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 *Document Revision History on page 19*)

BCNET 2019

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.

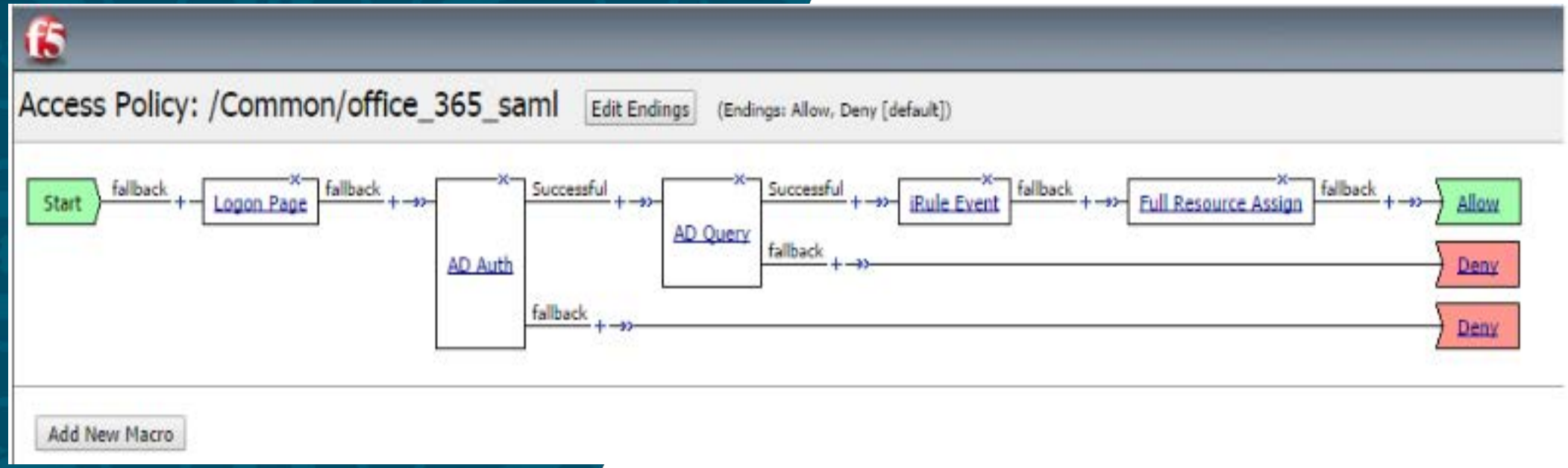
O365 iApp f5.microsoft_office_365_idp.v1.1.0 template deployment consists of a questionnaire. See the questionnaire with answers provided below.

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

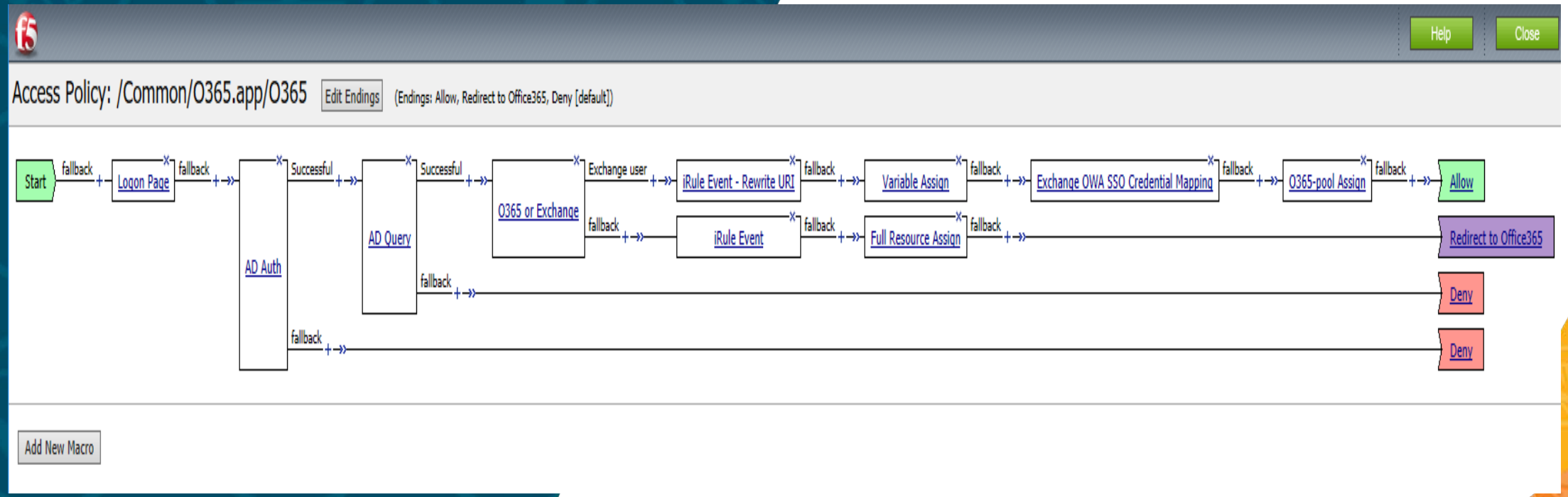
Implementing Office 365 and MS Exchange 2013 user access with BIGIP Access Policy Manager



BCNET 2019

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	myCapU Email Sign In
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]

