buypass™
securing transactions

BUYPASS CODE – OFFICE365
Using ADFS 2.0 proxy

Buypass OPEN

Version: 0.1
Document date: 03.03.2014

History of change

Version	Date	Status	Description/Change
0.1	03.03.2014	Draft	First draft
1.0	26.06.2014	First version	

Contributors

Company name	Name
Buypass AS	Oskar Otterskog

Table of content

1   Overview

This guide describes how you can integrate Buypass Code in Microsoft ADFS 2.0 to activate 2-factor authentication for Office365 and other applications. Buypass offers a small integration packet that runs in an ADFS 2.0 proxy to require a Buypass Code OTP for users signing in from outside the corporate network.

1.1   Technical requirements

1.1.1   Software requirements
- Windows 2008 (R2) / Windows 2012 (R2)
- .NET 4.5
- An installed and configured Buypass Code Service Connector (See Service_Connector_7.25.0.25_installationGuide_EN_25022014.pdf)
- Office365 has been setup for SSO to an on-premise ADFS 2.0 server with an ADFS 2.0 proxy and has working SSO based on user's existing AD password

1.1.2   Network connectivity
- The ADFS 2.0 integration packet needs to communicate with the Service Connector via Radius (default port 1812)

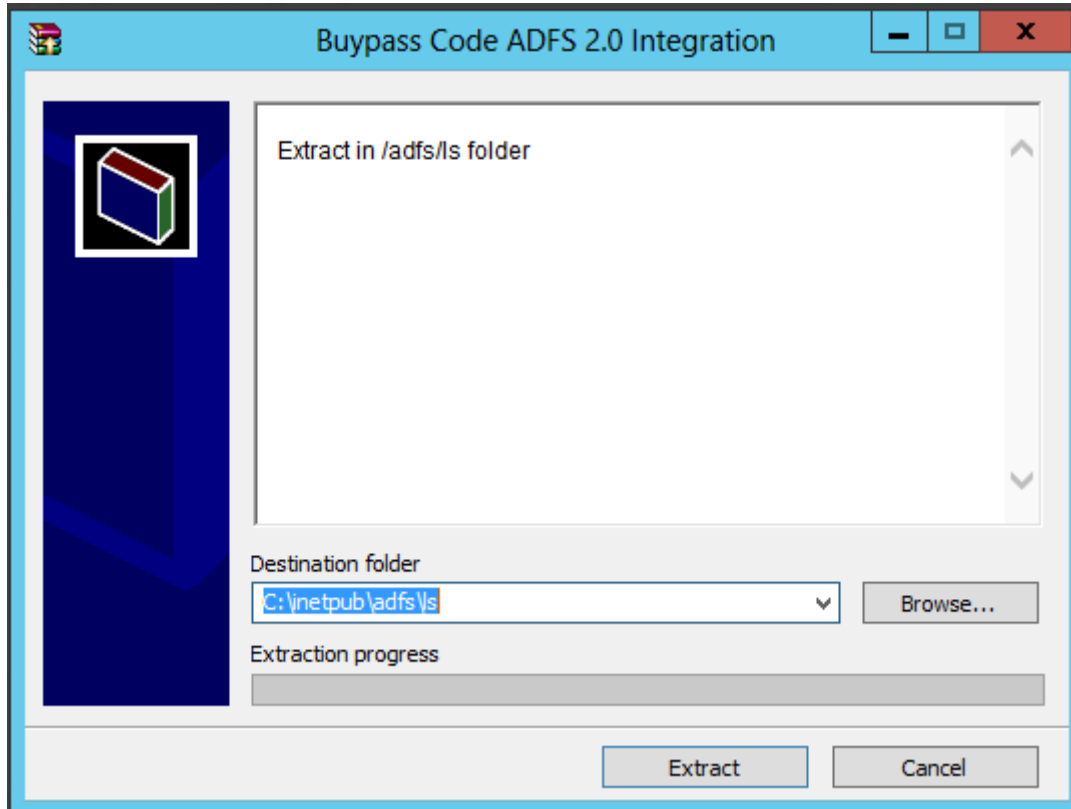# 2   Integration setup

2.1   Buypass Code Manager configuration
Login to Buypass Code manager and create a new radius configuration. The IP-address should be the IP of the ADFS 2.0 proxy.

For more information about Radius configuration, see
BP Code Manager7.25.0.25_AdminGuide_EN.pdf.

2.2 Installation and configuration of Buypass Code ADFS 2.0 integration

1. Download Buypass_Code_ADFS_2_0_Integration.exe from Buypass Ekstranett.

2. Run Buypass_Code_ADFS_2_0_Integration.exe on the ADFS 2.0 proxy server and extract the files into the \adfs\ls folder of the IIS.

