

# IWA\_FAILOVER\_FORM LOGIN

B.K. Rhim

## IWA\_FAILOVER\_FORM LOGIN

- There is sample file in community site but it is not working in Chrome or FireFox browser due to active X
- CA SSO has roadmap to support this feature but it is not available at this moment as out of the box
- Need something work in CA SSO R12.5X environment
- JSP based code which can be used CA Access Gateway (aka Secure Proxy Server)

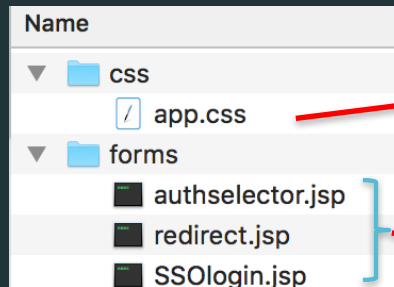
## Prerequisites

- SSO environment is ready
- Access Gateway (Secure Proxy Server) server is running properly.
- Windows Authentication (IWA) login is configured and working fine.

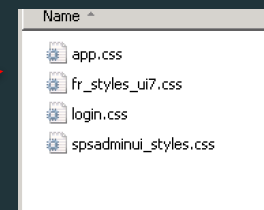
# Preparation

1. Unzip the files and copy it into  
CA Access gateway server

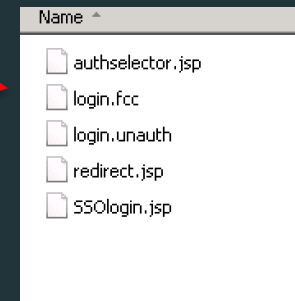
<Access Gateway Install folder>\secure-proxy\Tomcat\webapps\proxyui\



"css" folder



"forms" folder



# Preparation

## 2. Create Windows Authentication scheme

**Scheme Common Setup**

- Authentication Scheme Type: Windows Authentication Template
- Protection Level: 5 [1-1,000, higher is more secure]
- ☒ Password Policies enabled for this Authentication Scheme

**Scheme Setup**

This scheme supports: ☒ Active Directory / LDAP, ☐ Win NT

☐ Use Relative Target

- Server Name: smsserver.forwardinc.ca
- Port: 9090
- ☐ Use SSL Connection
- Target: /proxyui/forms/authselector.jsp
- User DN Lookup: (sAMAccountName=%{UID})

Windows Authentication Scheme

Access Gateway Server Server name, port, user DN lookup and target. Target should be /proxyui/forms/authenticationselector.jsp

# Preparation

2. Create JSP based form login page (optional)
  - Create JSP based form login in CA Access gateway

The screenshot shows the 'General' configuration page for an authentication scheme. The 'Name' field is 'JSP\_FORM\_LOGIN'. The 'Scheme Common Setup' section shows 'Authentication Scheme Type' set to 'HTML Form Template' and 'Protection Level' set to '5'. The 'Scheme Setup' section shows 'Web Server Name' as 'smsserver.forwardinc.ca', 'Port' as '9090', and 'Target' as '/proxyui/forms/SSOlogin.jsp'. The 'Target' field is highlighted with a red rectangle. There are also checkboxes for 'Use Relative Target', 'Use SSL Connection', 'Allow this scheme to save credentials', and 'Support non-browser clients'. An 'Additional Attribute List' field is at the bottom.

HTML Form Login

Access Gateway Server, port  
Target  
/proxyui/forms/SSOlogin.jsp

# Preparation

## 3A. Create realms and rule for login

- Make authentication pages as unprotected

• = Required

General	
• Name	Login_JSP
Domain	DOMAIN-SPSADMINUI-spsagent

Resource	
• Agent	spsagent
Resource Filter	/proxyui/forms/
Effective Resource	spsagent/proxyui/forms/
Default Resource Protection	<input type="radio"/> Protected <input checked="" type="radio"/> Unprotected
Authentication Scheme	Basic

Rules	
-------	--

Access Gateway way agent name

Resource filter /proxyui/forms/

Check "unprotected option"

# Preparation

## 3B. Create realms and rule for login

- Make protected realm and rule for redirect.jsp

**General**

• Name: Protect\_Redirect Description: [empty]

Domain: DOMAIN-SPSADMINUI-spsagent

**Resource**

• Agent: spsagent Lookup Ag

Resource Filter: /proxyui/forms/redirect

Effective Resource: spsagent/proxyui/forms/redirect

Default Resource Protection: Protected

Authentication Scheme: JSP\_FORM\_LOGIN

Access Gateway way agent name

Protect with any form login

Resource filter /proxyui/forms/redirect

**Attributes**

• Name: redirect\_rule Description: Protect\_Redirect

Domain: DOMAIN-SPSADMINUI-spsagent

**Resource \***

Resource: [empty]

Effective Resource: spsagent/proxyui/forms/redirect\*

Regular Expression: ☒

**Allow/Deny and Enable/Disable**

☒ Allow Access

☐ Deny Access

Enabled: ☒

**Action**

☒ Web Agent actions

☐ Authentication events

☐ Authorization events

☐ Impersonation events

• Action: Get, Head, LOCK, MOVE

Action: GET, POST



# Test Procedure

1. Change authselector.jsp setting depending on customer's environment
2. Protect Web site with newly created IWA\_FAILOVER\_FORM login page
3. Login from windows domain and a user can login the site without any authentication scheme
4. Login from non windows domain and a user can login the site with form authentication
5. Test it from Chrome and Fireforx

