

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)

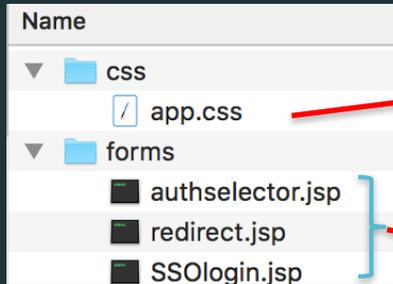
Prerequisites

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

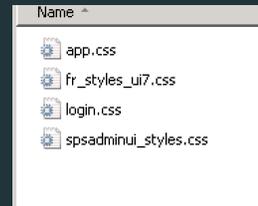
Preparation

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

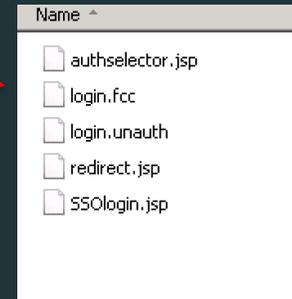
<Access Gateway Install folder>\secure-proxy\Tomcat\webapps\proxyui\



"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 configuration interface for an authentication scheme. The 'General' section has the name 'JSP_FORM_LOGIN'. The 'Scheme Common Setup' section has the 'Authentication Scheme Type' set to 'HTML Form Template' and 'Protection Level' set to '5'. The 'Scheme Setup' section has '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 box. 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 Description

Domain

Resource

• Agent

Resource Filter

Effective Resource

Default Resource Protection Protected Unprotected

Authentication Scheme

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
- Domain: DOMAIN-SPSADMINUI-spsagent

Resource

- Agent: spsagent
- 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

Realm and Resource

- Name: redirect_rule
- Domain: DOMAIN-SPSADMINUI-spsagent
- Resource: *
- 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

Resource *

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

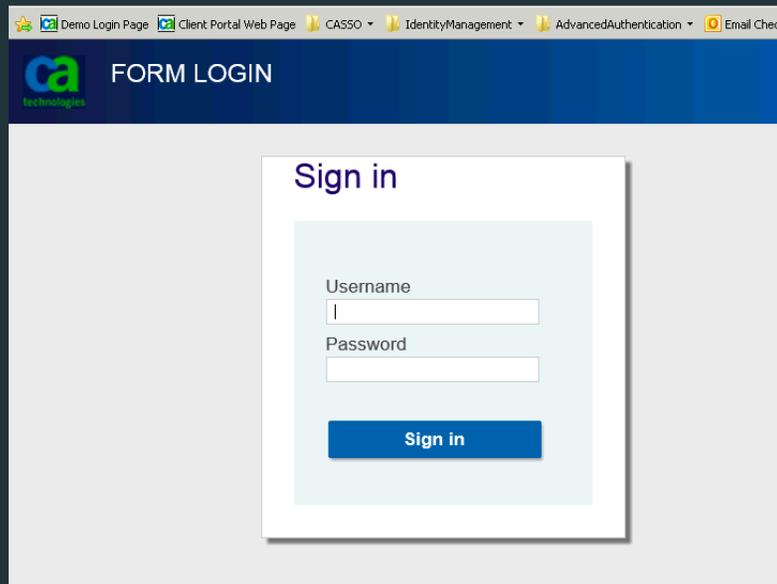
String ntlmSsoLoginUrl = "https://infra00.forwardinc.ca:8443/siteminderagent/ntlm/creds.ntc"; // IWA login page
String ntlmDomain = "FORWARDINC" ; // Windows Domain Name
String formProtectURL = "http://smsserver.forwardinc.ca:9090/proxyui/forms/redirect.jsp" ; // Protected by CA SSO Form Login
```

IWA login web site

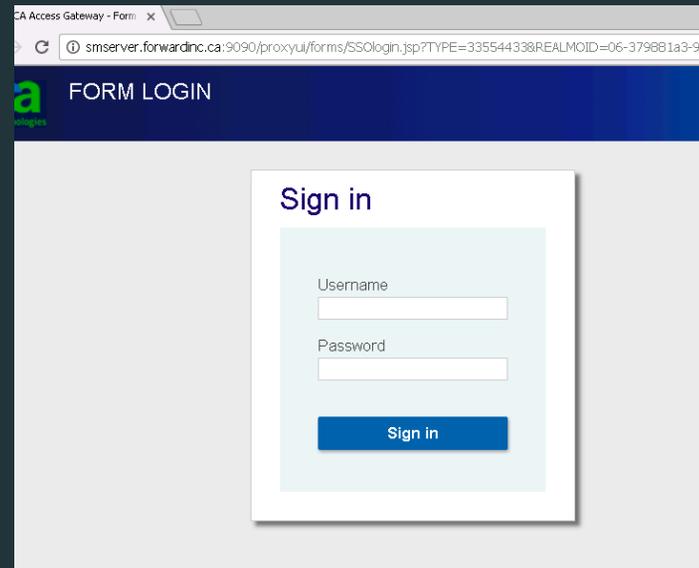
Windows Domain Name

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

Test result (Before windows domain)

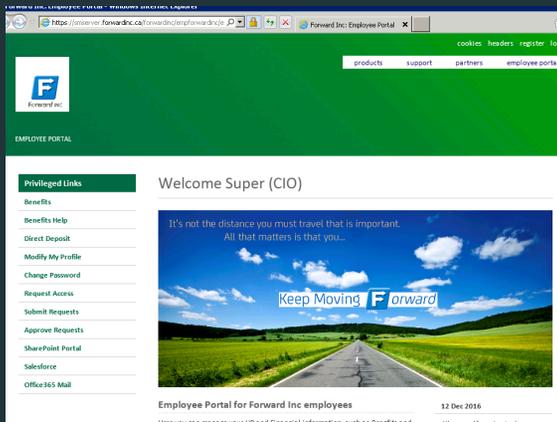


IE

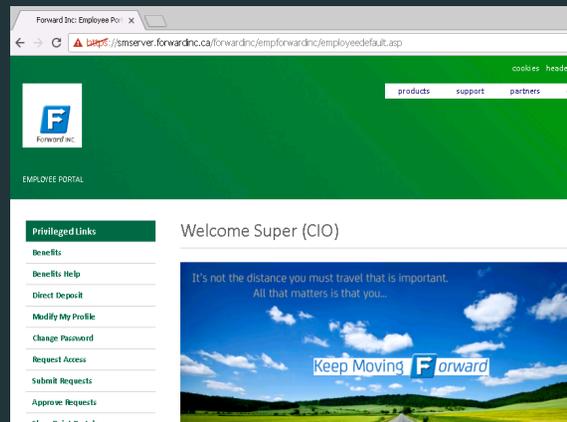


Chrome

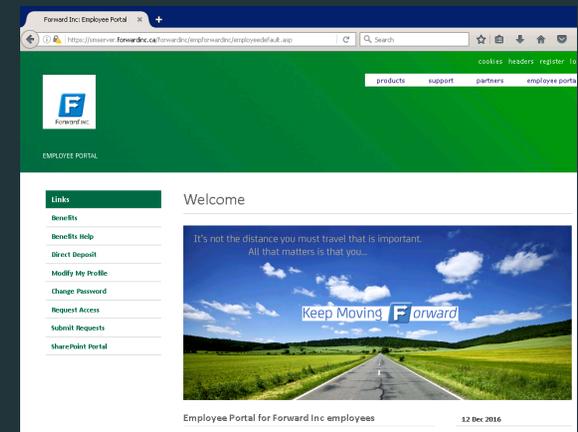
Test result (after windows domain login)



IE



Chrome



Firefox