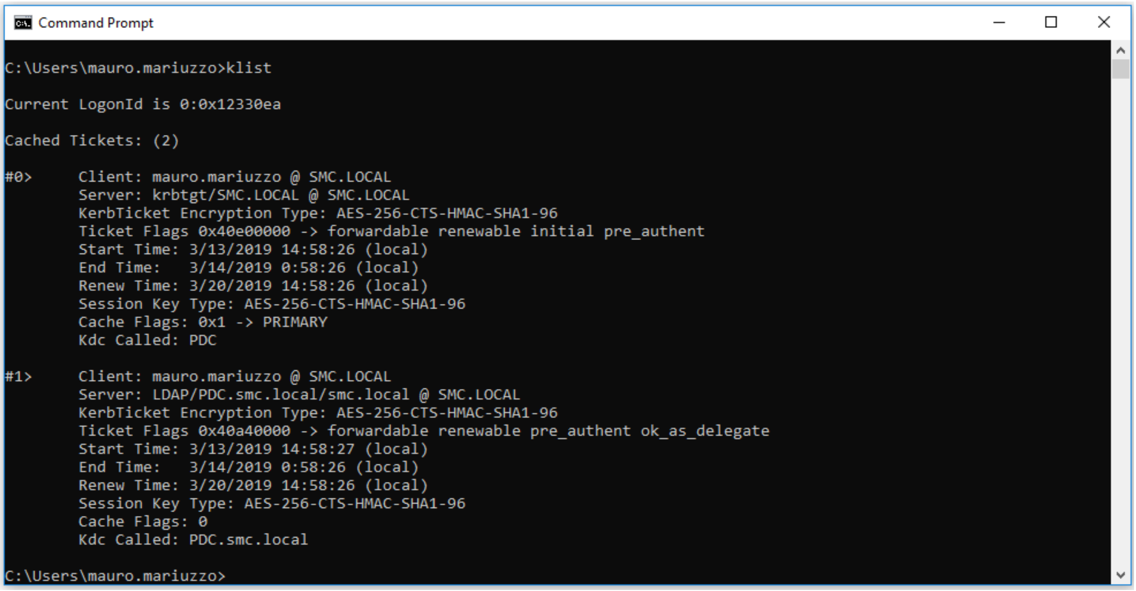
Welcome to Liferay Digital Experience Platform 7.0.10 GA1 (Wilberforce / Build 7010 / June 15, 2016).

Basically:

- the Kerberos plugin responded with 401
- Firefox interacted with the Windows operating system to obtain a valid Kerberos ticket for the workstation user (in our case "SMC\mauro.mariuzzo") for the resource "http://portal.smc.local"

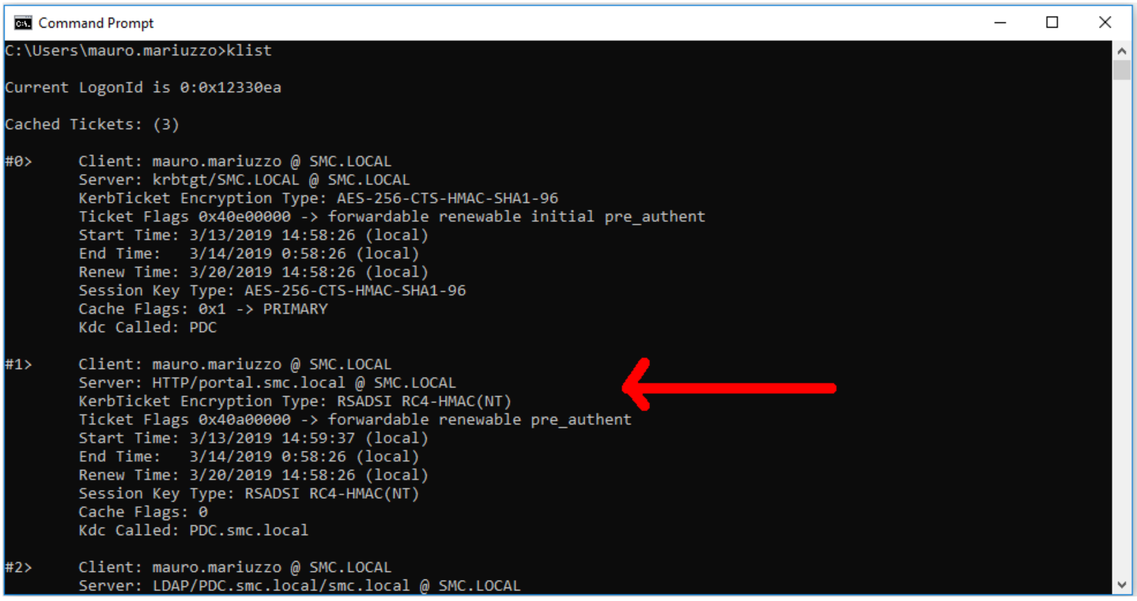
- Firefox sent the ticket to Liferay who validated and retrieved the username "mauro.mariuzzo@SMC.LOCAL"
- in Liferay the user exists and is presented in the browser

As further proof we can compare the outcome of the klist command before and after logging in to Liferay.



```
C:\Users\mauro.mariuzzo>klist

Current LogonId is 0:0x12330ea

Cached Tickets: (2)

#0>     Client: mauro.mariuzzo @ SMC.LOCAL
        Server: krbtgt/SMC.LOCAL @ SMC.LOCAL
        KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
        Ticket Flags 0x40e00000 -> forwardable renewable initial pre_authent
        Start Time: 3/13/2019 14:58:26 (local)
        End Time:   3/14/2019 0:58:26 (local)
        Renew Time: 3/20/2019 14:58:26 (local)
        Session Key Type: AES-256-CTS-HMAC-SHA1-96
        Cache Flags: 0x1 -> PRIMARY
        Kdc Called: PDC

#1>     Client: mauro.mariuzzo @ SMC.LOCAL
        Server: LDAP/PDC.smc.local/smc.local @ SMC.LOCAL
        KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
        Ticket Flags 0x40a40000 -> forwardable renewable pre_authent ok_as_delegate
        Start Time: 3/13/2019 14:58:27 (local)
        End Time:   3/14/2019 0:58:26 (local)
        Renew Time: 3/20/2019 14:58:26 (local)
        Session Key Type: AES-256-CTS-HMAC-SHA1-96
        Cache Flags: 0
        Kdc Called: PDC.smc.local

C:\Users\mauro.mariuzzo>
```

