

# BUYPASS CODE – OFFICE365

Using ADFS 2.0 proxy

**Byypass OPEN**

Version: 0.1  
Document date: 03.03.2014

**Byypass AS**

Nydalsveien 30A, PO Box 4364 Nydalen  
N-0402 Oslo, Norway

Tel.: +47 23 14 59 00  
Fax: +47 23 14 59 01

E-mail: [kundeservice@buypass.no](mailto:kundeservice@buypass.no)  
VAT: NO 983 163 327

[www.buypass.no](http://www.buypass.no)

## 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 .....4**
- 1.1 Technical requirements.....4
- 1.1.1 Software requirements..... 4
- 1.1.2 Network connectivity..... 4
- 2 Integration setup .....4**
- 2.1 Bypass Code Manager configuration.....4
- 2.2 Install and configure Bypass Code ADFS 2.0 integration .....5

# 1 Overview

This guide describes how you can integrate Bypass Code in Microsoft ADFS 2.0 to activate 2-factor authentication for Office365 and other applications. Bypass offers a small integration packet that runs in an ADFS 2.0 proxy to require a Bypass 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 Bypass 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 Bypass Code Manager configuration

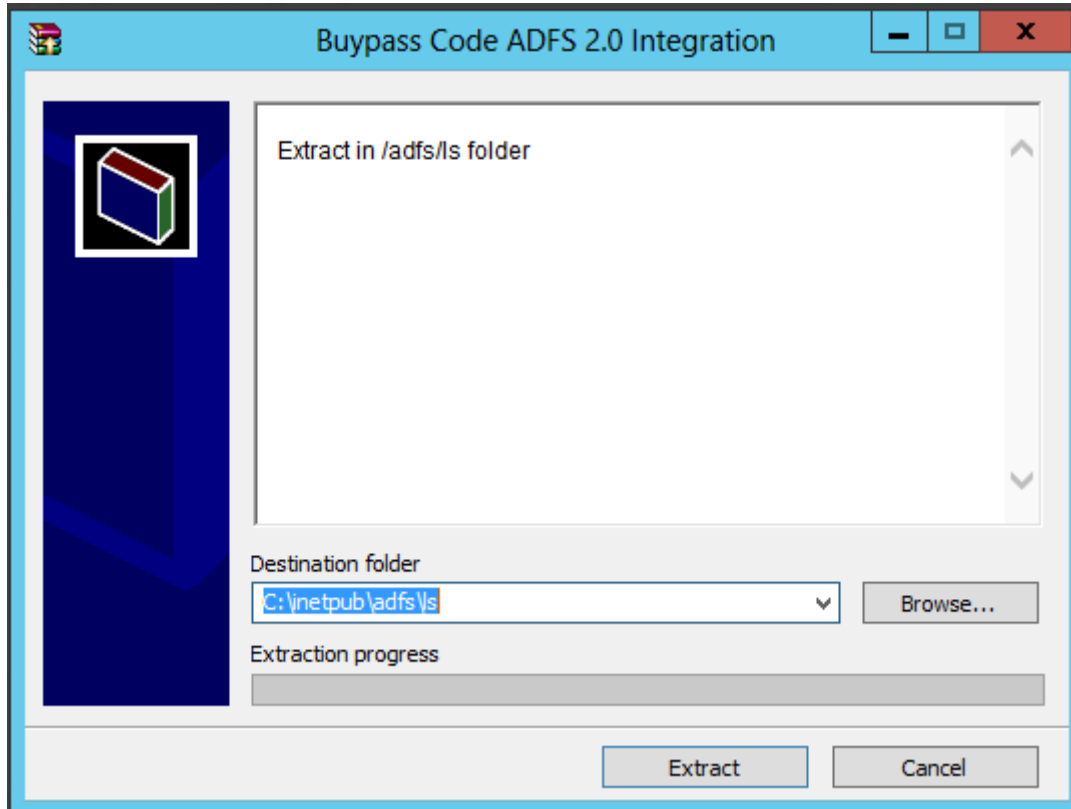
Login to Bypass Code manager and create a new radius configuration. The IP-address should be the IP of the ADFS 2.0 proxy.

The screenshot shows the 'Radius konfigurasjon' page in the Bypass Code Manager. The sidebar on the left contains navigation links: **Hjem**, **Logger**, **Administrasjon**, **Konfigurasjon** (with sub-links for LDAP, Radius, Ekstern Radius, and Brukersted), **Pålogget: oott2**, **Rolle: Superbruker**, **For brukersted: Test Redundans**, and a **[Logg ut]** link. The main content area has the following fields:  
- **IP-adresse:** 192.168.173.44  
- **Shared secret:** [masked with dots]  
- **Beskrivelse:** adfsproxy i lab  
- **Tilgjengelige LDAPs:** ldap://192.168.171.32, ldap://10.0.0.1  
- **Valgt LDAPs:** ldap://192.168.171.15  
Navigation buttons between the LDAP lists include '<', '>', '<<', and '>>'. At the bottom, there are **Tilbake** and **Lagre** buttons, and a note: '\* betyr at feltet må være utfyllt.'

For more information about Radius configuration, see [BP Code Manager7.25.0.25\\_AdminGuide\\_EN.pdf](#).