BCNET 2019

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

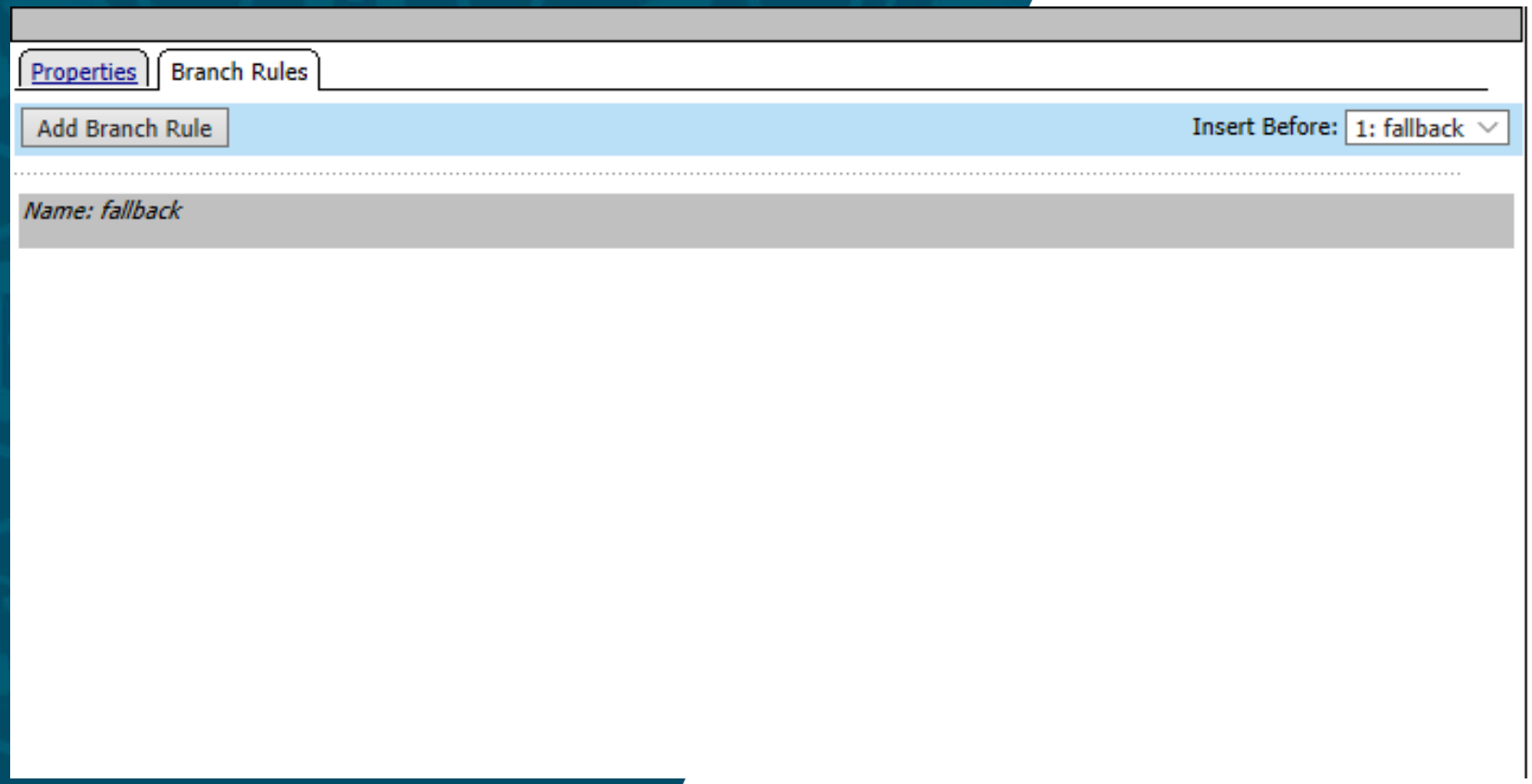
Logon Page

Save Password Checkbox	Save Password
New Password Prompt	New Password
Verify Password Prompt	Verify Password
Pasword 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

