



BCNET[→]2019

Welcome to BCNET 2019

Keynote Presentation



Implementing Office 365 and MS Exchange 2013 user access with BIGIP Access Policy Manager

Necessity to configure F5 BIG-IP APM to handle MS Office365 user authentication came from a requirement to migrate MS Office 365 US tenant user email accounts into on premises MS Exchange Server and make this migration as transparent to the users as possible.

Implementing Office 365 and MS Exchange 2013 user access with BIGIP Access Policy Manager

F5 Deployment Guide



Configuring the BIG-IP APM as a SAML 2.0 Identity Provider for Microsoft Office 365

Welcome to the F5® deployment guide for configuring the BIG-IP® Access Policy Manager (APM) to act as a SAML Identity Provider for Microsoft® Office 365. This document contains guidance on configuring the BIG-IP® APM as an IdP for Office 365 to perform Single Sign-On between the local Active Directory user accounts and Office 365-based resources such as Microsoft Outlook Web App and Microsoft SharePoint®.

Using this guide, you can configure the BIG-IP system version 11.3 and later using an iApp application template. There is also an appendix with manual configuration tables for users who prefer to create each individual object.

Products and applicable versions

Product	Version
BIG-IP APM	11.3 - 13.0
iApp Template Version	f5.microsoft_office_365_idp.v1.1.1rc1
Deployment Guide version	2.1 (see <i>Document Revision History</i> on page 19)

Implementing Office 365 and MS Exchange 2013 user access with BIGIP Access Policy Manager

Deployment Guide



Deploying the BIG-IP System v11 with Microsoft Exchange 2010 and 2013 Client Access Servers

Welcome to the F5 and Microsoft® Exchange® 2010 and 2013 Client Access Server deployment guide. Use this document for guidance on configuring the BIG-IP system version 11 and later to provide additional security, performance and availability for Exchange Server 2010 and Exchange Server 2013 Client Access Servers.

When configured according to the instructions in this guide, whether using an iApp template or manually, the BIG-IP system will perform as a reverse proxy for Exchange CAS servers, and will also perform functions such as load balancing, compression, encryption, caching, and pre-authentication.

Implementing Office 365 and MS Exchange 2013 user access with BIGIP Access Policy Manager

f5.microsoft_office_365_idp.v1.1.0 template was used to deploy O365 iApp. After O365 iApp was deployed it was modified to include MS Exchange 2013 authentication configuration.

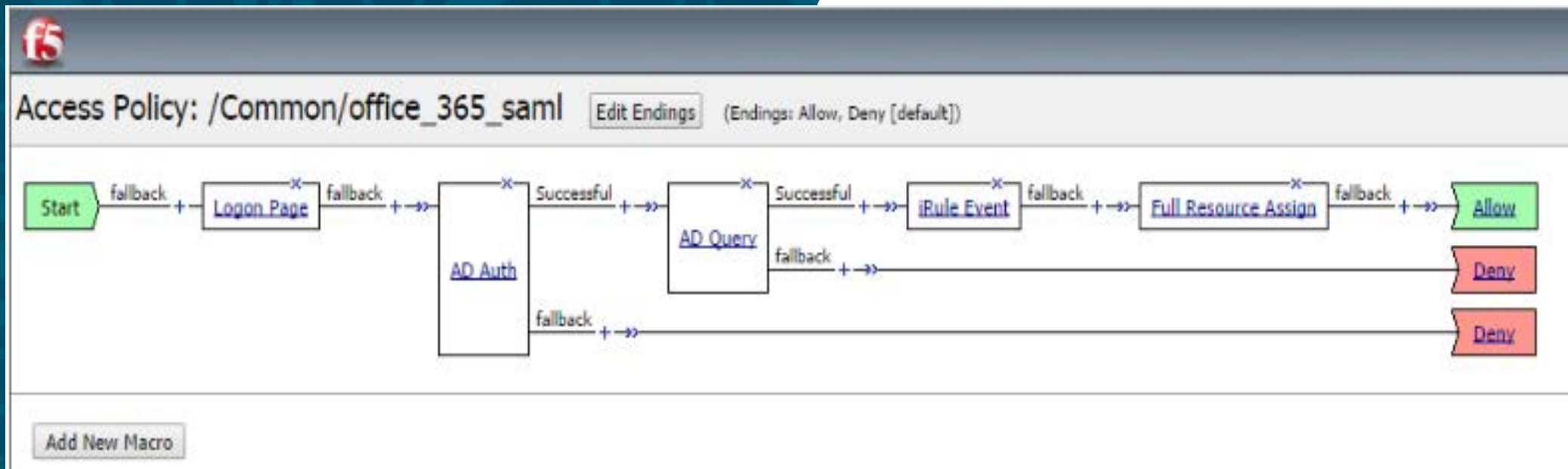
O365 iApp f5.microsoft_office_365_idp.v1.1.0 template deployment consists of a questionnaire. See the questionnaire with answers provided below.

How is your EntityID formatted?	My EntityID is a URL
What EntityID do you want to use for your Office 365 IdP?	https://o365.capilanou.ca/idp
Should the iApp create a new AAA server or use an existing one?	Create a new AAA Server
Which Active Directory server IP address in your domain can this BIG-IP system contact?	dc1.prd.capilanou.ca 204.239.151.111 dc2.prd.capilanou.ca 204.239.151.112 dc4.prd.capilanou.ca 204.239.151.113
What is the FQDN of the Active Directory implementation for your Office 365 users?	prd.capilanou.ca

Implementing Office 365 and MS Exchange 2013 user access with BIGIP Access Policy Manager

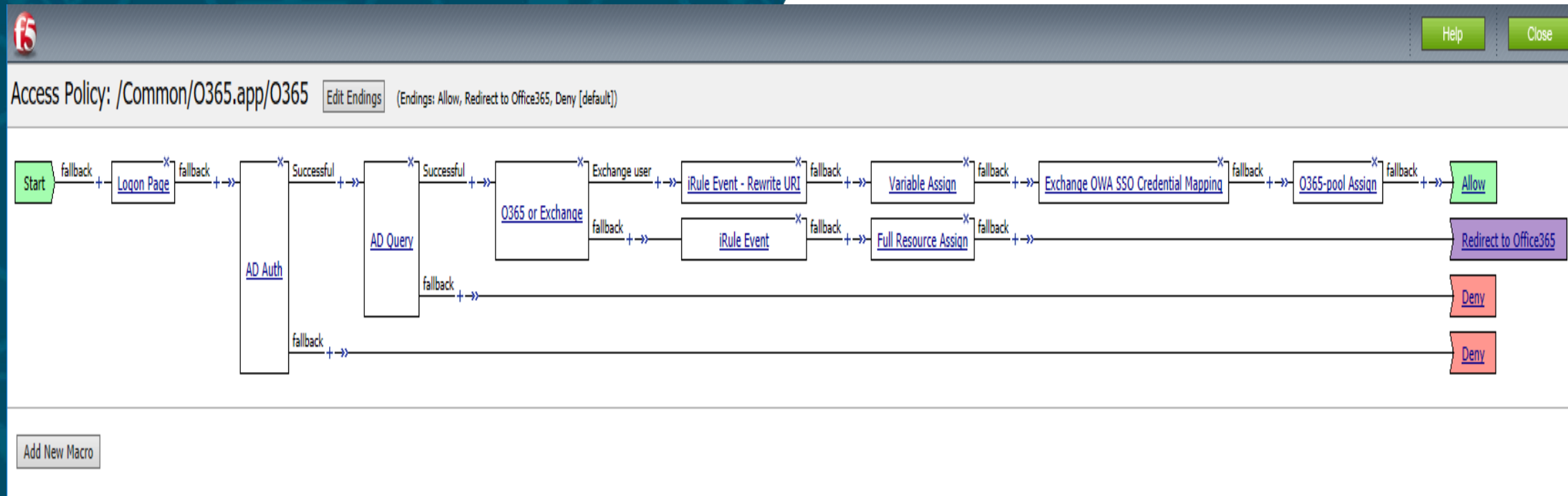
Does your Active Directory domain allow anonymous binding?	Require credentials for authentication
Which Active Directory user with administrative permissions do you want to use?	f5apm
What is the password associated with that account?	<provide_the_password>
How do you want to handle health monitoring for this pool?	Use a simple ICMP monitor for the Active Directory pool
What is the IP address clients will use to access the BIG-IP IdP Service?	192.168.10.59
What port do you want to use for the virtual server?	443
Which certificate do you want to use to encrypt your SAML Assertion?	SAMLOffice365prod.crt
What is the associated private key?	SAMLOffice365prod.key

Implementing Office 365 and MS Exchange 2013 user access with BIGIP Access Policy Manager



Implementing Office 365 and MS Exchange 2013 user access with BIGIP Access Policy Manager

After O365 iApplication was deployed O365 Access Profile is required to be modified to accommodate MS Exchange 2013 SSO part. When all modifications are made that should look like below.