Known tickets before accessing the portal



```
C:\Users\mauro.mariuzzo>klist

Current LogonId is 0:0x12330ea

Cached Tickets: (3)

#0>     Client: mauro.mariuzzo @ SMC.LOCAL
        Server: krbtgt/SMC.LOCAL @ SMC.LOCAL
        KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
        Ticket Flags 0x40e00000 -> forwardable renewable initial pre_authent
        Start Time: 3/13/2019 14:58:26 (local)
        End Time:   3/14/2019 0:58:26 (local)
        Renew Time: 3/20/2019 14:58:26 (local)
        Session Key Type: AES-256-CTS-HMAC-SHA1-96
        Cache Flags: 0x1 -> PRIMARY
        Kdc Called: PDC

#1>     Client: mauro.mariuzzo @ SMC.LOCAL
        Server: HTTP/portal.smc.local @ SMC.LOCAL
        KerbTicket Encryption Type: RSADSI RC4-HMAC(NT)
        Ticket Flags 0x40a00000 -> forwardable renewable pre_authent
        Start Time: 3/13/2019 14:59:37 (local)
        End Time:   3/14/2019 0:58:26 (local)
        Renew Time: 3/20/2019 14:58:26 (local)
        Session Key Type: RSADSI RC4-HMAC(NT)
        Cache Flags: 0
        Kdc Called: PDC.smc.local

#2>     Client: mauro.mariuzzo @ SMC.LOCAL
        Server: LDAP/PDC.smc.local/smc.local @ SMC.LOCAL
```

Known tickets after accessing the portal

This shows that:

- before accessing the Login page, the Windows session tends not to have a token to access the portal
- in order to send the Kerberos token to Liferay the browser asks the operating system to "negotiate" it with the Domain Controller. At the end of this client-only phase the Windows workstation will have a Token relative to the Service Principal Name

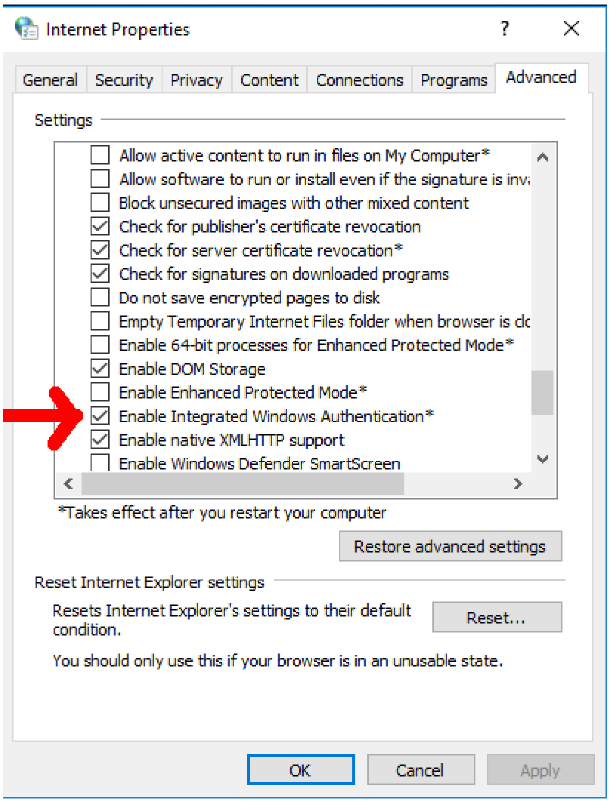
6.2. INTERNET EXPLORER

In Windows systems, the Internet Explorer browser is enabled by default to manage the Integrated Windows Authentication. However, unlike Mozilla Firefox, it is not possible to decide which authentication mechanism will be used by the Browser between Kerberos and NTLM.

The same logic also applies to Microsoft Edge and Google Chrome as they take advantage of the same configuration as Internet Explorer.

To verify that the IWA is enabled, access the "Internet Options" tool and

- go to the "Advanced" tab
- in the "Settings" box look for "Enable Integrated Windows Authentication"



☐ Allow active content to run in files on My Computer*
☐ Allow software to run or install even if the signature is inv
☐ Block unsecured images with other mixed content
☑ Check for publisher's certificate revocation
☑ Check for server certificate revocation*
☑ Check for signatures on downloaded programs
☐ Do not save encrypted pages to disk
☐ Empty Temporary Internet Files folder when browser is clc
☐ Enable 64-bit processes for Enhanced Protected Mode*
☑ Enable DOM Storage
☐ Enable Enhanced Protected Mode*
☑ Enable Integrated Windows Authentication*
☑ Enable native XMLHTTP support
☐ Enable Windows Defender SmartScreen

*Takes effect after you restart your computer

Reset Internet Explorer settings

Resets Internet Explorer's settings to their default condition.

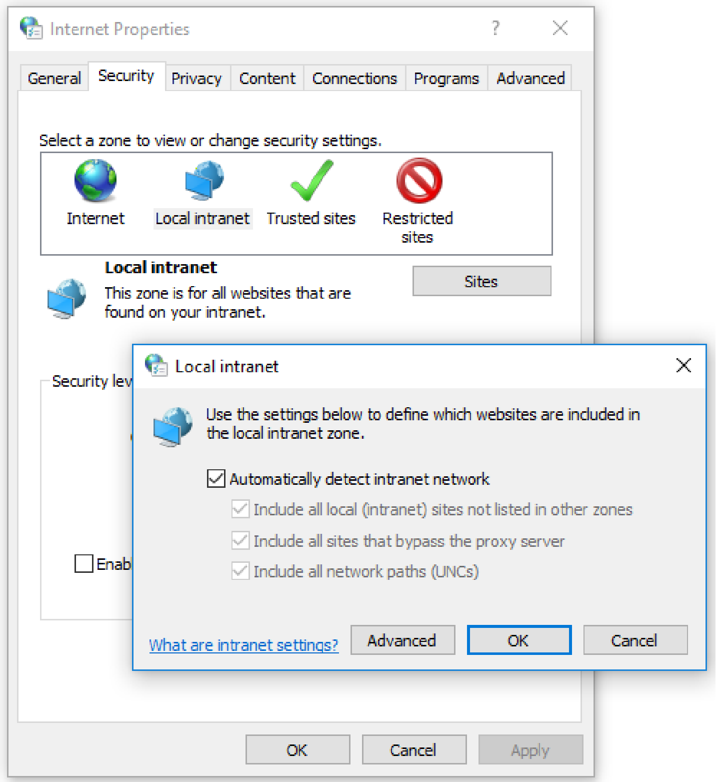
You should only use this if your browser is in an unusable state.

Having verified that the management is active, we must register the VirtualHost of the portal among the sites for which it is possible to use the IWA.

Since version 10 of Internet Explorer, the negotiation phase is started only for the sites explicitly indicated as being part of the local Intranet.

Again, from the "Internet Options" tool

- go to the "Security" tab
- select "Local Intranet" and then click on the "Sites" button.



Select a zone to view or change security settings.

Local intranet

This zone is for all websites that are found on your intranet.

Local intranet

Use the settings below to define which websites are included in the local intranet zone.