Cancel Save Help

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

Logon Page



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

AD Auth

Properties | Branch Rules

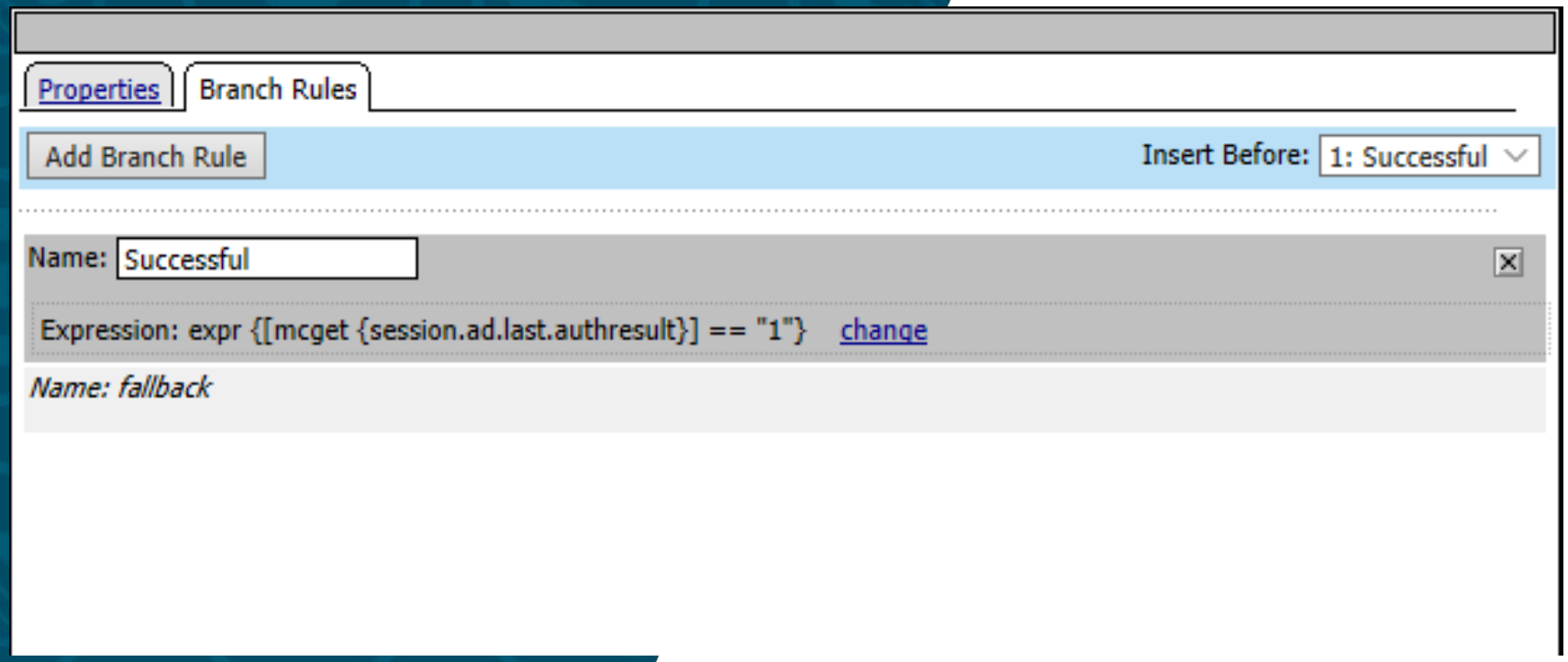
Name: AD Auth

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



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

AD Query

Properties | Branch Rules

Name: AD Query

Active Directory

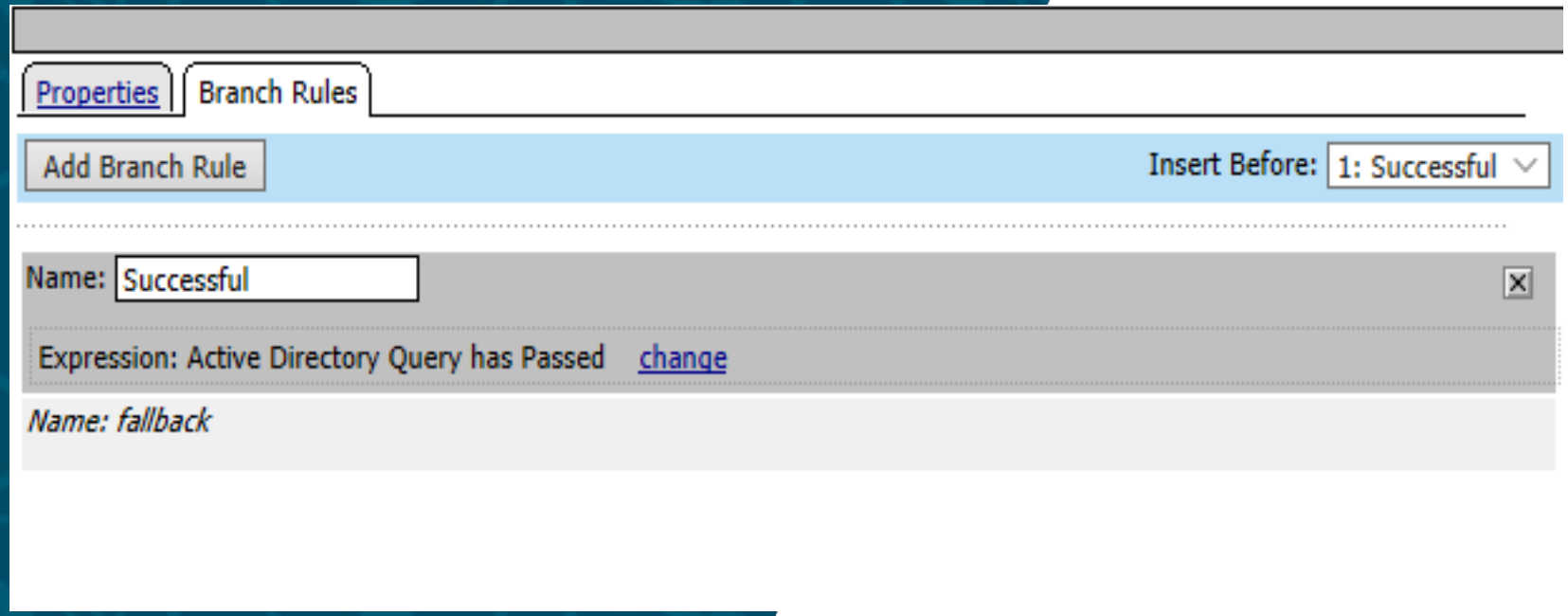
Type	Query
Server	/Common/O365.app/O365_apm_aaa