Implementing Office 365 and MS Exchange 2013 user access with BIGIP Access Policy Manager

Logon Page

Properties

Branch Rules

Name:

Logon Page

Logon Page Agent

Split domain from full Username

Yes

CAPTCHA Configuration


None

	Type	Post Variable Name	Session Variable Name	Values	Read Only
1	text	username	username		No
2	password	password	password		No
3	none	field3	field3		No
4	none	field4	field4		No
5	none	field5	field5		No

Implementing Office 365 and MS Exchange 2013 user access with BIGIP Access Policy Manager

Logon Page

Customization

Language	en ▾	Reset all defaults
Form Header Text	<h1>myCapU Email Sign In</h1>	
Logon Page Input Field #1	Enter your CapU email address	
Logon Page Input Field #2	Password	
Logon Button	Sign in	
Front Image	 [Replace Image] [Revert to Default]	

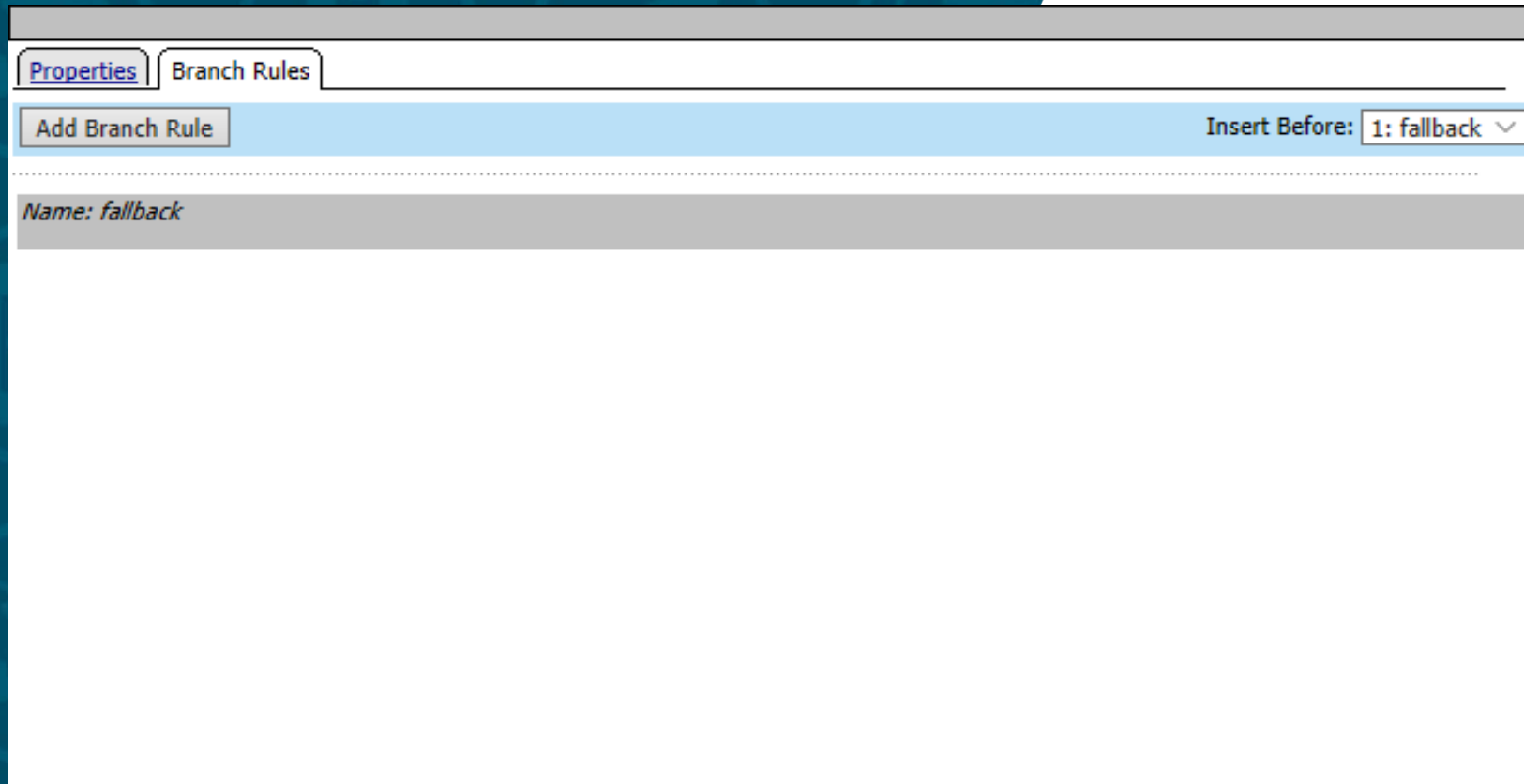
Implementing Office 365 and MS Exchange 2013 user access with BIGIP Access Policy Manager

Logon Page

Save Password Checkbox	Save Password
New Password Prompt	New Password
Verify Password Prompt	Verify Password
Password and Password Verification do not Match	Password and confirmation do not match.
Don't change password	Do not change password
Logon Page Original URL	Click here if already logged in

Implementing Office 365 and MS Exchange 2013 user access with BIGIP Access Policy Manager

Login Page



The screenshot shows the 'Branch Rules' configuration page in the BIGIP Access Policy Manager. At the top, there are two tabs: 'Properties' and 'Branch Rules', with 'Branch Rules' being the active tab. Below the tabs is a light blue header bar containing an 'Add Branch Rule' button on the left and an 'Insert Before:' dropdown menu on the right, which is currently set to '1: fallback'. Below this header, a grey bar displays the text 'Name: fallback'. The main area of the page is empty, suggesting a single rule is configured.

Implementing Office 365 and MS Exchange 2013 user access with BIGIP Access Policy Manager

AD Auth

Properties

Branch Rules

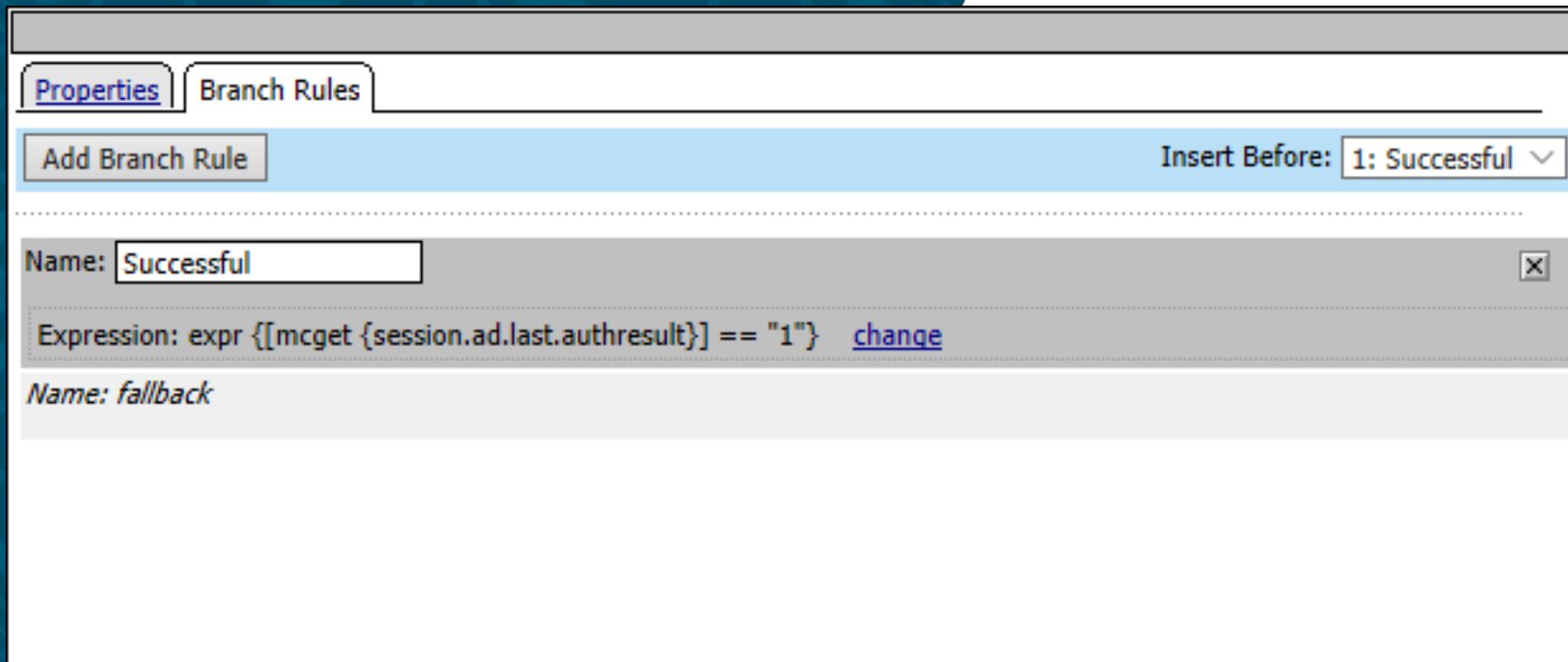
Name:

Active Directory

Type	Authentication ▾
Server	/Common/O365.app/O365_apm_aaa ▾
Cross Domain Support	Disabled ▾
Complexity check for Password Reset	Disabled ▾
Show Extended Error	Disabled ▾
Max Logon Attempts Allowed	3 ▾
Max Password Reset Attempts Allowed	3 ▾

Implementing Office 365 and MS Exchange 2013 user access with BIGIP Access Policy Manager

AD Auth



The screenshot shows the 'Branch Rules' tab in the BIGIP Access Policy Manager interface. At the top, there are two tabs: 'Properties' and 'Branch Rules'. Below the tabs is a button labeled 'Add Branch Rule'. To the right of this button is a dropdown menu labeled 'Insert Before:' with the value '1: Successful' selected. Below this is a section for a new rule. The 'Name:' field contains the text 'Successful'. Below the name field is a text area for the 'Expression:' containing the code 'expr {[mcget {session.ad.last.authresult}] == "1"}'. To the right of the expression is a blue link labeled 'change'. Below the expression field is a section labeled 'Name: fallback'.

Properties Branch Rules

Add Branch Rule Insert Before: 1: Successful

Name: Successful

Expression: `expr {[mcget {session.ad.last.authresult}] == "1"}` [change](#)

Name: fallback

Implementing Office 365 and MS Exchange 2013 user access with BIGIP Access Policy Manager

AD Query

Properties

Branch Rules

Name:

Active Directory

Type	<input type="text" value="Query"/>
Server	<input type="text" value="/Common/O365.app/O365_apm_aaa"/>
SearchFilter	<input type="text" value="samAccountName=%{session.logon.last.username}"/>
Fetch Primary Group	<input type="text" value="Disabled"/>
Cross Domain Support	<input type="text" value="Disabled"/>
Fetch Nested Groups	<input type="text" value="Disabled"/>
Complexity check for Password Reset	<input type="text" value="Disabled"/>
Max Password Reset Attempts Allowed	<input type="text" value="3"/>
Prompt user to change password before expiration	<input type="text" value="none"/> <input type="text" value="0"/>

Add new entry

Insert Before:

Required Attributes (optional)

Implementing Office 365 and MS Exchange 2013 user access with BIGIP Access Policy Manager

AD Query

Properties **Branch Rules**

Add Branch Rule Insert Before: 1: Successful ▾

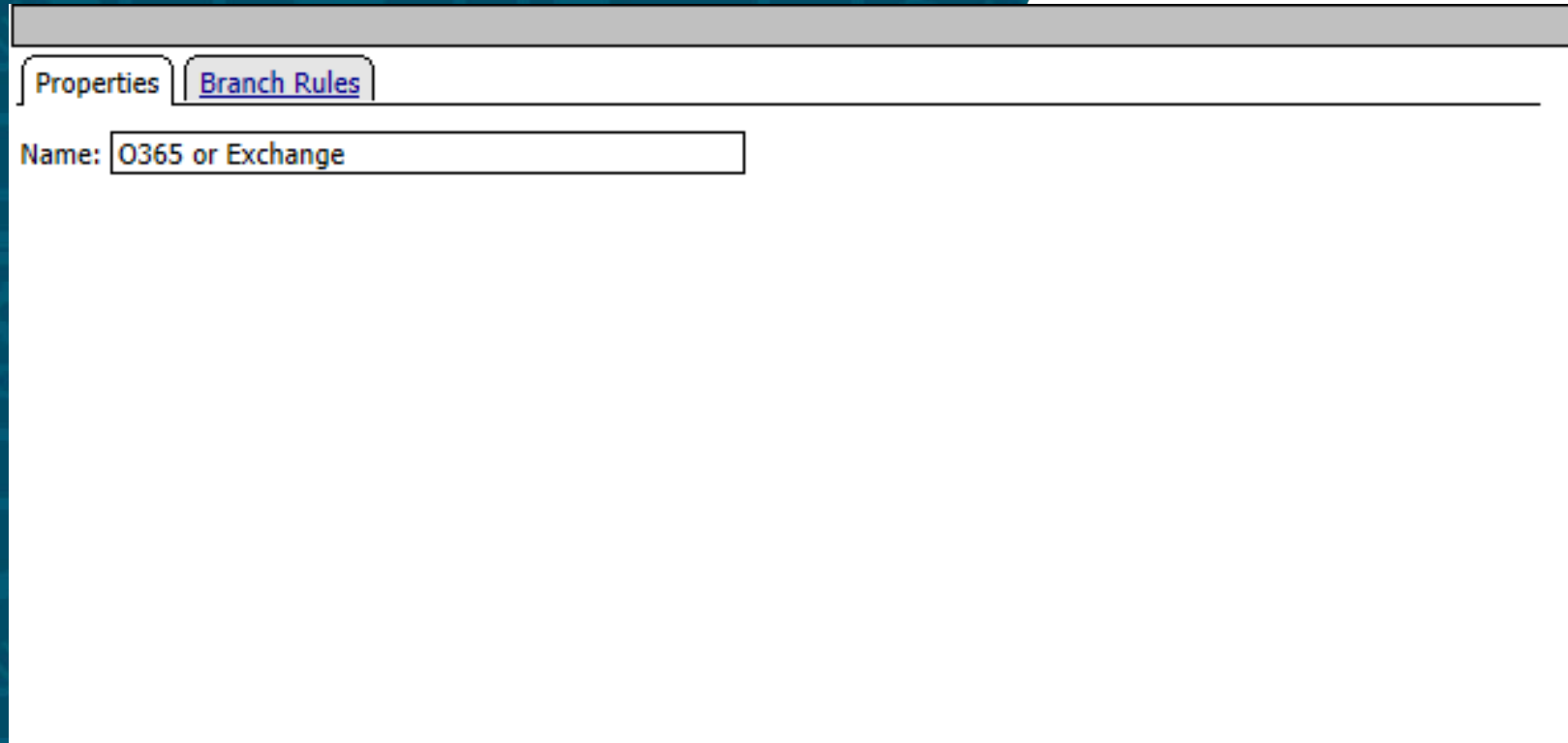
Name: ✕

Expression: Active Directory Query has Passed [change](#)

Name: *fallback*

Implementing Office 365 and MS Exchange 2013 user access with BIGIP Access Policy Manager