3. Open \adfs\ls\web.config and locate

```
<localAuthenticationTypes>
    <add name="TlsClient" page="auth/sslclient/" />
    <add name="Basic" page="auth/basic/" />
    <add name="Forms" page="FormsSignIn.aspx" />
</localAuthenticationTypes>
```
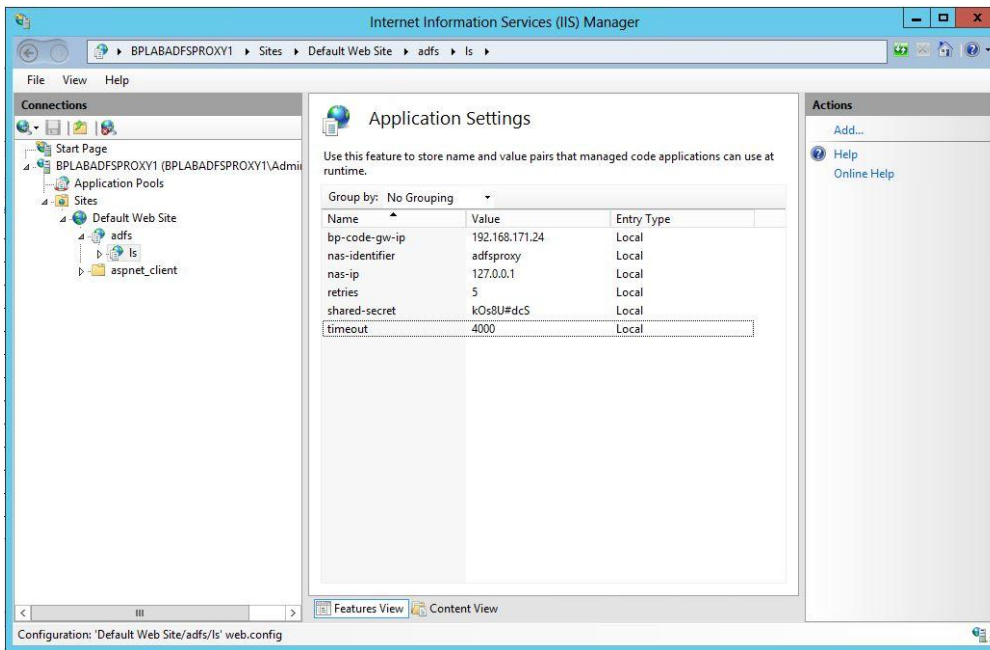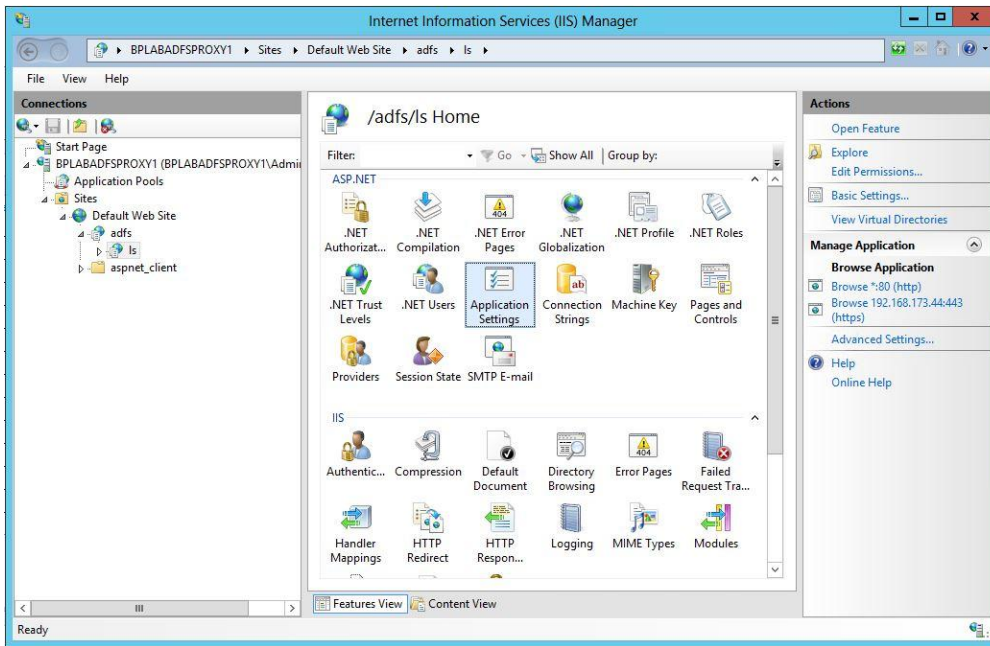
Note that the order and the number of items may differ.

4. Put <add name="Forms" page="FormsSignIn.aspx" /> at the top and change FormsSignIn.aspx to BpCodeFormsSignIn.aspx. It should now look something like

```
<localAuthenticationTypes>
    <add name="Forms" page="BpCodeFormsSignIn.aspx" />
    <add name="TlsClient" page="auth/sslclient/" />
    <add name="Basic" page="auth/basic/" />
</localAuthenticationTypes>
```

5. In IIS Manager, select /adfs/ls Home and double click "Application Settings".

6. Enter settings according to the table below

Name	Example Value	Required/Opt ional	Description
primary-bp-code-gw-ip	192.168.50.3	Required	IP-Address to primary Buypass Code Service Connector
shared-secret	Verysecretkey	Required	The pre shared secret that is configured in Buypass Code Manager
secondary-bp-code-gw-ip	192.168.50.4	Optional	IP-Address to secondary Buypass Code Service Connector. Used for redundancy.

nas-ip	192.168.50.1	Optional	RADIUS attribute used to differentiate between several Radius clients that have the same IP. Has to be declared in Buypass Code Manager as well.
nas-identifier	MyIdentifier	Optional	RADIUS attribute used to differentiate between several Radius clients that have the same IP. Has to be declared in Buypass Code Manager as well.
retries	5	Optional	The number of times to try communicating with Buypass Code Service Connector if no response. Default: 3
timeout	5000	Optional	The socket timeout in ms. Default: 3000
port	1812	Optional	The port to use for sending UDP packets to the Buypass Code Service Connector. Default: 1812
normalize-username	true	Optional	Normalizes the username that is used to authenticate to Buypass Code. This makes "EXAMPLE\username", "username@examle.com" and "username" to be treated as only "username". Default: false

7. If the ADFS proxy and the Buypass Code Service Connector run on different servers, make sure that firewalls accepts traffic on the specified ports.

8. Restart IIS from IIS Manager.

9. The ADFS 2.0 login screen should now look like the figure below.