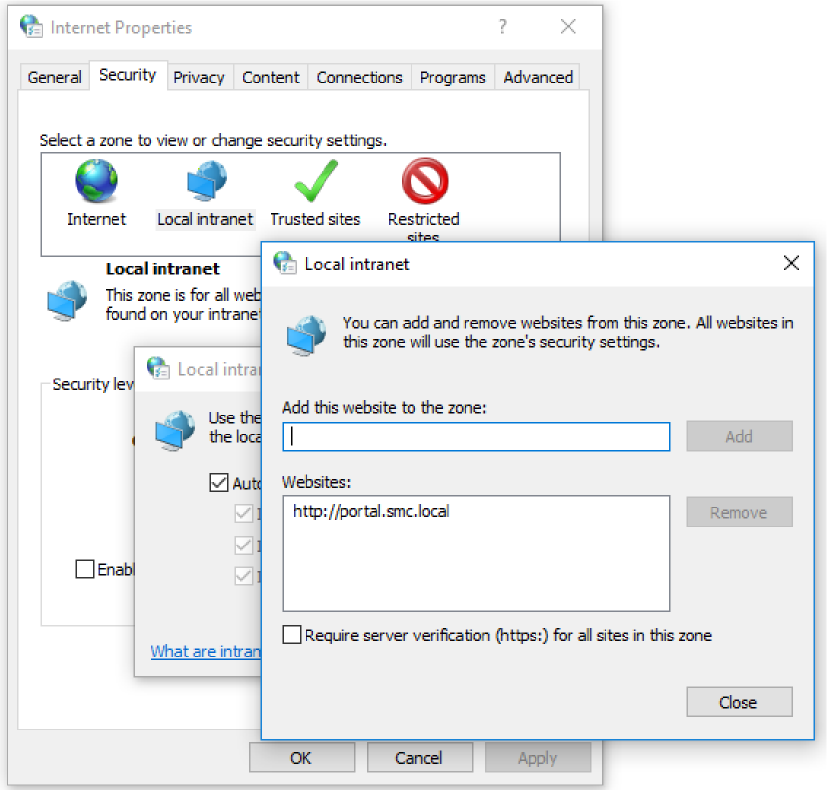
☑ Automatically detect intranet network

☑ Include all local (intranet) sites not listed in other zones

☑ Include all sites that bypass the proxy server

☑ Include all network paths (UNCs)

- On the window that appears, make sure that "Automatically detect intranet network" and all its childred are checked and click on the "Advanced" button



Select a zone to view or change security settings.

Local intranet

This zone is for all web found on your intrane

Local intranet

You can add and remove websites from this zone. All websites in this zone will use the zone's security settings.

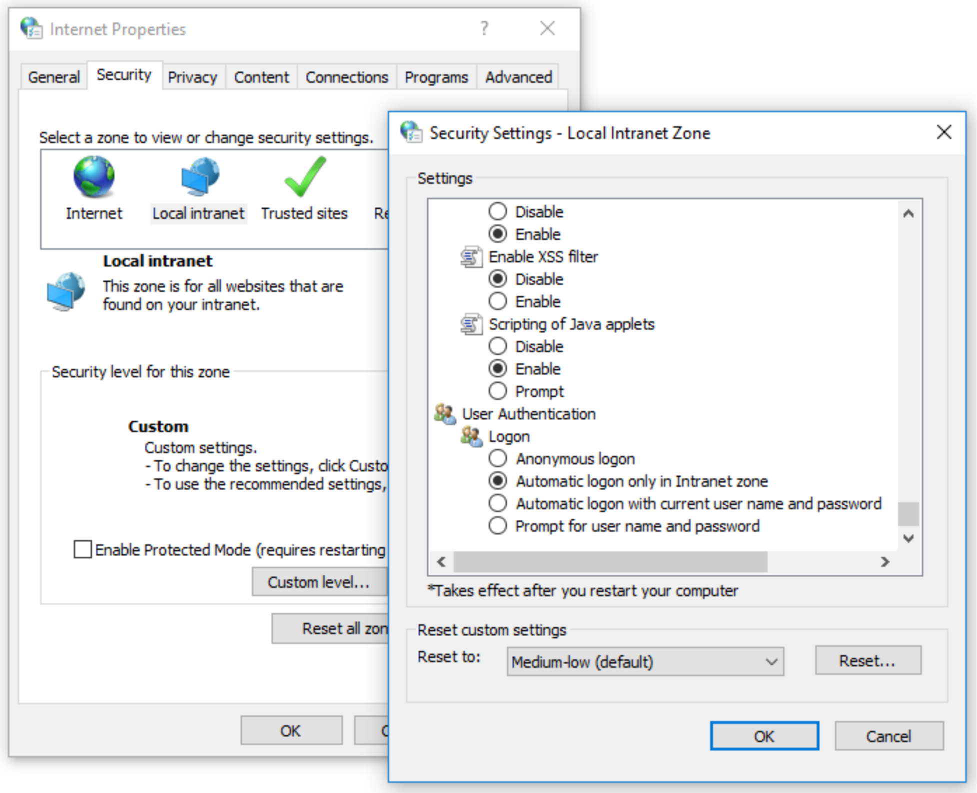
Add this website to the zone:

Websites:

http://portal.smc.local

□ Require server verification (https:) for all sites in this zone

- add the portal's VirtualHost among the sites to be considered as "Local Intranet"
- Save with "OK" to return to the options screen for the Local Intranet
- Click on the "Custom level" button and in the dialog that appears make sure that "Automatic access only in the Intranet area" is selected in the "User authentication" block



Internet Properties

General | Security | Privacy | Content | Connections | Programs | Advanced

Select a zone to view or change security settings.

Internet | Local intranet | Trusted sites | Re

Local intranet
This zone is for all websites that are found on your intranet.

Security level for this zone

Custom
Custom settings.
- To change the settings, click Custo
- To use the recommended settings,

□ Enable Protected Mode (requires restarting

Custom level... | Reset all zon

OK | C

Security Settings - Local Intranet Zone

Settings

○ Disable
● Enable
Enable XSS filter
● Disable
○ Enable
Scripting of Java applets
○ Disable
● Enable
○ Prompt
User Authentication
Logon
○ Anonymous logon
● Automatic logon only in Intranet zone
○ Automatic logon with current user name and password
○ Prompt for user name and password

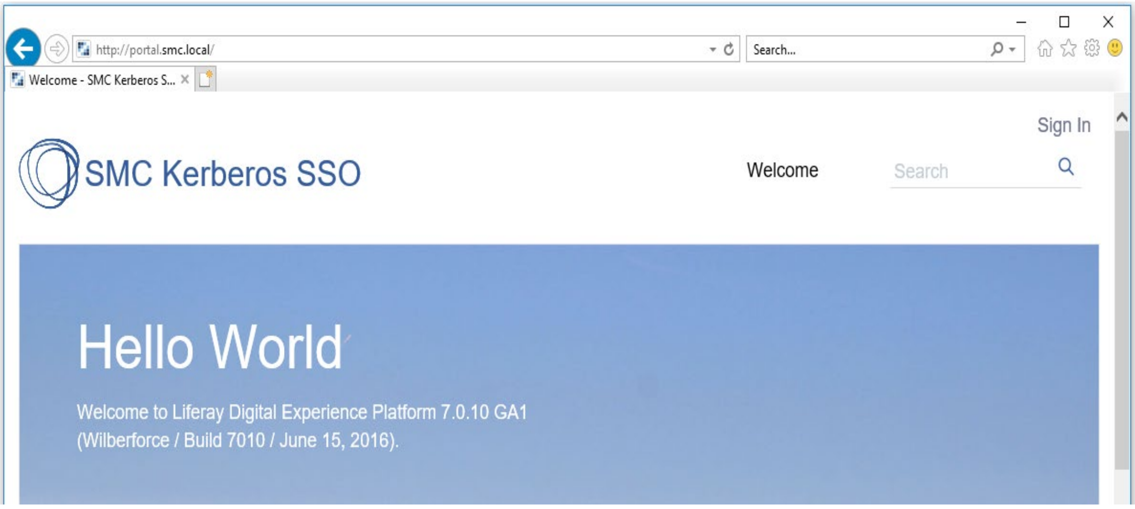
*Takes effect after you restart your computer

Reset custom settings
Reset to: Medium-low (default) | Reset...