SearchFilter	samAccountName=%{session.logon.last.username}
Fetch Primary Group	Disabled
Cross Domain Support	Disabled
Fetch Nested Groups	Disabled
Complexity check for Password Reset	Disabled
Max Password Reset Attempts Allowed	3
Prompt user to change password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

Add new entry Insert Before:

Required Attributes (optional)

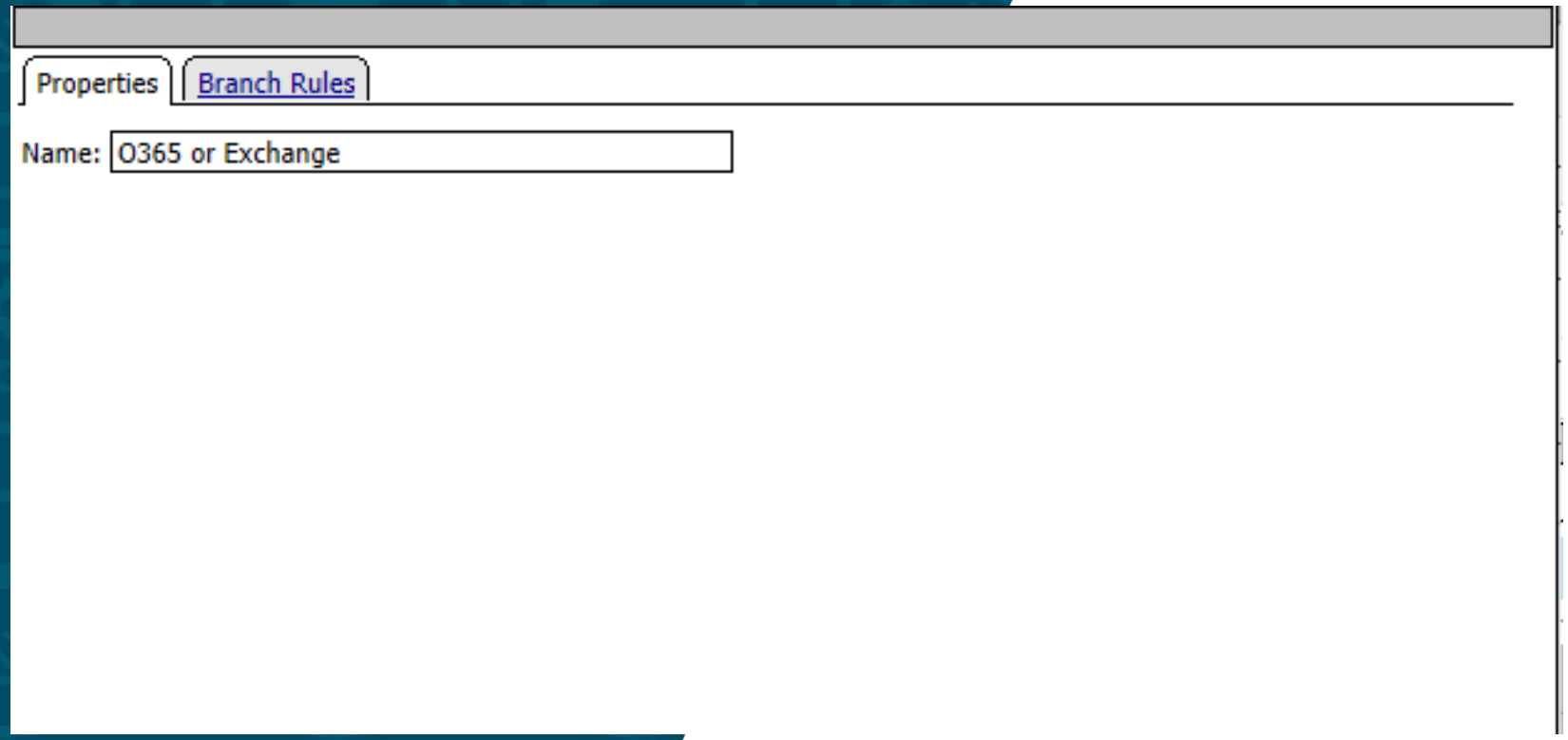
Implementing Office 365 and MS Exchange 2013 user access with BIGIP Access Policy Manager