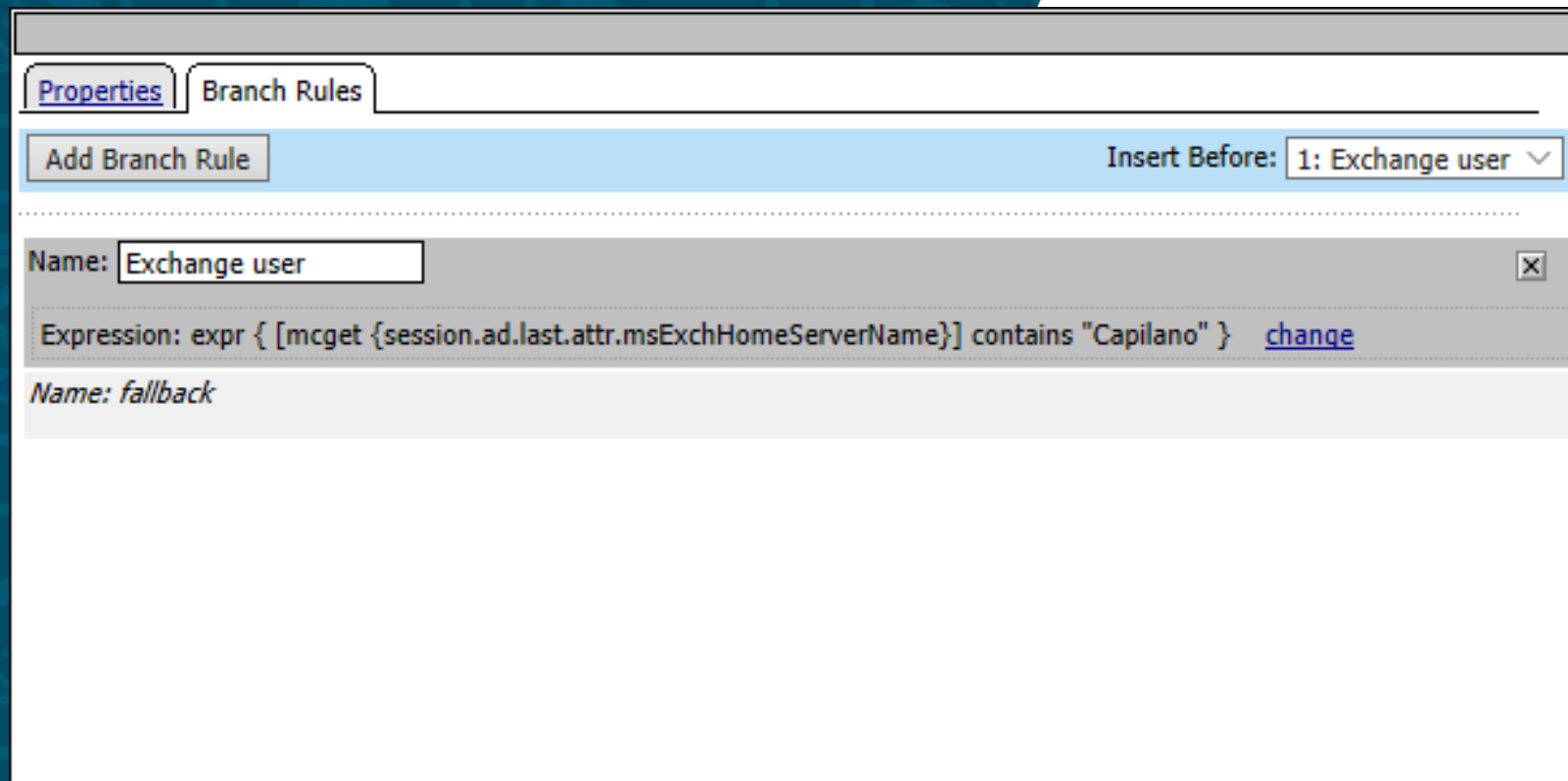
O365 or Exchange



The screenshot shows the BIGIP Access Policy Manager web interface. At the top, there are two tabs: 'Properties' and 'Branch Rules'. The 'Branch Rules' tab is selected. Below the tabs, there is a text input field labeled 'Name:' containing the text 'O365 or Exchange'. The rest of the interface is empty.

Implementing Office 365 and MS Exchange 2013 user access with BIGIP Access Policy Manager

O365 or Exchange



The screenshot shows the 'Branch Rules' tab in the BIGIP Access Policy Manager configuration interface. At the top, there are two tabs: 'Properties' and 'Branch Rules'. Below the tabs is a button labeled 'Add Branch Rule'. To the right of this button is a dropdown menu labeled 'Insert Before:' with the value '1: Exchange user' selected. Below this is a section for editing a rule. It has a 'Name:' field containing 'Exchange user' and a close button (X). Below the name field is an 'Expression:' field containing the text: `expr { [mcget {session.ad.last.attr.msExchHomeServerName}] contains "Capilano" }`. To the right of the expression is a blue link labeled 'change'. Below the expression field is a section labeled 'Name: fallback'.

Properties Branch Rules

Add Branch Rule Insert Before: 1: Exchange user

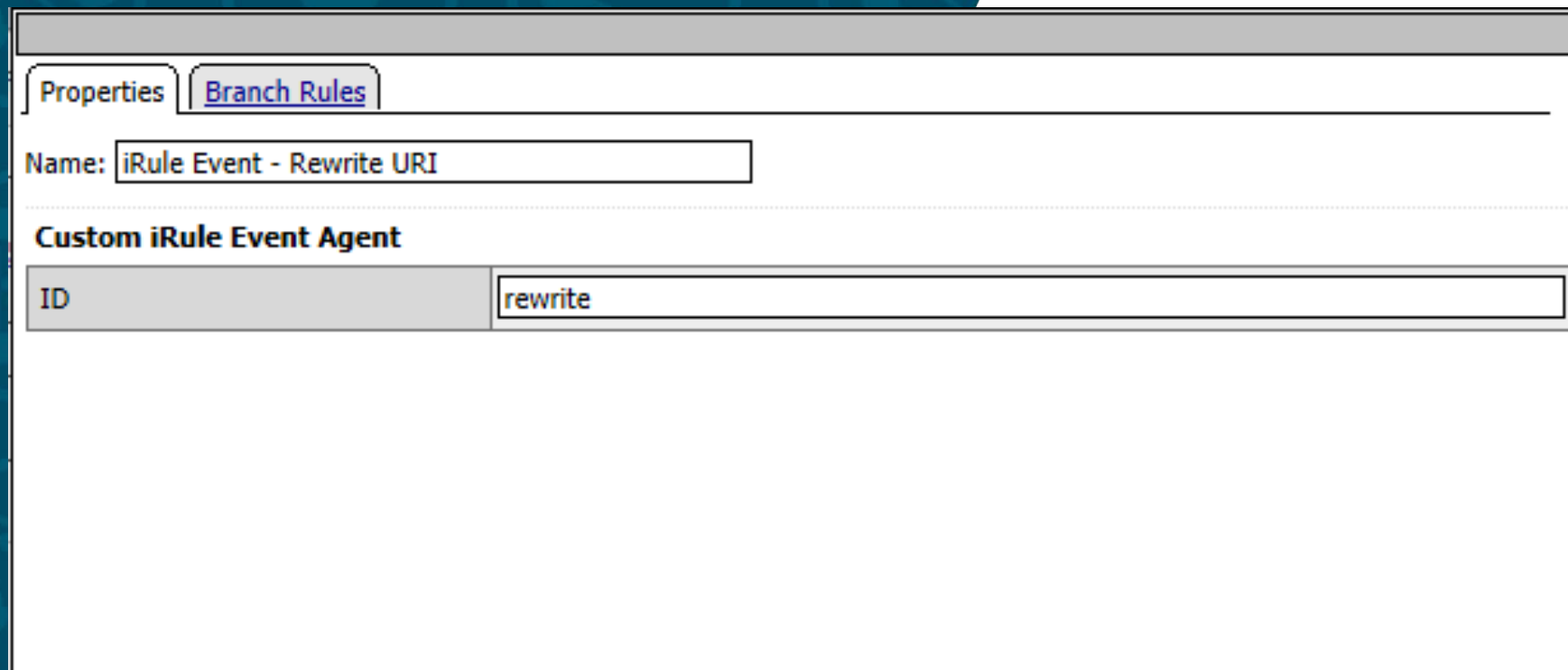
Name: Exchange user

Expression: `expr { [mcget {session.ad.last.attr.msExchHomeServerName}] contains "Capilano" }` [change](#)

Name: fallback

Implementing Office 365 and MS Exchange 2013 user access with BIGIP Access Policy Manager

iRule Event – Rewrite URI



The screenshot shows the configuration interface for an iRule Event in the BIGIP Access Policy Manager. The interface has a dark blue header with the title "iRule Event – Rewrite URI". Below the header, there are two tabs: "Properties" and "Branch Rules". The "Branch Rules" tab is selected. Under the "Branch Rules" tab, there is a text field labeled "Name:" with the value "iRule Event - Rewrite URI". Below this, there is a section titled "Custom iRule Event Agent". Under this section, there is a table with two columns: "ID" and "Value". The "ID" column has the value "rewrite" and the "Value" column is empty.

ID	Value
rewrite	

Implementing Office 365 and MS Exchange 2013 user access with BIGIP Access Policy Manager

iRule Event – Rewrite URI

The screenshot shows the configuration interface for an iRule in the BIGIP Access Policy Manager. At the top, there are two tabs: 'Properties' and 'Branch Rules'. The 'Branch Rules' tab is selected. Below the tabs, there is a light blue bar containing an 'Add Branch Rule' button on the left and an 'Insert Before:' dropdown menu on the right, which is currently set to '1: fallback'. Below this bar, a horizontal dotted line separates the header from the main content area. The main content area has a grey header bar with the text 'Name: fallback'. The rest of the area is white and currently empty.