## Authselector.jsp

```
// Please change following variables based on your environment

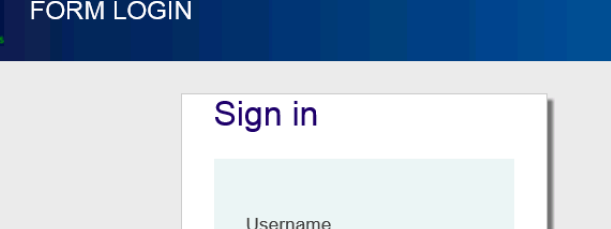
String ntlmSsoLoginUrl = "https://infra00.forwardinc.ca:8443/siteminderagent/ntlm/creds.ntc"; // IWA login page
String ntlmDomain = "FORWARDINC" ; // Windows Domain Name
String formProtectURL = "http://smsserver.forwardinc.ca:9090/proxyui/forms/redirect.jsp" ; // Protected by CA SSO Form Login
```

IWA login web site

Windows Domain Name

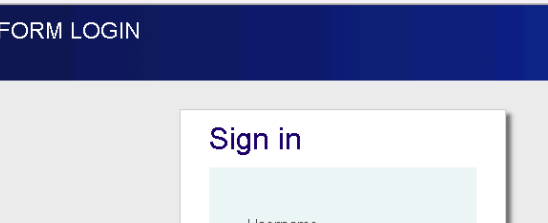
Temporary redirect page when a user does not login to windows domain.

## Test result (Before windows domain)



The screenshot displays the 'Client Portal Web Page' for CA Technologies. The page features a dark blue header with the CA Technologies logo on the left and the text 'FORM LOGIN' in white. A navigation bar at the top contains links for 'Demo Login Page', 'Client Portal Web Page', 'CASSO', 'IdentityManagement', 'AdvancedAuthentication', and 'Email Che...'. The main content area is a light gray rectangle containing a white box with a light blue background. Inside this box, the text 'Sign in' is displayed in a large, dark blue font. Below this, there are two input fields: 'Username' and 'Password', each with a white input box. A blue button with the text 'Sign in' in white is positioned below the input fields.

IE



CA Access Gateway - Form x

➤ [smsserver.forwardinc.ca:9090/proxyui/forms/SSOlogin.jsp?TYPE=33554433&REALMOID=06-379881a3-5](https://smsserver.forwardinc.ca:9090/proxyui/forms/SSOlogin.jsp?TYPE=33554433&REALMOID=06-379881a3-5)

**a**  
images

## FORM LOGIN

### Sign in

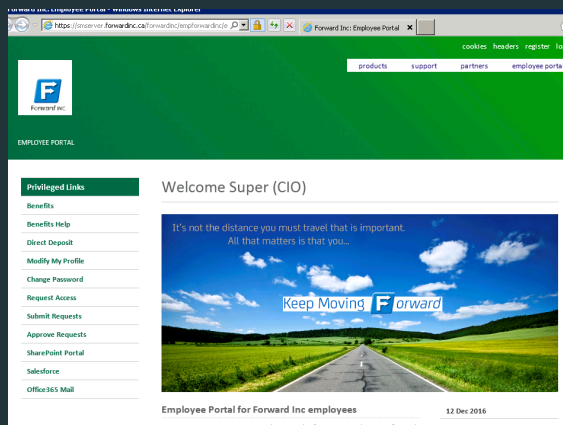
Username

Password

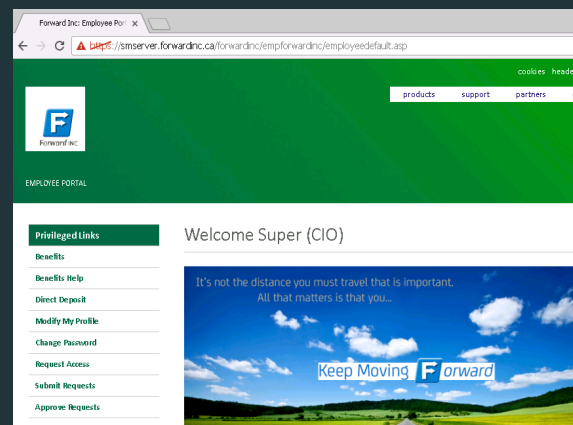
Sign in

## Chrome

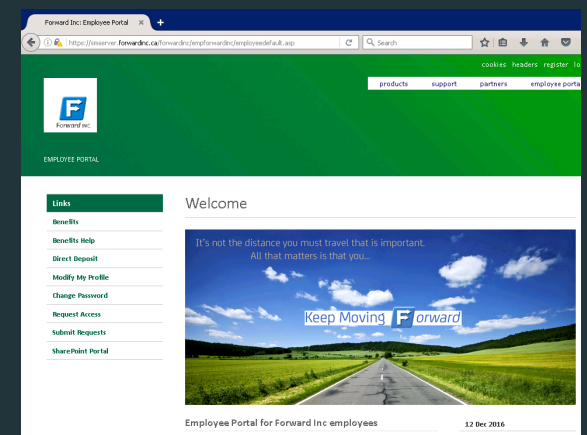
# Test result (after windows domain login)



IE



Chrome



Firefox