AD Query



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

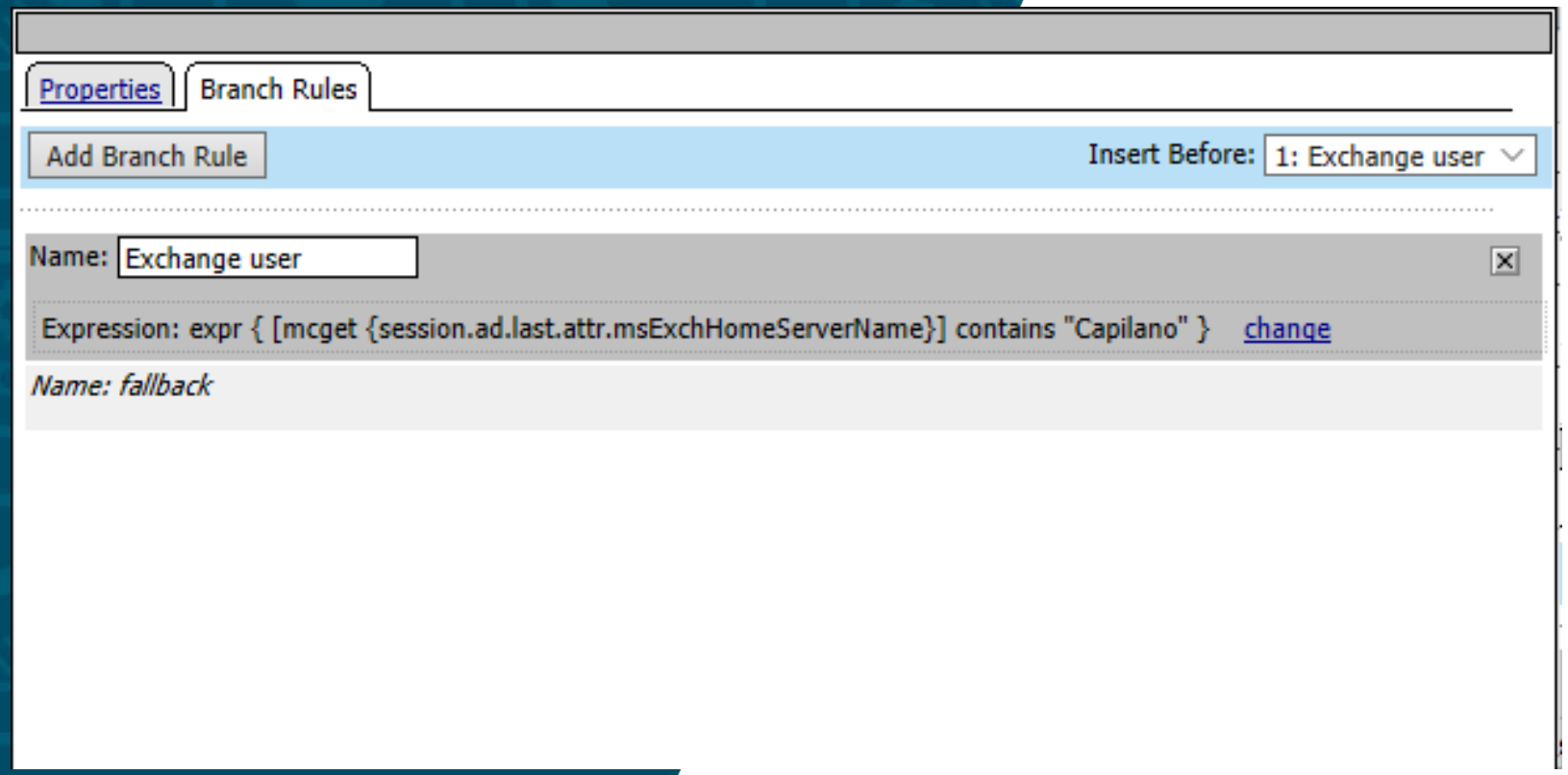
O365 or Exchange



BCNET 2019

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

O365 or Exchange



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

iRule Event – Rewrite URI

Properties | Branch Rules

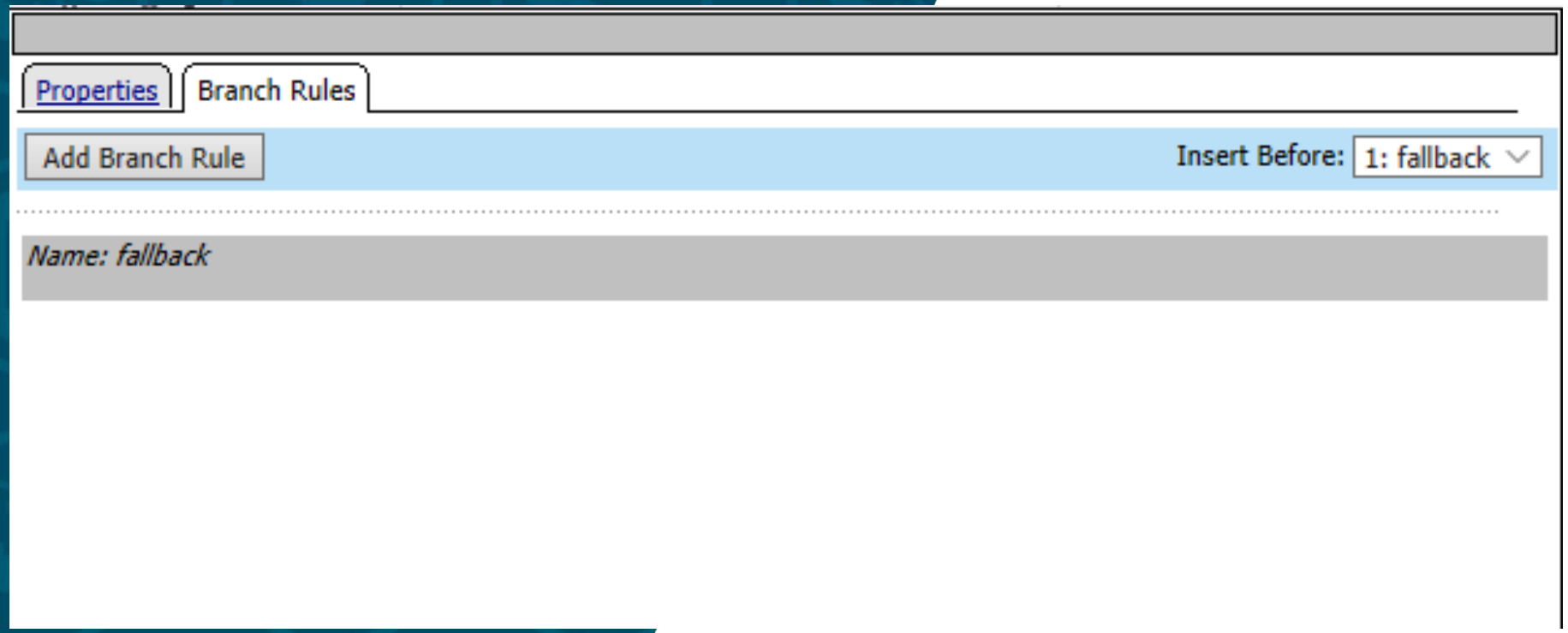
Name: iRule Event - Rewrite URI

Custom iRule Event Agent

ID	rewrite

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

iRule Event – Rewrite URI



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

iRule Event

Properties | Branch Rules

Name: iRule Event

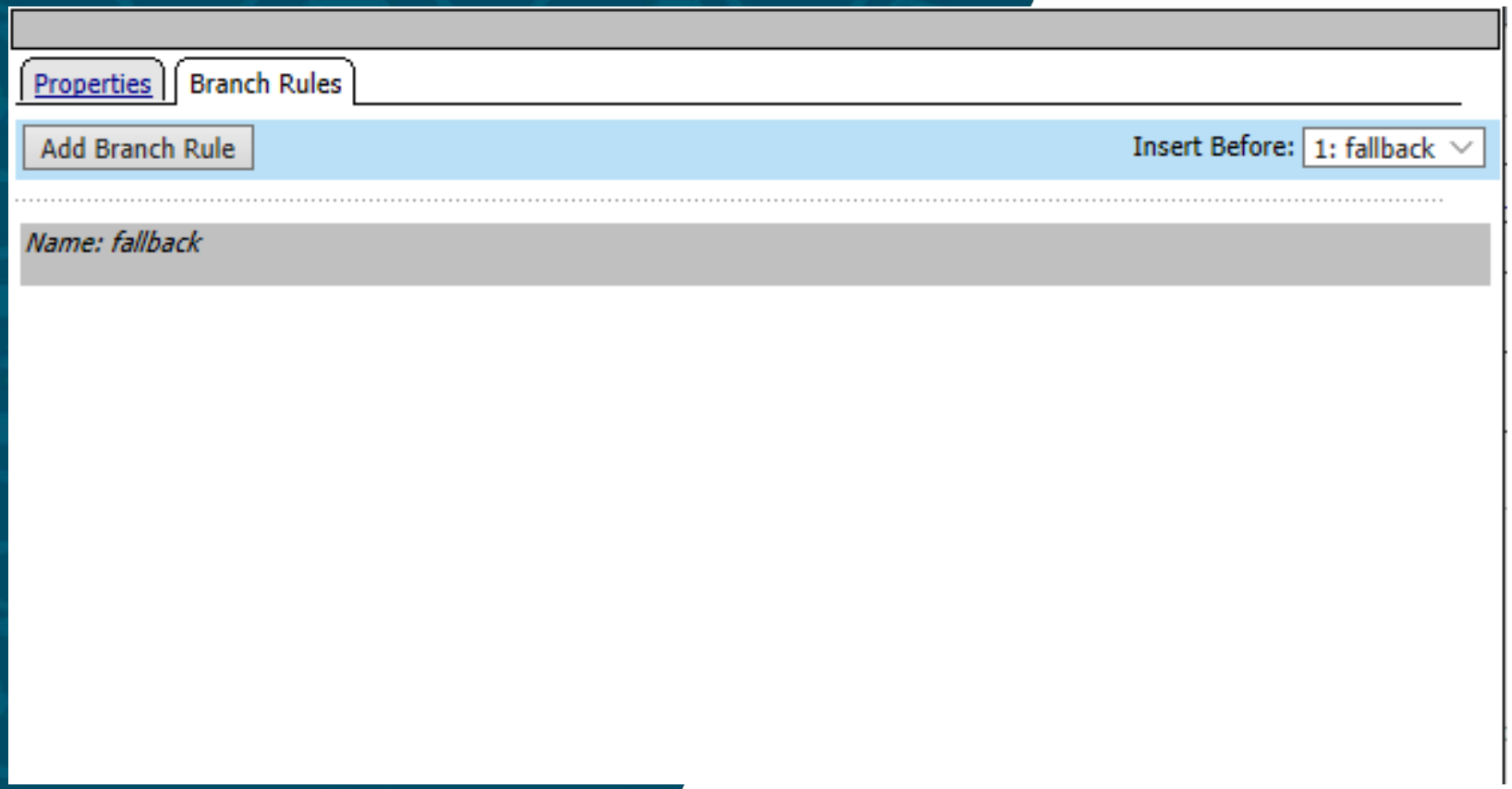
Custom iRule Event Agent

ID	encode

BCNET 2019

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

iRule Event