OK | Cancel

- Confirm the configuration with "OK"

Using Internet Explorer 11, access the public page of the portal and then click on "Sign In". The authentication mechanism is activated at the end of which we find ourselves on the "Welcome" page (as Login Landing Page); but authenticated.



http://portal.smc.local/

Welcome - SMC Kerberos S...

Sign In

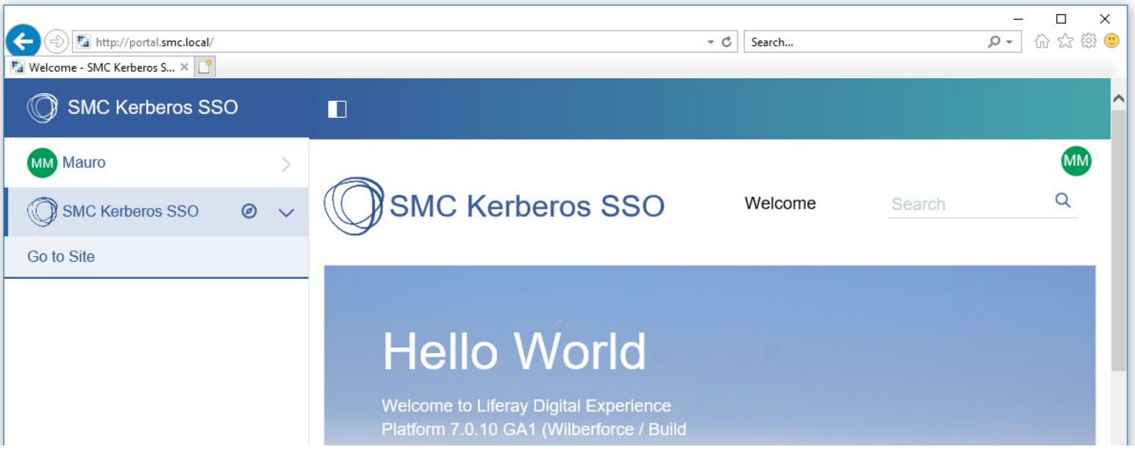
SMC Kerberos SSO

Welcome

Search

Hello World

Welcome to Liferay Digital Experience Platform 7.0.10 GA1 (Wilberforce / Build 7010 / June 15, 2016).

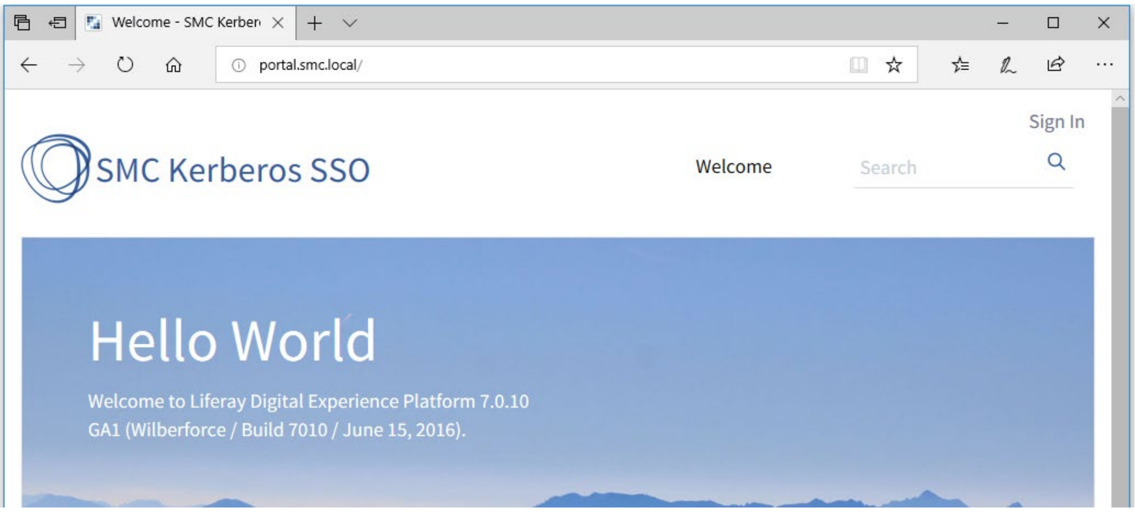


Hello World

Welcome to Liferay Digital Experience Platform 7.0.10 GA1 (Wilberforce / Build

6.3. MICROSOFT EDGE

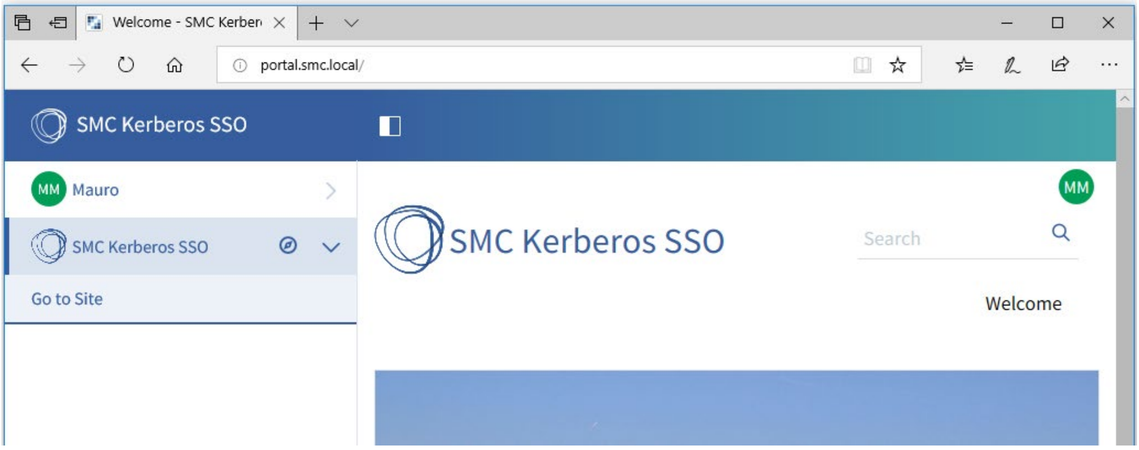
This browser uses the same components and the same configuration of Internet Explorer.