Implementing Office 365 and MS Exchange 2013 user access with BIGIP Access Policy Manager

iRule Event

Properties	Branch Rules
Name: <input type="text" value="iRule Event"/>	
<hr/>	
Custom iRule Event Agent	
ID	<input type="text" value="encode"/>

Implementing Office 365 and MS Exchange 2013 user access with BIGIP Access Policy Manager

iRule Event

The screenshot shows the configuration interface for an iRule in the BIGIP Access Policy Manager. At the top, there are two tabs: 'Properties' and 'Branch Rules'. The 'Branch Rules' tab is currently selected. Below the tabs, there is a light blue bar containing an 'Add Branch Rule' button on the left and an 'Insert Before:' dropdown menu on the right, which is set to '1: fallback'. Below this bar, a grey box displays the text 'Name: fallback'. The main area below the grey box is empty.

Implementing Office 365 and MS Exchange 2013 user access with BIGIP Access Policy Manager

Variable Assign

Properties

Branch Rules

Name: Variable Assign

Variable Assign

Add new entry

Insert Before: 1

	Assignment	
1	session.server.landinguri = expr { "/" } change	<input type="checkbox"/>

Implementing Office 365 and MS Exchange 2013 user access with BIGIP Access Policy Manager

Variable Assign

The screenshot shows the 'Branch Rules' configuration page in the BIGIP Access Policy Manager. At the top, there are two tabs: 'Properties' and 'Branch Rules', with 'Branch Rules' being the active tab. Below the tabs is a light blue bar containing an 'Add Branch Rule' button on the left and an 'Insert Before:' dropdown menu on the right, which is currently set to '1: fallback'. A horizontal dotted line separates this bar from the main content area. In the main content area, there is a single rule entry with a grey background and the text 'Name: fallback'.

Implementing Office 365 and MS Exchange 2013 user access with BIGIP Access Policy Manager

Full Resource Assign

Properties

Branch Rules

Name: Full Resource Assign

Resource Assignment

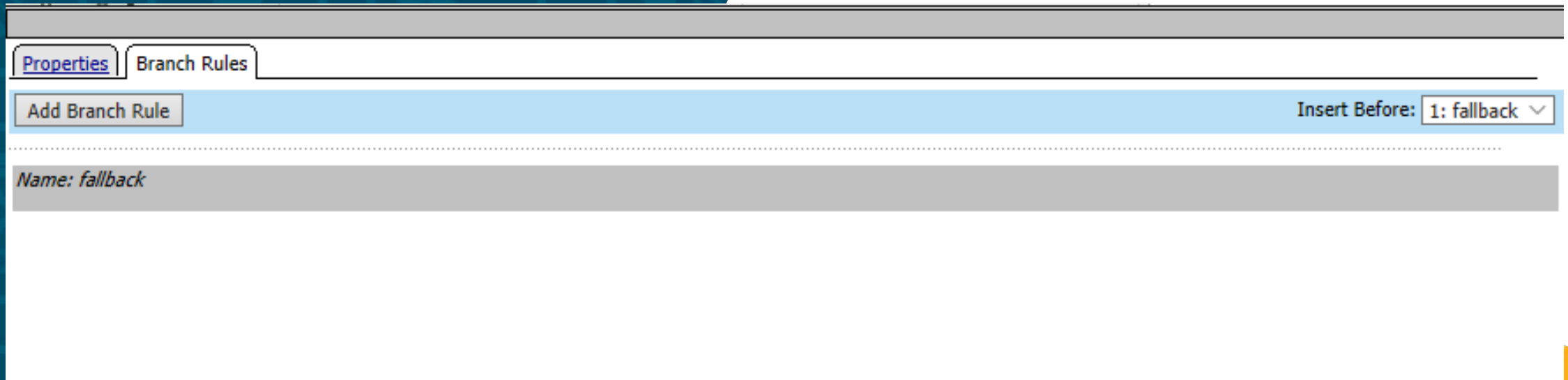
Add new entry

Expression: Empty [change](#)

1 SAML: /Common/0365.app/0365_apm_saml_resource_sso
[Add/Delete](#)

Implementing Office 365 and MS Exchange 2013 user access with BIGIP Access Policy Manager

Full Resource Assign



The screenshot displays the BIGIP Access Policy Manager web interface. At the top, there are two tabs: 'Properties' and 'Branch Rules', with 'Branch Rules' being the active tab. Below the tabs is a light blue bar containing an 'Add Branch Rule' button on the left and an 'Insert Before:' dropdown menu on the right, which is currently set to '1: fallback'. Below this bar is a grey bar with the text 'Name: fallback'. The main content area below is empty.

Implementing Office 365 and MS Exchange 2013 user access with BIGIP Access Policy Manager

Redirect to Office365

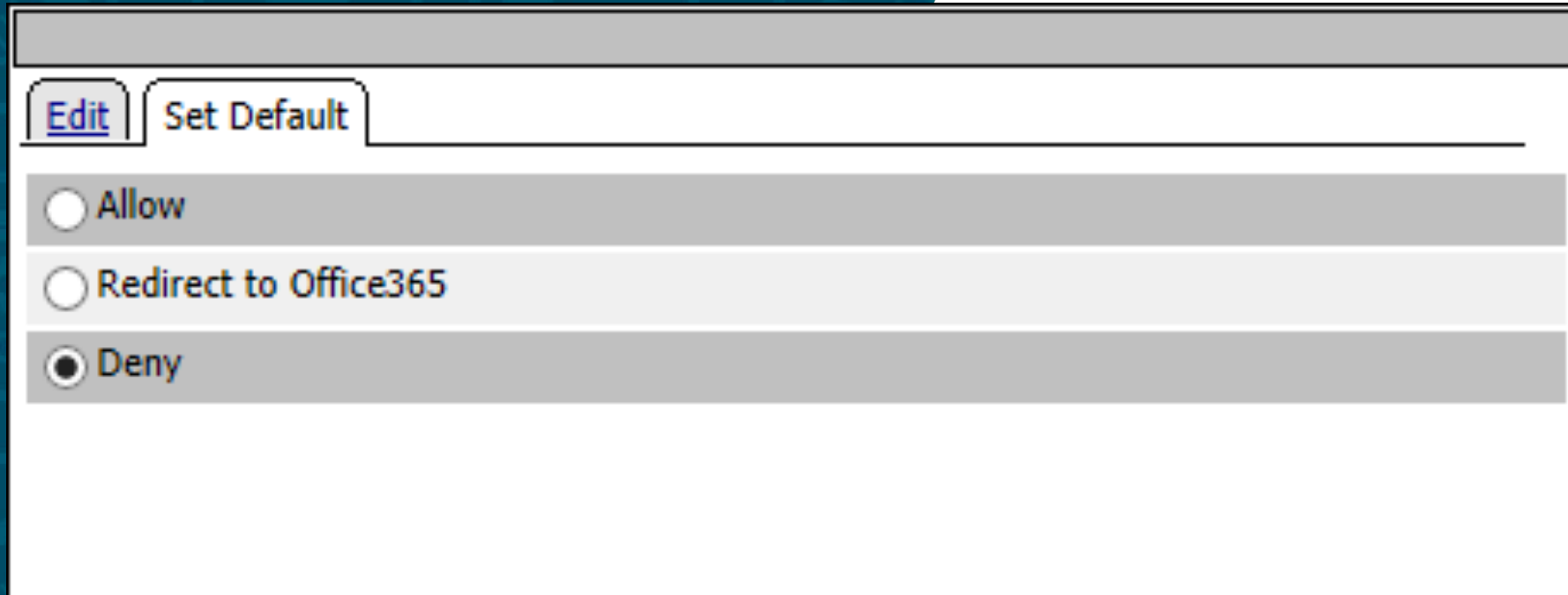
The screenshot displays the BIGIP Access Policy Manager configuration window. At the top, there are 'Edit' and 'Set Default' buttons. Below them is an 'Add Ending' button and a dropdown menu showing '1: Allow'. The main configuration area contains three policy rules:

- Rule 1:** Name: Allow, Priority: #1. Radio buttons: Deny, Redirect, Allow (selected).
- Rule 16:** Name: Redirect to Office365, Priority: #16. Radio buttons: Deny, Redirect (selected), Allow. Url: <https://outlook.office365.com/owa/my.capilanou.ca>. A checkbox for 'Close session after redirect' is present and unchecked.
- Rule 2:** Name: Deny, Priority: #2. Radio buttons: Deny (selected), Redirect, Allow. A 'default' label is visible to the right.

At the bottom, there is a '+ Customization' link.

Implementing Office 365 and MS Exchange 2013 user access with BIGIP Access Policy Manager

Redirect to Office365



The screenshot shows a web-based configuration interface for BIGIP Access Policy Manager. At the top, there are two tabs: 'Edit' and 'Set Default'. Below the tabs, there are three radio button options: 'Allow', 'Redirect to Office365', and 'Deny'. The 'Deny' option is currently selected, indicated by a filled black circle. The 'Redirect to Office365' option is highlighted with a light gray background, suggesting it is the target configuration.