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

Variable Assign

Properties | Branch Rules

Name: Variable Assign

Variable Assign

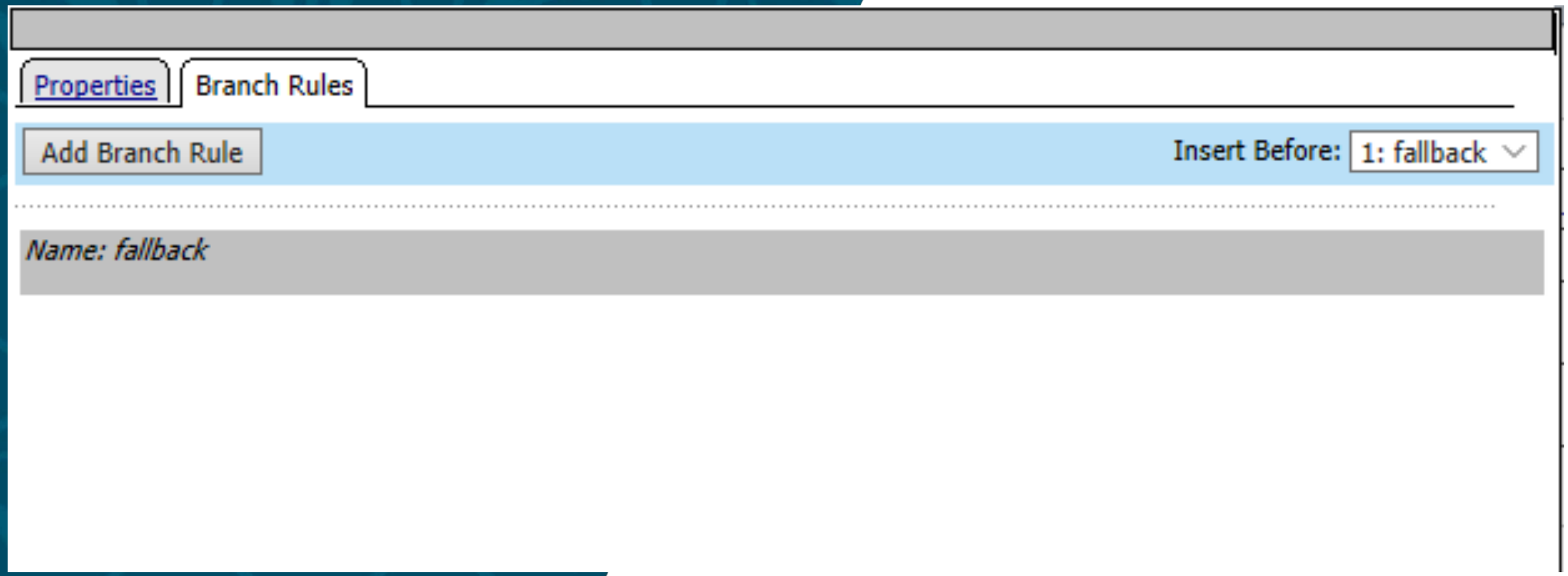
Add new entry

Insert Before: 1

	Assignment	
1	session.server.landinguri = expr { "/" } change	

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

Variable Assign



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

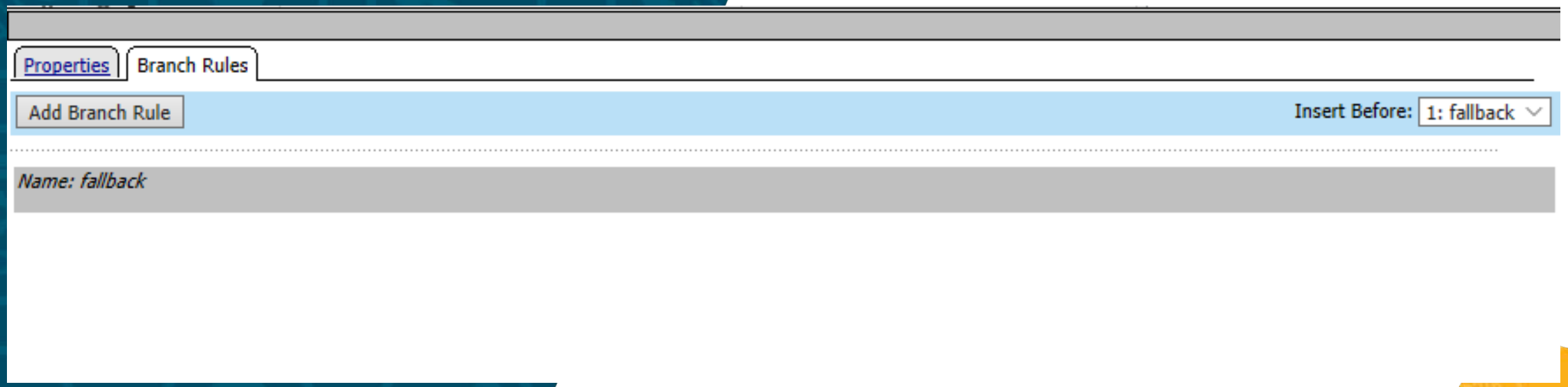
Expression: *Empty* change

1 **SAML:** /Common/O365.app/O365_apm_saml_resource_sso

Add/Delete

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

Full Resource Assign



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

Redirect to Office365

Edit | Set Default

Add Ending | 1: Allow

Name: Allow #1

Deny Redirect Allow

Name: Redirect to Office365 #16

Deny Redirect Allow

Url:

https://outlook.office365.com/owa/my.capilanou.ca

Close session after redirect

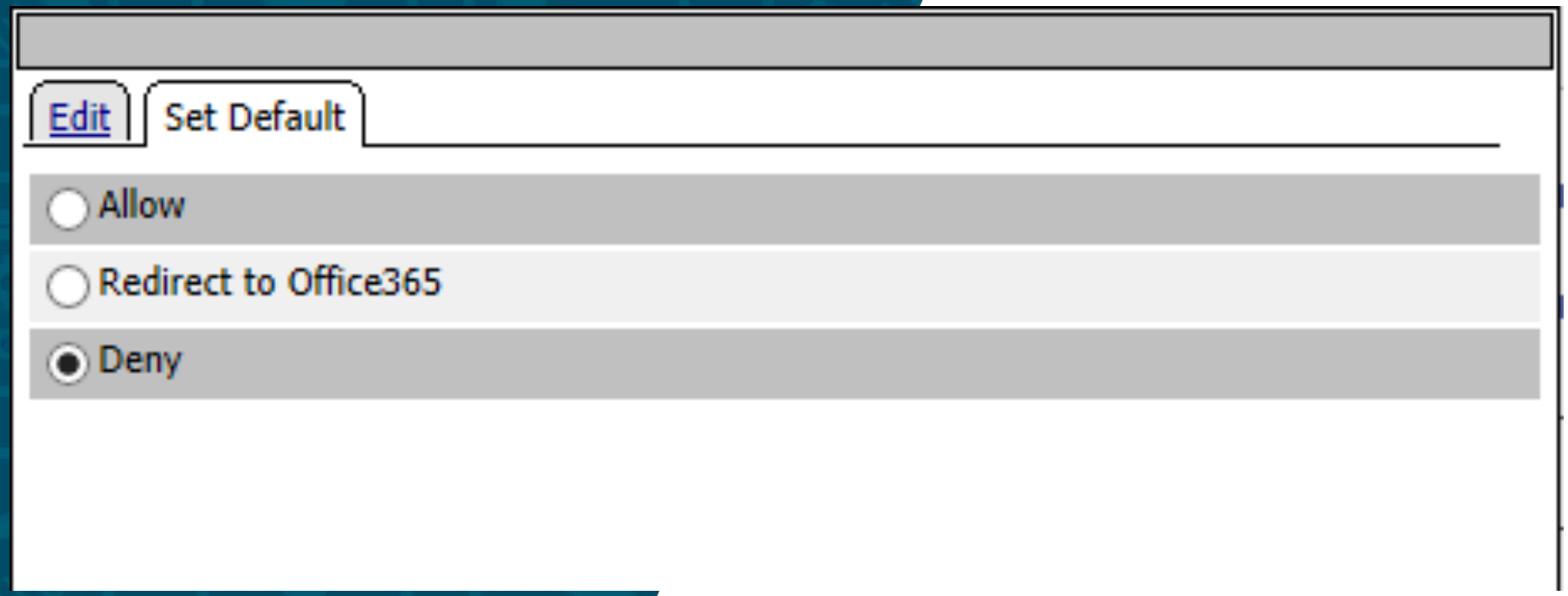
Name: Deny #2 default

Deny Redirect Allow

Customization

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

Redirect to Office365



BCNET 2019

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

Exchange OWA SSO Credential Mapping

Properties | Branch Rules

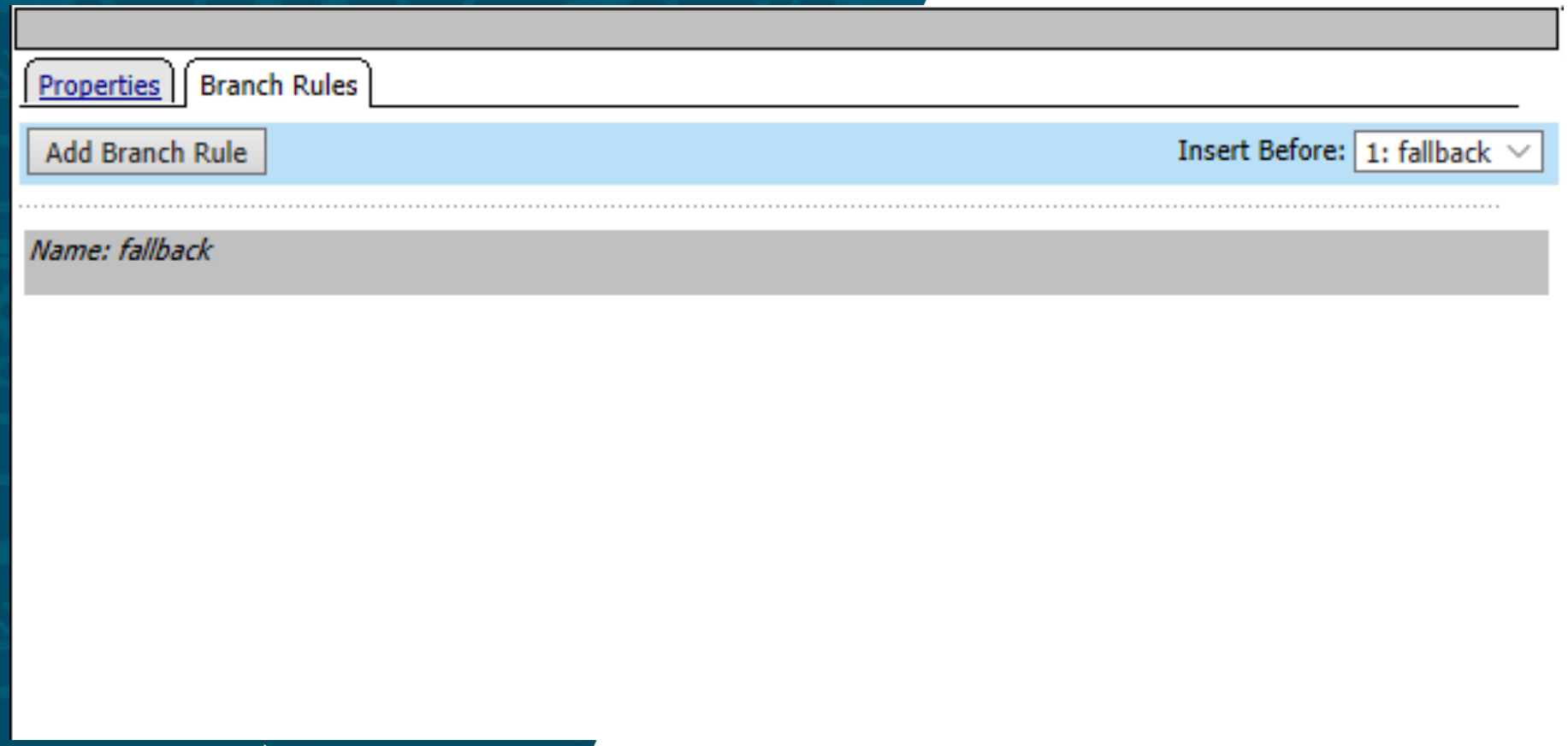
Name: Exchange OWA SSO Credential Mapping

Variable Assign: SSO Credential Mapping

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

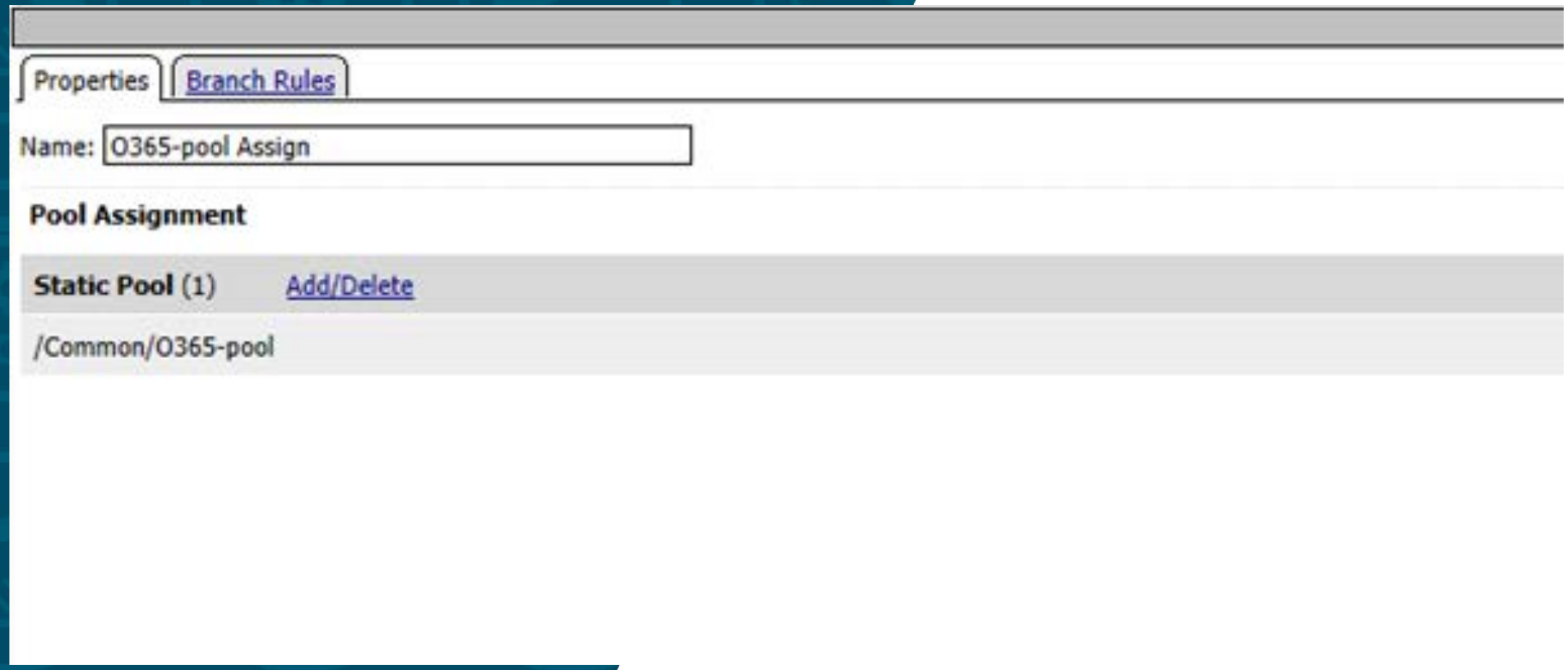
Implementing Office 365 and MS Exchange 2013 user access with BIGIP Access Policy Manager