Hello World

Welcome to Liferay Digital Experience Platform 7.0.10 GA1 (Wilberforce / Build 7010 / June 15, 2016).

Access to portal public page



Login landing page after click on “Sign In”

7. WORKSTATION ON DIFFERENT DOMAIN

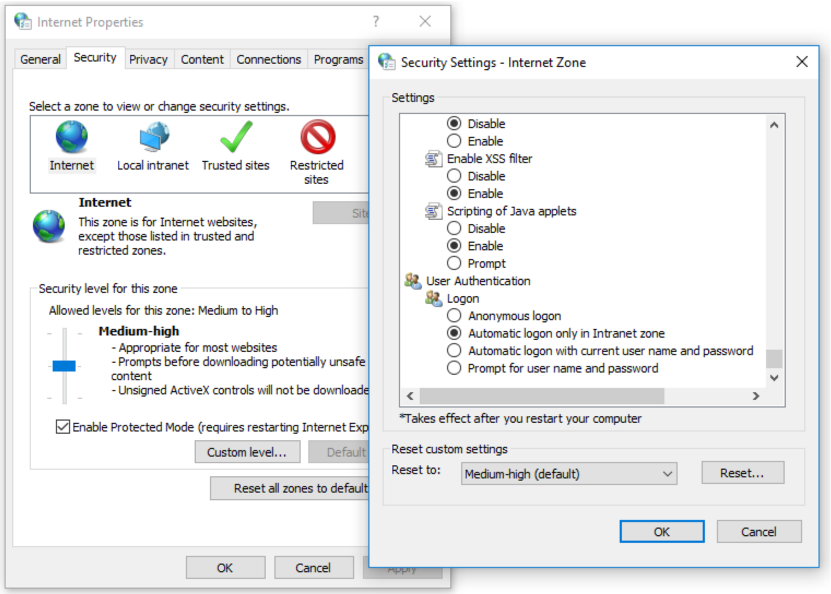
When the access is made from a workstation and / or user registered on a domain other than the one connected to the Service Principal Name (in our case SMC.LOCAL); we expect that Kerberos will not be used.

7.1. INTERNET EXPLORER

From a workstation joined on a different Active Directory domain not connected to "SMC.LOCAL" to which we have accessed with a user not present in the "SMC.LOCAL" domain, we use Internet Explorer to access the portal.

Before doing so, thanks to the "Internet Options" tool, we verify that:

- in the "Local Intranet" section, automatic access is only provided for resources that are registered as "Intranet"



Internet Properties

Select a zone to view or change security settings.

Internet
This zone is for Internet websites, except those listed in trusted and restricted zones.

Security level for this zone
Allowed levels for this zone: Medium to High
Medium-high
- Appropriate for most websites
- Prompts before downloading potentially unsafe content
- Unsigned ActiveX controls will not be downloade

☑ Enable Protected Mode (requires restarting Internet Exp

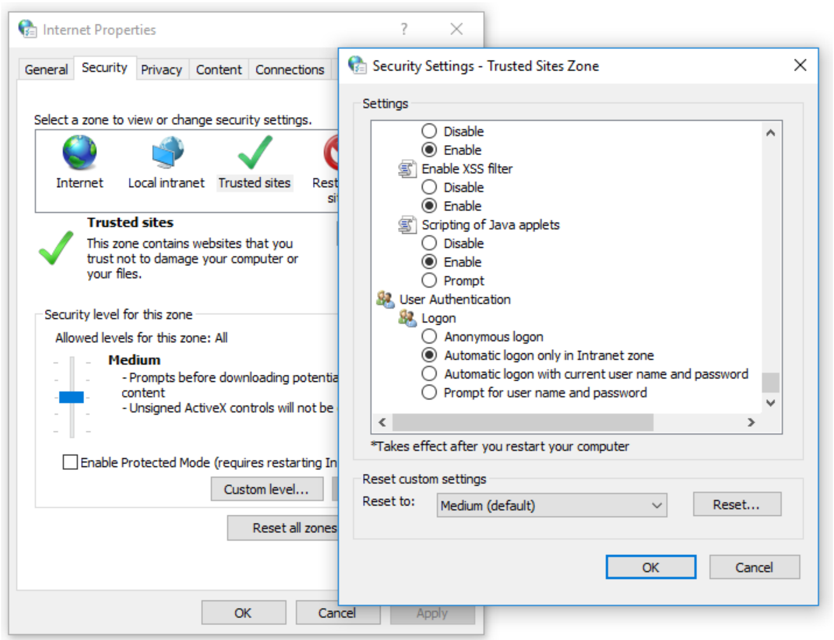
Security Settings - Internet Zone

Settings
● Disable
○ Enable
Enable XSS filter
○ Disable
● Enable
Scripting of Java applets
○ Disable
● Enable
○ Prompt
User Authentication
Logon
○ Anonymous logon
● Automatic logon only in Intranet zone
○ Automatic logon with current user name and password
○ Prompt for user name and password

*Takes effect after you restart your computer

Reset custom settings
Reset to: Medium-high (default)

- also in the "Trusted Sites" section, automatic access is allowed only for resources registered as "Intranet"



Internet Properties

General | Security | Privacy | Content | Connections

Select a zone to view or change security settings.

Internet | Local intranet | Trusted sites | Rest si

Trusted sites

This zone contains websites that you trust not to damage your computer or your files.

Security level for this zone

Allowed levels for this zone: All

Medium

- Prompts before downloading potentia content
- Unsigned ActiveX controls will not be

☐ Enable Protected Mode (requires restarting In

Custom level... | Reset all zones

OK | Cancel | Apply

Security Settings - Trusted Sites Zone

Settings

○ Disable
● Enable
Enable XSS filter
○ Disable
● Enable
Scripting of Java applets
○ Disable
● Enable
○ Prompt
User Authentication
Logon
○ Anonymous logon
● Automatic logon only in Intranet zone
○ Automatic logon with current user name and password
○ Prompt for user name and password