Implementing Office 365 and MS Exchange 2013 user access with BIGIP Access Policy Manager

Exchange OWA SSO Credential Mapping

Properties

Branch Rules

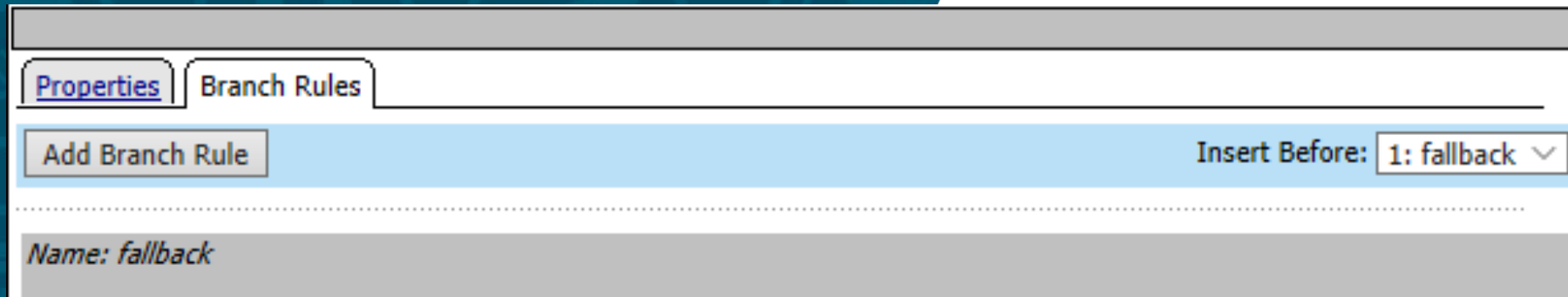
Name: Exchange OWA SSO Credential Mapping

Variable Assign: SSO Credential Mapping

SSO Token Username	<div>Username from Logon Page</div> <div>mcget {session.logon.last.username}</div>
SSO Token Password	<div>Password from Logon Page</div> <div>mcget {session.logon.last.password}</div>

Implementing Office 365 and MS Exchange 2013 user access with BIGIP Access Policy Manager

Exchange OWA SSO Credential Mapping



The screenshot shows the 'Branch Rules' tab in the BIGIP Access Policy Manager configuration interface. At the top, there are two tabs: 'Properties' and 'Branch Rules'. Below the tabs is a light blue bar containing an 'Add Branch Rule' button on the left and an 'Insert Before:' dropdown menu on the right, which is currently set to '1: fallback'. Below this bar is a list of existing branch rules. The first rule is visible, with the name 'fallback'.

Name
<i>fallback</i>

Implementing Office 365 and MS Exchange 2013 user access with BIGIP Access Policy Manager

O365-pool Assign



The screenshot shows the configuration interface for a policy named "O365-pool Assign". It features two tabs: "Properties" and "Branch Rules", with "Branch Rules" currently selected. Below the tabs, the "Name" field is populated with "O365-pool Assign". Under the "Pool Assignment" section, there is a table with one entry: "Static Pool (1)" with a path of "/Common/O365-pool". A blue "Add/Delete" link is positioned to the right of the "Static Pool (1)" entry.

Pool Assignment	
Static Pool (1)	Add/Delete
/Common/O365-pool	

Implementing Office 365 and MS Exchange 2013 user access with BIGIP Access Policy Manager

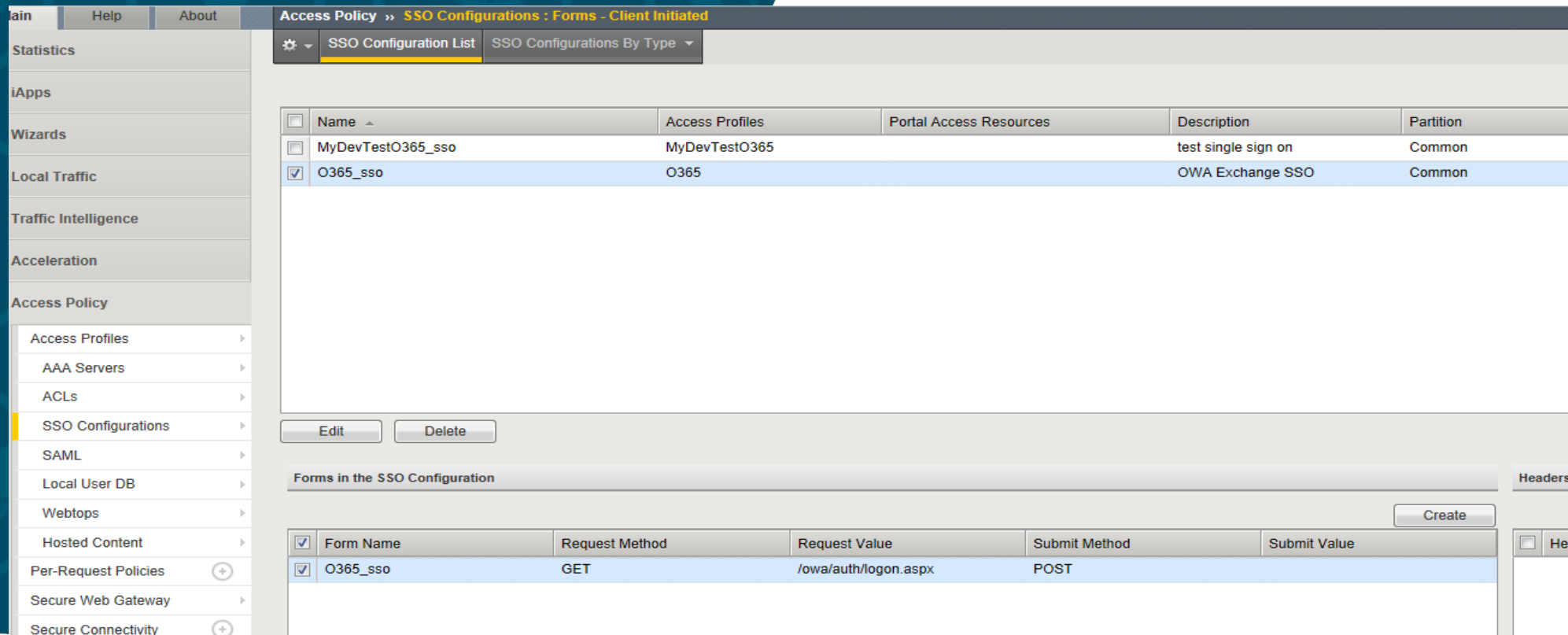
O365-pool Assign

The screenshot displays the BIGIP Access Policy Manager web interface. At the top, there are two tabs: 'Properties' and 'Branch Rules', with 'Branch Rules' being the active tab. Below the tabs is a light blue bar containing an 'Add Branch Rule' button on the left and an 'Insert Before: 1: fallback' dropdown menu on the right. A horizontal dotted line separates this header from the main content area. The main content area has a grey header bar with the text 'Name: fallback' in italics. The rest of the content area is white and currently empty.

Implementing Office 365 and MS Exchange 2013 user access with BIGIP Access Policy Manager

Create SSO Client Initiated Form for MS Exchange.

Our SSO Configuration calls O365_sso. See below.



The screenshot displays the BIGIP Access Policy Manager web interface. The left sidebar shows the navigation menu with 'Access Policy' expanded, and 'SSO Configurations' selected. The main content area is titled 'Access Policy >> SSO Configurations : Forms - Client Initiated'. It features a table of SSO configurations and a section for forms within a selected configuration.

