2. – Integration without programming

- 2.1 – Microsoft RD Web Access portal
- 2.2 – Active Directory and LDAP
- 2.3 – Radius
- 2.4 – OAuth2
- 2.5 – SAML
- 2.6 – Single Sign-On (SSO) with HTTP basic authentication

2.1 – Microsoft RD Web Access portal

Assume your web portal address is: https://MyRDPortal/RdWeb. You need to set up the following two entries in gateway.conf:

```
webfeed = https://MyRDPortal/RDWeb/feed/webfeed.aspx
directoryIndex = login.html
```

Checklist:

- Verify the web feed URL with your browser. You'll see a cookie or XML displayed.
- Clean the browser cache if your gateway start page is not changed to login.html
- Make sure NTLM authentication on IIE is enabled:
  https://technet.microsoft.com/enus/library/cc754628(v=ws.10).aspx
- Make sure RDWeb/Pages and RDWeb/Feed on IIS is using "Windows authentication" authentication mode instead of "Forms Authentication".

2.2 – Active Directory and LDAP

If all your users are domain users, please create a plain text file (encoding: UTF-8 without Byte Order Mark) with following context:

```
{
  "source":{
    "type": "AD",
    "properties": {
      "server": "ADServerAddress"
    }
  }
}
```

Save it as users.json or other name and specify the location of this file in gateway.conf:

```
user = C:\\workspace\\data\\users.json
```

You can configure servers used by all the users in servers.json and specify the location of servers.json in gateway.conf:

```
server = C:\\workspace\\data\\servers.json
```

If you are using a LDAP server, please change the type to “LDAP”. You can also configure AD/LDAP users in users.json:

```
{
"users": [
  {
    "name": "user1",
    "password": "user1",
    "servers": [
      "RdpServer1",
      "TEST",
      "Excel 2010"
    ],
    "isDomainUser": true,
    "transferCredential": true,
    domainServer: "serverAddr"
```

```
    }
}
```

2.3 – Radius

```
{
  "source": {
    "type": "RADIUS",
    "properties": {
      "server": "192.168.12.128",
      "port": "1812",
      "accountingPort": "1813",
      "sharedSecret": "test123"
      "timeout": "60000",
      "retryCount": "3"
    }
  }
}
```

- Make sure the IP of Spark Gateway is listed as a client on RADIUS server.
- Make sure the timeout is at least 60000 milliseconds if your RADIUS server is using multi factor authentication, like Azure MFA.

2.4 – OAuth2

First, save your OAuth2 provider configuration into a JSON file, for example:

```
{
  "providers" : [{
    "name" : "Google",
    "client_id" : "650561938988-t2r66k1ms3hpoi3k1e2g7l2adlarau8s.apps.googleusercontent.com",
    "client_secret" : "-D-nhxWn2E97tZWWLg5IQ6Ak",
    "request_uri" : "https://accounts.google.com/o/oauth2/auth",
    "redirect_uri" : "http://localhost/oauth2callback",
    "access_token_uri": "https://oauth2.googleapis.com/token",
    "auth_uri": "/login_chrome.html",
    "scope": "openid email"
  },
  {
    "name" : "Live",
    "client_id" : "0000000040133A31",
    "client_secret" : "p9WwBr2Pyrq6mtaeZCwTSwqbIF39Br3Z",
    "request_uri" : "https://login.live.com/oauth20_authorize.srf",
    "redirect_uri" : "http://www.remotespark2.com/oauth2callback",
    "access_token_uri": "https://login.live.com/oauth20_token.srf",
    "scope": "wl.emails",
    "profile_uri": "https://apis.live.net/v5.0/me"
  }]
}
```

Second, specify the position of this file in gateway.conf:

```
oauth2 = \\user\\local\bin\\SparkViewGateway\\oauth2.json
```

For more information, please check the source code of login.html.

2.5 – SAML

You can get the integration of SAML from this document.

2.6 – Single Sign-On (SSO) with HTTP basic authentication

You can enable HTTP Basic Authentication on SparkView by setting `authorization=Basic` in gateway.conf, so all the RDP connections will use credentials from the HTTP Authorization header.

This can be used for VPN SSO integration etc