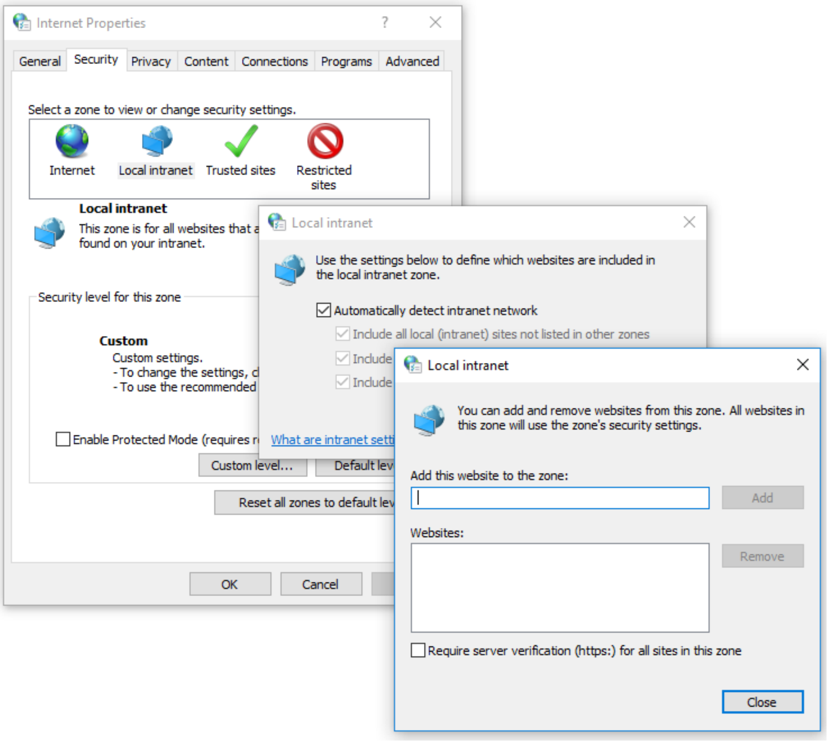
*Takes effect after you restart your computer

Reset custom settings

Reset to: Medium (default) | Reset...

OK | Cancel

- The "http: //portale.smc.local" resource is not registered either as a reliable site or as an Intranet site



Internet Properties

General | Security | Privacy | Content | Connections | Programs | Advanced

Select a zone to view or change security settings.

Internet | Local intranet | Trusted sites | Restricted sites

Local intranet

This zone is for all websites that a found on your intranet.

Security level for this zone

Custom

Custom settings.
- To change the settings, c
- To use the recommended

☐ Enable Protected Mode (requires r

Custom level... | Default lev

Reset all zones to default lev

OK | Cancel

Local intranet

Use the settings below to define which websites are included in the local intranet zone.

☑ Automatically detect intranet network

☑ Include all local (intranet) sites not listed in other zones

☑ Include

☑ Include

What are intranet setti

Local intranet

You can add and remove websites from this zone. All websites in this zone will use the zone's security settings.

Add this website to the zone:

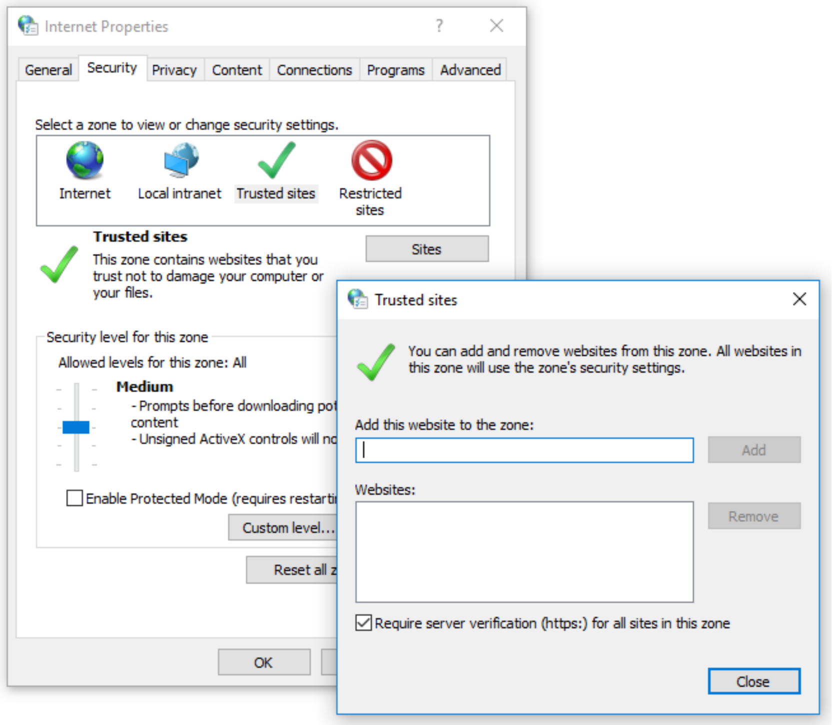
Add

Websites:

Remove

☐ Require server verification (https:) for all sites in this zone

Close



Internet Properties

Select a zone to view or change security settings.

Trusted sites

This zone contains websites that you trust not to damage your computer or your files.

Security level for this zone

Allowed levels for this zone: All

Medium

- Prompts before downloading pot
content
- Unsigned ActiveX controls will no

□ Enable Protected Mode (requires restarti

Trusted sites

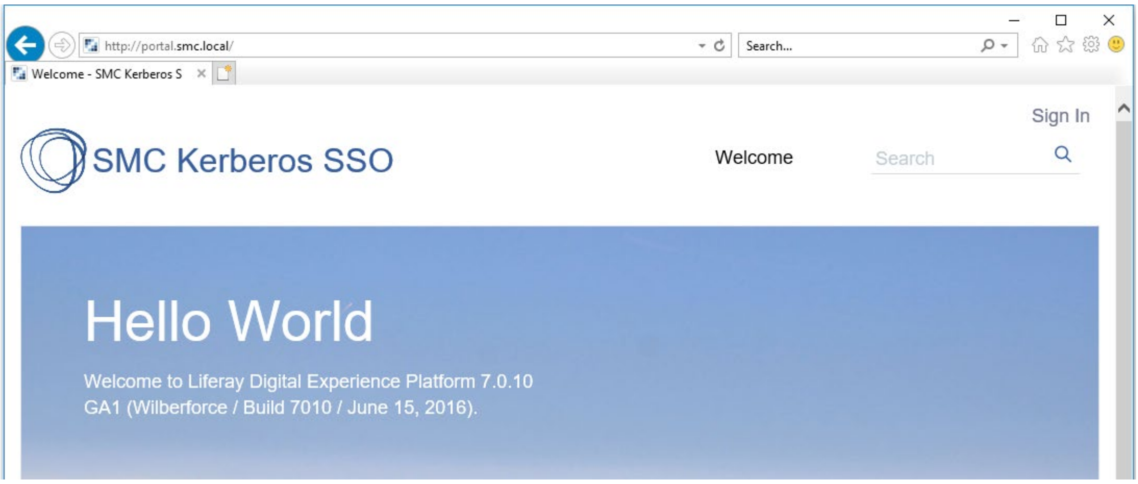
You can add and remove websites from this zone. All websites in this zone will use the zone's security settings.