SSO Configuration List

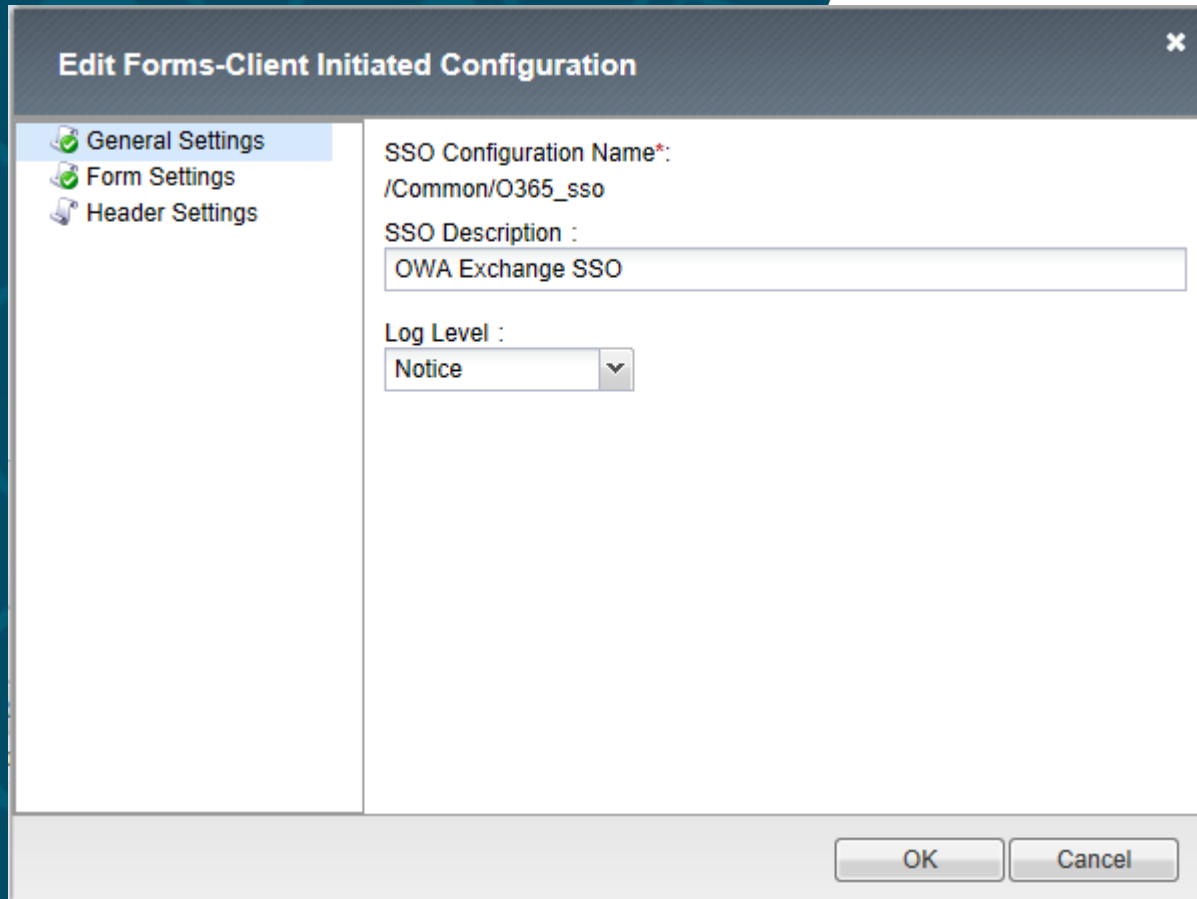
<input type="checkbox"/>	Name	Access Profiles	Portal Access Resources	Description	Partition
<input type="checkbox"/>	MyDevTestO365_sso	MyDevTestO365		test single sign on	Common
<input checked="" type="checkbox"/>	O365_sso	O365		OWA Exchange SSO	Common

Forms in the SSO Configuration

<input checked="" type="checkbox"/>	Form Name	Request Method	Request Value	Submit Method	Submit Value
<input checked="" type="checkbox"/>	O365_sso	GET	/owa/auth/logon.aspx	POST	

Implementing Office 365 and MS Exchange 2013 user access with BIGIP Access Policy Manager

Let's walk through O365_sso configuration.



Edit Forms-Client Initiated Configuration

General Settings
Form Settings
Header Settings

SSO Configuration Name*:
/Common/O365_sso

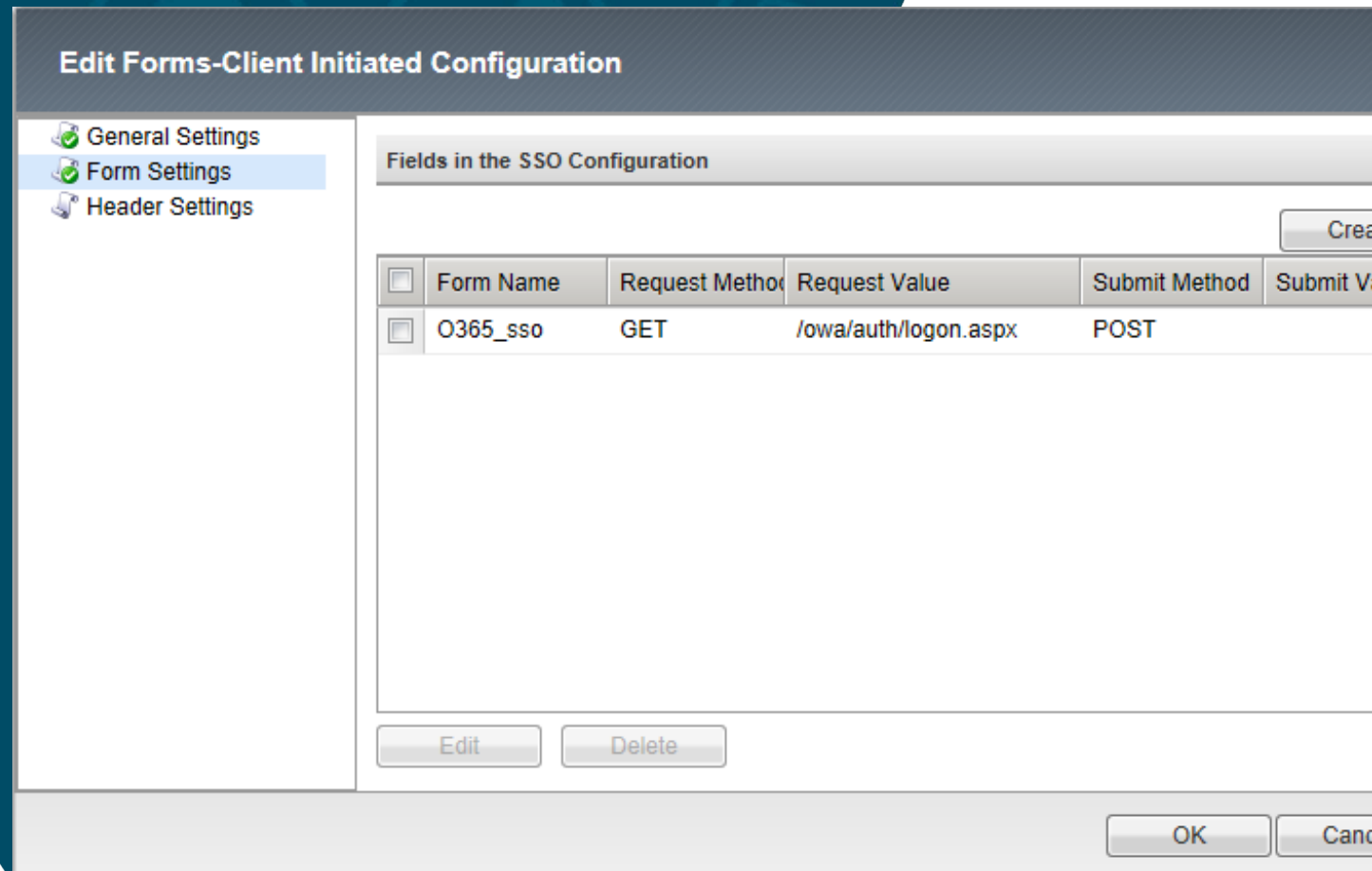
SSO Description :
OWA Exchange SSO

Log Level :
Notice

OK Cancel

Implementing Office 365 and MS Exchange 2013 user access with BIGIP Access Policy Manager

O365_sso configuration continue.



Edit Forms-Client Initiated Configuration

General Settings
Form Settings
Header Settings

Fields in the SSO Configuration

<input type="checkbox"/>	Form Name	Request Method	Request Value	Submit Method	Submit Value
<input type="checkbox"/>	O365_sso	GET	/owa/auth/logon.aspx	POST	

Edit Delete

OK Cancel

Implementing Office 365 and MS Exchange 2013 user access with BIGIP Access Policy Manager

O365_sso configuration continue.

Edit Form Definition

Parameter Settings

- ☒ Form Parameters
- ☒ Form Detection
- ☒ Form Identification
- ☒ Logon Detection
- ☒ Advanced Settings
 - ☒ Javascript Injection
 - ☒ Submit Detection

Form Name*:
O365_sso

Form Description :
OWA Exchange SSO

OK Cancel

Implementing Office 365 and MS Exchange 2013 user access with BIGIP Access Policy Manager

O365_sso configuration continue.