## 2.2 Installation and configuration of Bypass Code ADFS 2.0 integration

1. Download Bypass\_Code\_ADFS\_2\_0\_Integration.exe from Bypass Ekstranett.
2. Run Bypass\_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

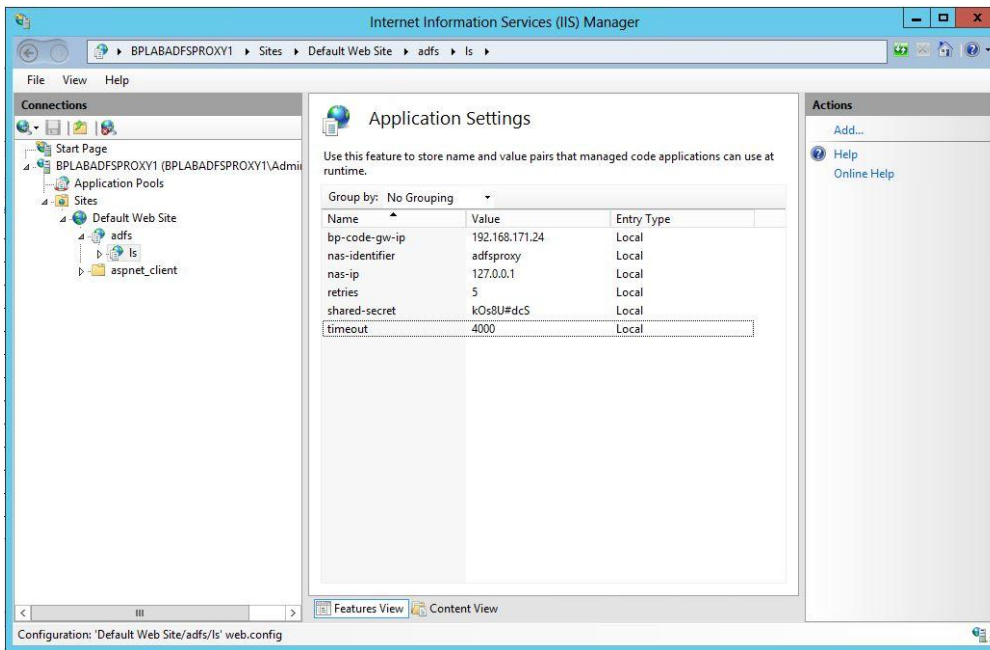
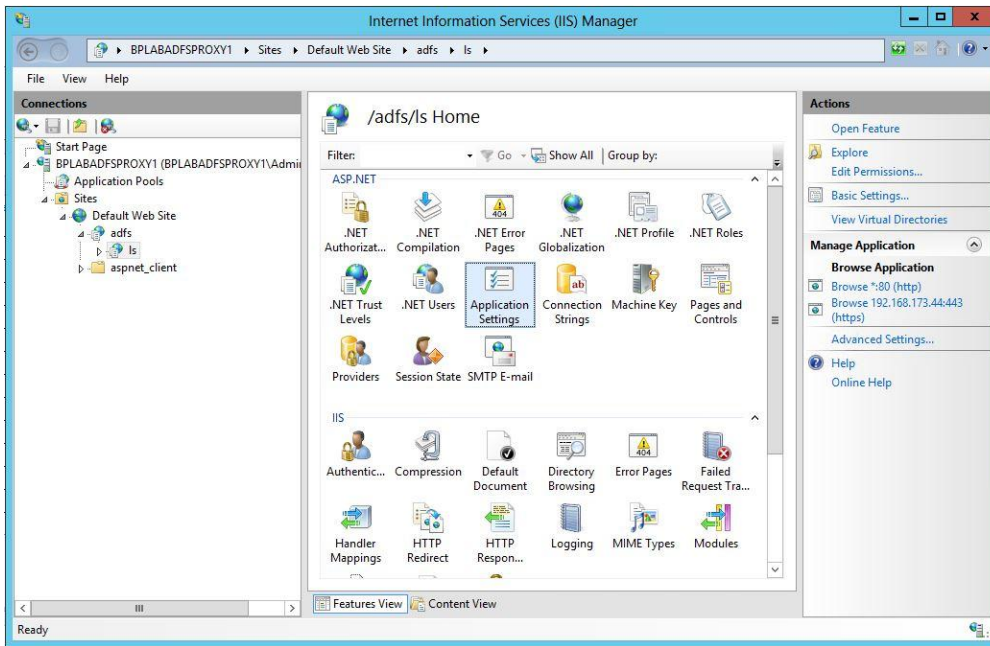
```
<localAuthenticationTypes>
  <add name="TlsClient" page="auth/sslclient/" />
  <add name="Basic" page="auth/basic/" />
  <add name="Forms" page="FormsSignIn.aspx" />
</localAuthenticationTypes>
```

**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/Optional	Description
primary-bp-code-gw-ip	192.168.50.3	Required	IP-Address to primary Bypass Code Service Connector
shared-secret	Verysecretkey	Required	The pre shared secret that is configured in Bypass Code Manager
secondary-bp-code-gw-ip	192.168.50.4	Optional	IP-Address to secondary Bypass 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 Bypass 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 Bypass Code Manager as well.
retries	5	Optional	The number of times to try communicating with Bypass 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 Bypass Code Service Connector. Default: 1812
normalize-username	true	Optional	Normalizes the username that is used to authenticate to Bypass Code. This makes "EXAMPLE\username", "username@example.com" and "username" to be treated as only "username". Default: false

- If the ADFS proxy and the Bypass Code Service Connector run on different servers, make sure that firewalls accepts traffic on the specified ports.
- Restart IIS from IIS Manager.
- The ADFS 2.0 login screen should now look like the figure below.