Add this website to the zone:

Websites:

☑ Require server verification (https:) for all sites in this zone

Open the browser to the public page of the portal to confirm that this is reachable from the workstation



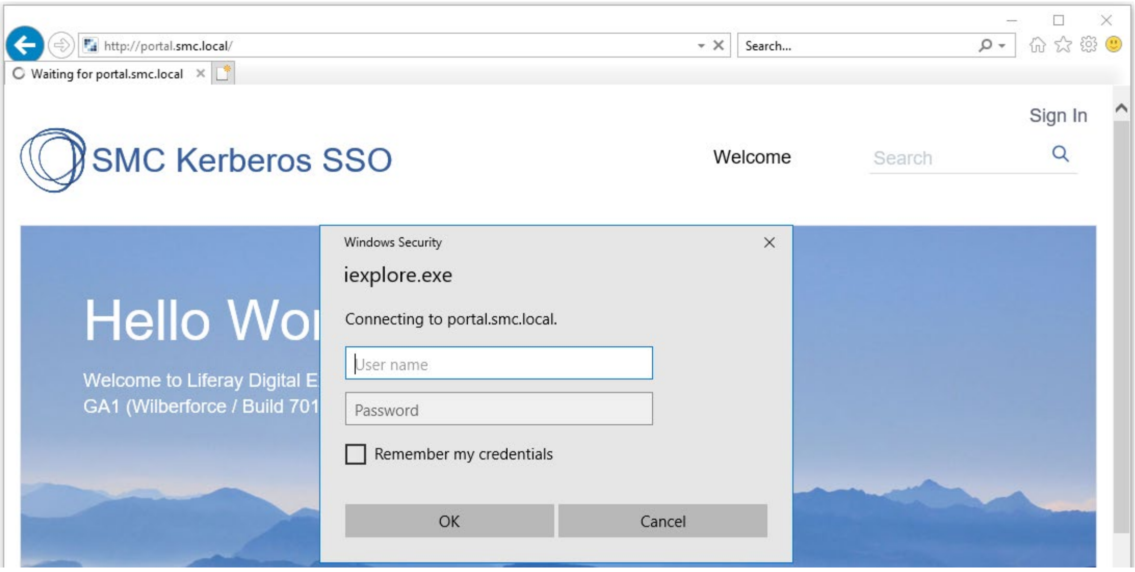
http://portal.smc.local/

Hello World

Welcome to Liferay Digital Experience Platform 7.0.10 GA1 (Wilberforce / Build 7010 / June 15, 2016).

Click on "Sign In" to activate the process of negotiating the authentication token. Since we do not meet the requirements to obtain a Kerberos token we expect not to be automatically recognized.

Having no indication on how to treat the site "http://portale.smc.local" Internet Explorer, which is designed to use NTLM when it cannot use Kerberos, presents us with a form for entering credentials (we are in phase 4 described in chapter "2.1 OPERATIONAL FLOW").



http://portal.smc.local/
Search...
Waiting for portal.smc.local
SMC Kerberos SSO
Welcome
Search
Sign In
Hello Wo
Welcome to Liferay Digital E
GA1 (Wilberforce / Build 701
User name
Password
□ Remember my credentials
OK
Cancel

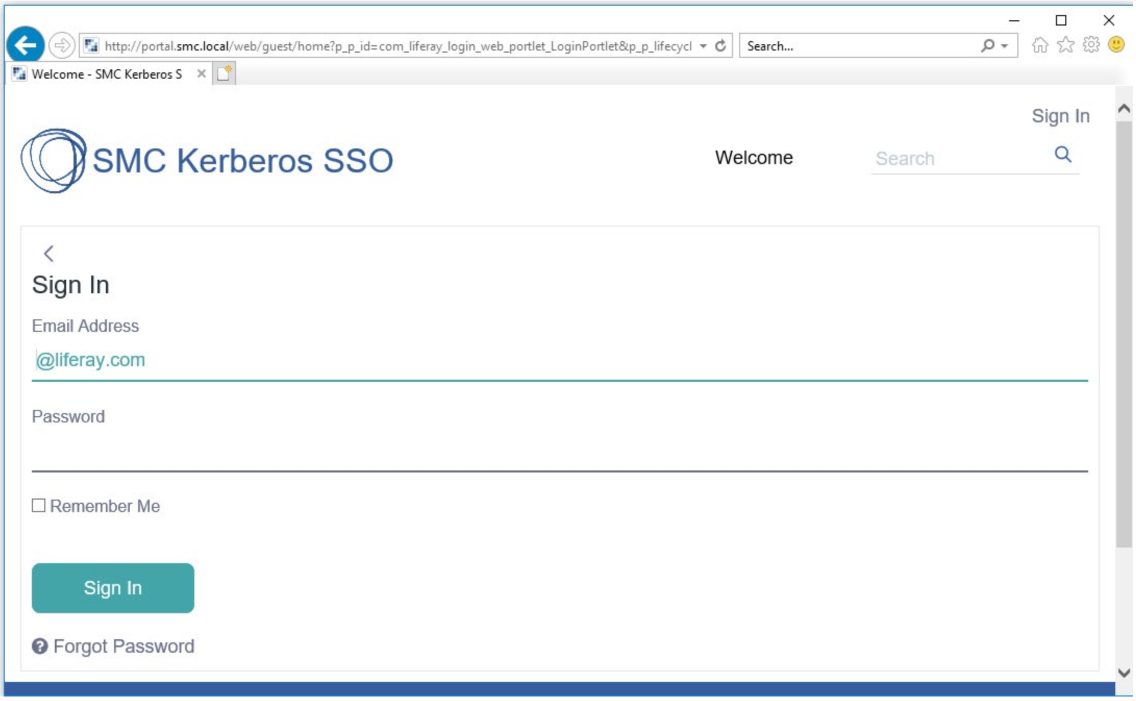
Windows Security

iexplore.exe

Connecting to portal.smc.local.

A modal window appears that makes us understand that Internet Explorer has received the answer with a 401 result and asks us to identify ourselves, still before analyzing the content of the response provided by Liferay.

Here **the only correct action is to press Cancel**, to display the Liferay Login page.



If, instead, we insert the credentials these are supplied to Liferay as NTLMSSP token, as can be seen from the logs

```
2019-03-13 16:41:48.718 DEBUG [ajp-nio-10019-exec-4][SpnegoFilter:205] header=Negotiate
TlRMTVNTUAABAAAAl4II4gAAAAAAAAAAAAAAAAAAAAAAKAO5CAAAADw==
2019-03-13 16:41:48.719 DEBUG [ajp-nio-10019-exec-4][SpnegoFilter:298] authorization=Negotiate
TlRMTVNTUAABAAAAl4II4gAAAAAAAAAAAAAAAAAAAAAAKAO5CAAAADw==
2019-03-13 16:41:48.719 DEBUG [ajp-nio-10019-exec-4][SpnegoFilter:309] Obtained token =
NTLMSSP_____��_�__________________�B____ [Sanitized]
2019-03-13 16:41:48.720 DEBUG [ajp-nio-10019-exec-4][SpnegoFilter:316] Because NTLMSSP return on standard
flow - begin
```

This token is not accepted by our plugin which does not authenticate us. Unfortunately, entering credentials lets us enter the short-circuit described in "8.3 SHORT CIRCUIT NTLMSSP".

If, on the other hand, the portal url "http://portal.smc.local" is registered as a "Local Intranet" or as a "Trusted site", the NTLMSSP token is automatically generated without presenting the modal form. The fact remains that even in this case we enter the short circuit described in "8.3 SHORT CIRCUIT NTLMSSP".