Edit Form Definition

Parameter Settings

- Form Parameters
- Form Detection
- Form Identification
- Logon Detection
- Advanced Settings
 - Javascript Injection
 - Submit Detection

Form Parameters

Create

<input type="checkbox"/>	Form Parameter Name ▲	Form Parameter Value	Secure
<input type="checkbox"/>	password	%{session.sso.token.last.password}	true
<input type="checkbox"/>	username	%{session.sso.token.last.username}	

Edit Delete

OK Cancel

Implementing Office 365 and MS Exchange 2013 user access with BIGIP Access Policy Manager

O365_sso configuration continue.

Edit Form Definition

- Parameter Settings
- Form Parameters
- Form Detection**
- Form Identification
- Logon Detection
- Advanced Settings
- Javascript Injection
- Submit Detection

Detect Form by:

Request URI*:
/owa/auth/logon.aspx

OK Cancel

Implementing Office 365 and MS Exchange 2013 user access with BIGIP Access Policy Manager

O365_sso configuration continue.

Edit Form Definition

- Parameter Settings
 - Form Parameters
 - Form Detection
 - Form Identification**
 - Logon Detection
- Advanced Settings
 - Javascript Injection
 - Submit Detection

Identify Form by: Form Parameters

No user configurable settings

OK Cancel

Implementing Office 365 and MS Exchange 2013 user access with BIGIP Access Policy Manager

O365_sso configuration continue.

Edit Form Definition

- Parameter Settings
 - Form Parameters
 - Form Detection
 - Form Identification
 - Logon Detection**
- Advanced Settings
 - Javascript Injection
 - Submit Detection

Detect Login by: Presence of Cookie

Cookie Name*:
cadata

OK

Implementing Office 365 and MS Exchange 2013 user access with BIGIP Access Policy Manager

O365_sso configuration continue.

Edit Form Definition

- Parameter Settings
 - Form Parameters
 - Form Detection
 - Form Identification
 - Logon Detection
 - Advanced Settings (selected)
 - Javascript Injection
 - Submit Detection

Form Request

Request Method : GET

☐ Request Negative

☒ Request Prefix

Form Submit Request

☐ Submit Request Negative

☒ Submit Request Prefix

OK Cancel

Implementing Office 365 and MS Exchange 2013 user access with BIGIP Access Policy Manager

O365_sso configuration continue.

Edit Form Definition

- Parameter Settings
 - Form Parameters
 - Form Detection
 - Form Identification
 - Logon Detection
- Advanced Settings
 - Javascript Injection**
 - Submit Detection

Injection Method:

Extra Javascript*:
clkLgn()

OK

Implementing Office 365 and MS Exchange 2013 user access with BIGIP Access Policy Manager

O365_sso configuration continue.

Edit Form Definition

- Parameter Settings
 - Form Parameters
 - Form Detection
 - Form Identification
 - Logon Detection
- Advanced Settings
 - Javascript Injection
 - Submit Detection**

Disable Auto detect submit :
No

Scheme: URI

URI :

OK

Implementing Office 365 and MS Exchange 2013 user access with BIGIP Access Policy Manager

O365_sso configuration continue.

Edit Forms-Client Initiated Configuration

- General Settings
- Form Settings
- Header Settings**

Headers in the SSO Configuration

Create

<input type="checkbox"/>	Header Name	Header Value
--------------------------	-------------	--------------

Edit Delete

OK Cancel

Implementing Office 365 and MS Exchange 2013 user access with BIGIP Access Policy Manager

Add next objects:

- Create O365-pool pool to handle MS Exchange traffic. MExchangeCAS2013prod_owa_https_monitor was used to monitor the pool. The pool has two members, exfe1.prn.capilano.ca (204.239.151.64) and exfe2.prn.capilano.ca (204.239.151.65) CAS servers.
- O365_vs Virtual Server is created when the iApp was deployed. Create a Virtual Server to redirect HTTP traffic to O365_vs Virtual Server to communicate over HTTPS.
- Next iRules are attached to O365_vs serve, see the picture below.
/Common/O365.app/O365_encode_ObjectGUID_irule
iRule was created during the template deployment.

Implementing Office 365 and MS Exchange 2013 user access with BIGIP Access Policy Manager

iRules

Local Traffic » Virtual Servers : Virtual Server List » O365_vs

⚙️ Properties Resources Statistics

Load Balancing

Default Pool	None
Default Persistence Profile	None
Fallback Persistence Profile	None

Update

iRules

Name
/Common/_sys_APM_Office365_SAML_BasicAuth
/Common/O365.app/O365_encode_ObjectGUID_irule
/Common/O365-URI-rewrite-iRule
/Common/O365-ExchangeOWA-Logout-iRule

Implementing Office 365 and MS Exchange 2013 user access with BIGIP Access Policy Manager

_sys_APM_Office365_SAML_BasicAuth

```
when RULE_INIT {  
    set static::ACCESS_LOG_ECP_PREFIX "014d0002:7: ECP client"  
}  
when HTTP_REQUEST {  
    set http_path [string tolower [HTTP::path]]  
    set http_hdr_auth [HTTP::header Authorization]  
    set http_hdr_client_app [HTTP::header X-MS-Client-Application]  
    set http_hdr_client_ip [HTTP::header X-MS-Forwarded-Client-IP]  
    set MRHSession_cookie [HTTP::cookie value MRHSession]  
    ...  
}
```

Implementing Office 365 and MS Exchange 2013 user access with BIGIP Access Policy Manager

O365-URI-rewrite-iRule

```
when CLIENT_ACCEPTED {  
    ACCESS::restrict_irule_events disable  
}  
when ACCESS_POLICY_AGENT_EVENT {  
    if {[ACCESS::policy agent_id] eq "rewrite"} {  
        log local0. "Calling Rewrite iRule. URI: [HTTP::uri]"  
        if { [HTTP::uri] contains "/saml/idp/profile/redirectorpost/sso" } {  
            HTTP::uri /owa/  
            log local0. "Rewrite URI to [HTTP::uri]"  
        }  
    }  
}
```

Implementing Office 365 and MS Exchange 2013 user access with BIGIP Access Policy Manager

O365-ExchangeOWA-Logout-iRule

```
when RULE_INIT {  
    set static::cookie_sessionid [format "sessionid=null; path=/; Expires=Thur, 01-Jan-1970 00:00:00 GMT;"]  
    set static::cookie_cadata [format "cadata=null; path=/; Expires=Thur, 01-Jan-1970 00:00:00 GMT;"]  
    set static::cookie_usercontext [format "UserContext=null; path=/; Expires=Thur, 01-Jan-1970 00:00:00 GMT;"]  
}  
  
when ACCESS_SESSION_STARTED {  
    if { [string tolower [HTTP::uri]] contains "ua=0" } {  
        ACCESS::session remove  
        #    log local0. "****SESSION REMOVED****"  
    }  
}  
...
```

Implementing Office 365 and MS Exchange 2013 user access with BIGIP Access Policy Manager

O365_encode_ObjectGUID irule

```
when ACCESS_POLICY_AGENT_EVENT {  
  if {[ACCESS::policy agent_id] eq "encode"} {  
    set tmpVar [binary format H* [substr "[ACCESS::session data get  
session.ad.last.attr.objectGUID]" 2]]  
    ACCESS::session data set session.ad.last.attr.objectGUIDencoded [b64encode $tmpVar]  
  }  
}
```

Implementing Office 365 and MS Exchange 2013 user access with BIGIP Access Policy Manager

- After the changes outlined in this document were made to the initial iApp deployment this configuration should be able to handle authentication and SSO functionality for MS Office365 and MS Exchange users.
- Additional documentation:
<https://devcentral.f5.com/articles/office-365-logon-enhancement-username-capture-27497> “Office 365 Logon Enhancement – Username Capture”

Implementing Office 365 and MS Exchange 2013 user access with BIGIP Access Policy Manager

Limitations of the implementation.

Implementing Office 365 and MS Exchange 2013 user access with BIGIP Access Policy Manager

This configuration ignores an account's UPN. Users can be authenticated against one AD domain only. Additional APM logic needs to be put in place to accommodate authentication of users belonging to different AD domains.

Implementing Office 365 and MS Exchange 2013 user access with BIGIP Access Policy Manager

We found there is a learning curve to do the F5 BIG-IP APM branding and customizations. Graphical interface available in F5 BIG-IP APM we found was somewhat limited.

Implementing Office 365 and MS Exchange 2013 user access with BIGIP Access Policy Manager

There is an interesting example to see insights on how to modify F5 BIG-IP APM policy “Office 365 Logon Enhancement – Username Capture” at F5 DevCentral at <https://devcentral.f5.com/articles/office-365-logon-enhancement-username-capture-27497>