7.2. MOZILLA FIREFOX

This browser uses its own component to manage the Integrated Windows Authentication.

When we use a Firefox:

- that does not have "portale.smc.local" set as an URI configured for IWA, thenthe Liferay login page is presented
- that has "portale.smc.local" set as an URI configured for IWA, then an NTLMSSP token will be sent to Liferay. Token that will be rejected and will get us into the short-circuit described in "8.3 SHORT CIRCUIT NTLMSSP"

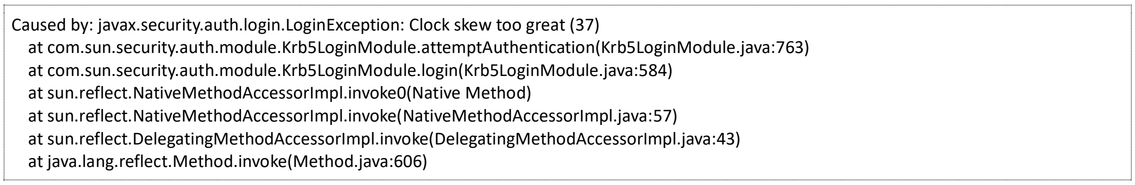
In both scenarios no modal login form will be presented to the user

8. TROUBLESHOOTING

8.1. CLOCK SKEW

As stated in chapter "4.1 TIME" the systems involved must be time synchronized with a maximum deviation of 5 minutes.

The presence of this stack trace in the Liferay log during the Kerberos token decoding indicates that the time of the Linux server hosting Liferay is not aligned with that of the other actors

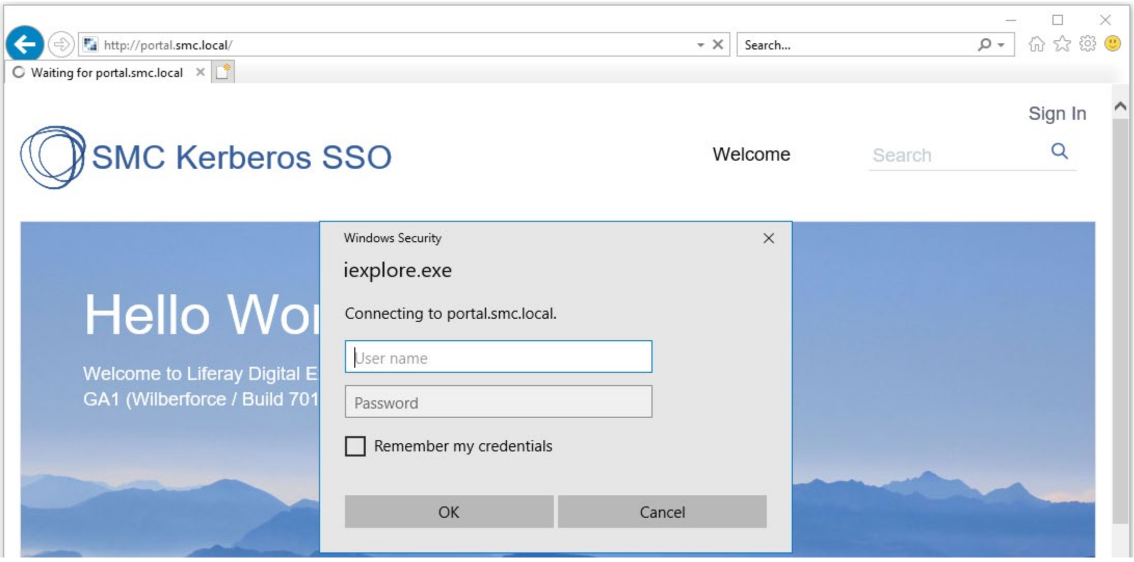


```
Caused by: javax.security.auth.login.LoginException: Clock skew too great (37)
   at com.sun.security.auth.module.Krb5LoginModule.attemptAuthentication(Krb5LoginModule.java:763)
   at com.sun.security.auth.module.Krb5LoginModule.login(Krb5LoginModule.java:584)
   at sun.reflect.NativeMethodAccessorImpl.invoke0(Native Method)
   at sun.reflect.NativeMethodAccessorImpl.invoke(NativeMethodAccessorImpl.java:57)
   at sun.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAccessorImpl.java:43)
   at java.lang.reflect.Method.invoke(Method.java:606)
```

8.2. INTERNET EXPLORER - SITI ATTENDIBILI

Internet Explorer should be able to use trusted sites to indicate that a certain VirtualHost is to be considered part of the Local Intranet, and therefore involved in Integrated Windows Authentication. As indicated in chapter "6.2 INTERNET EXPLORER" this is no longer sufficient.

Acting only on trusted sites Internet Explorer refuses to negotiate a Kerberos token and prepares to use NTLM. The consequence of this step is the almost certain appearance of a modal request form for credentials.



http://portal.smc.local/
Search...
Waiting for portal.smc.local
SMC Kerberos SSO
Welcome
Search
Sign In
Hello Wo
Welcome to Liferay Digital E
GA1 (Wilberforce / Build 701

Windows Security

iexplore.exe

Connecting to portal.smc.local.

User name
Password
□ Remember my credentials
OK
Cancel

This happens because in Internet Explorer (Microsoft Edge and Google Chrome) it is not possible to set which authentication mechanism to use, this will be selected between Kerberos and NTLM based on the context and the rules decided by Microsoft.

8.3. SHORT CIRCUIT NTLMSSP

The specifications of the Integrated Windows Authentication establishes that once the authentication phase has begun (point 3 of the flow described in "2.1 OPERATING FLOW") this must be completed.

The possible conclusions are:

- the token is acknowledged and the user is authenticated
- an error page is returned and the browser must be closed

Until the flow ends, any POST made by the browser is empty: the post-data is removed. This is because the browser respects the specifications that impose this behavior.

When our plugin receives an NTLMSSP token, it still presents the Liferay login portlet but it will still not be possible to access because "username" and "password" will never be sent by the browser.

9. USEFUL DOCUMENTATION

Some useful references

- "https://tools.ietf.org/html/rfc7235" reference specification for Negotiate
- "https://www.ietf.org/rfc/rfc2478.txt" reference specification of the SPNEGO component implemented by the standard jcifs library used by Liferay
- "http://www.oracle.com/technetwork/articles/idm/weblogic-sso-kerberos-1619890.html" the documentation to use the Integrated Windows Authentication on a webapp exposed by Oracle WebLogic
- "http://clintboessen.blogspot.it/2013/09/ie-10-prompting-for-credentials-windows.html" some hints on how to check why Internet Explorer shows a credential entry form
- "https://ping.force.com/Support/PingFederate/Integrations/How-to-configure-supported-browsers-for-Kerberos-NTLM" some instructions on how to configure browsers and understand the logic with which Internet Explorer chooses the authentication mechanism