Exchange OWA SSO Credential Mapping



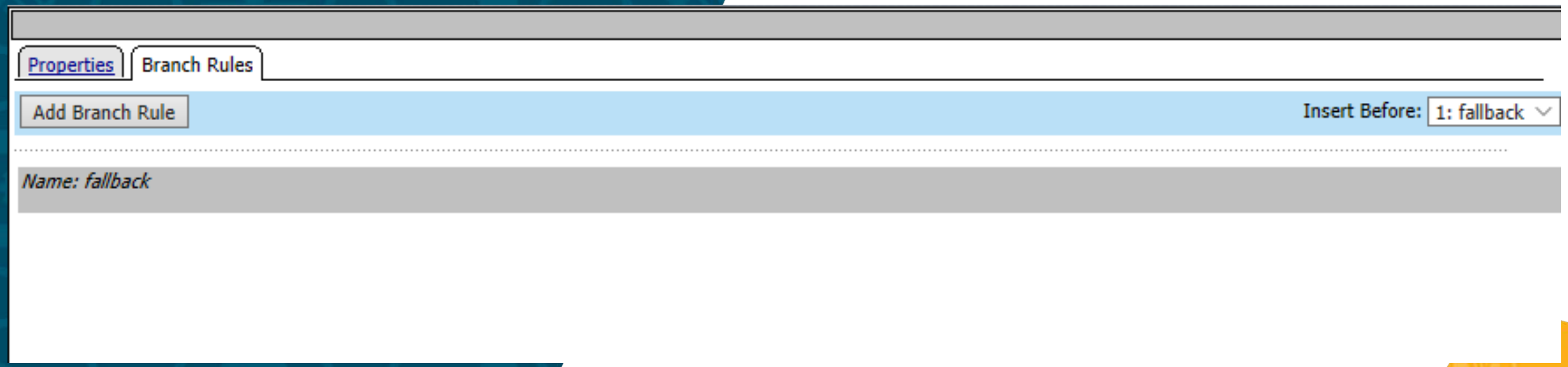
Implementing Office 365 and MS Exchange 2013 user access with BIGIP Access Policy Manager

O365-pool Assign



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

O365-pool Assign

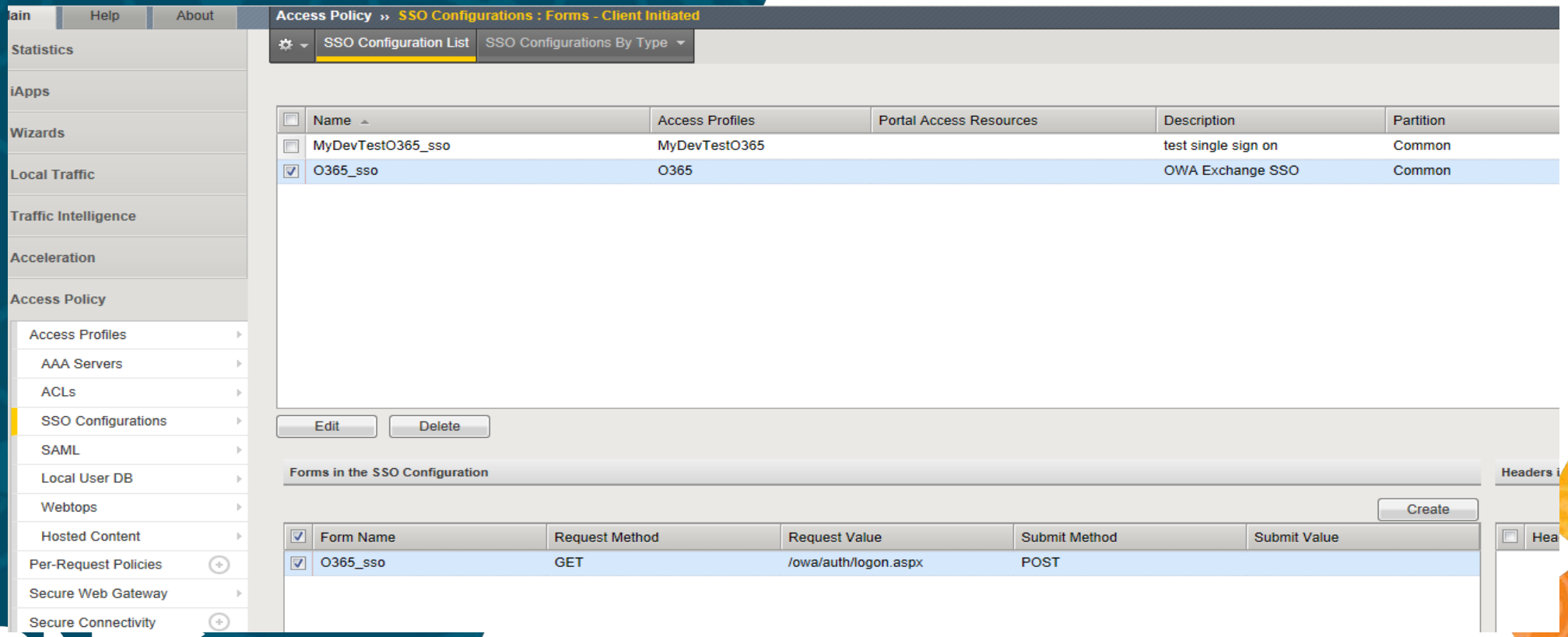


BCNET 2019

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

Create SSO Client Initiated Form for MS Exchange.

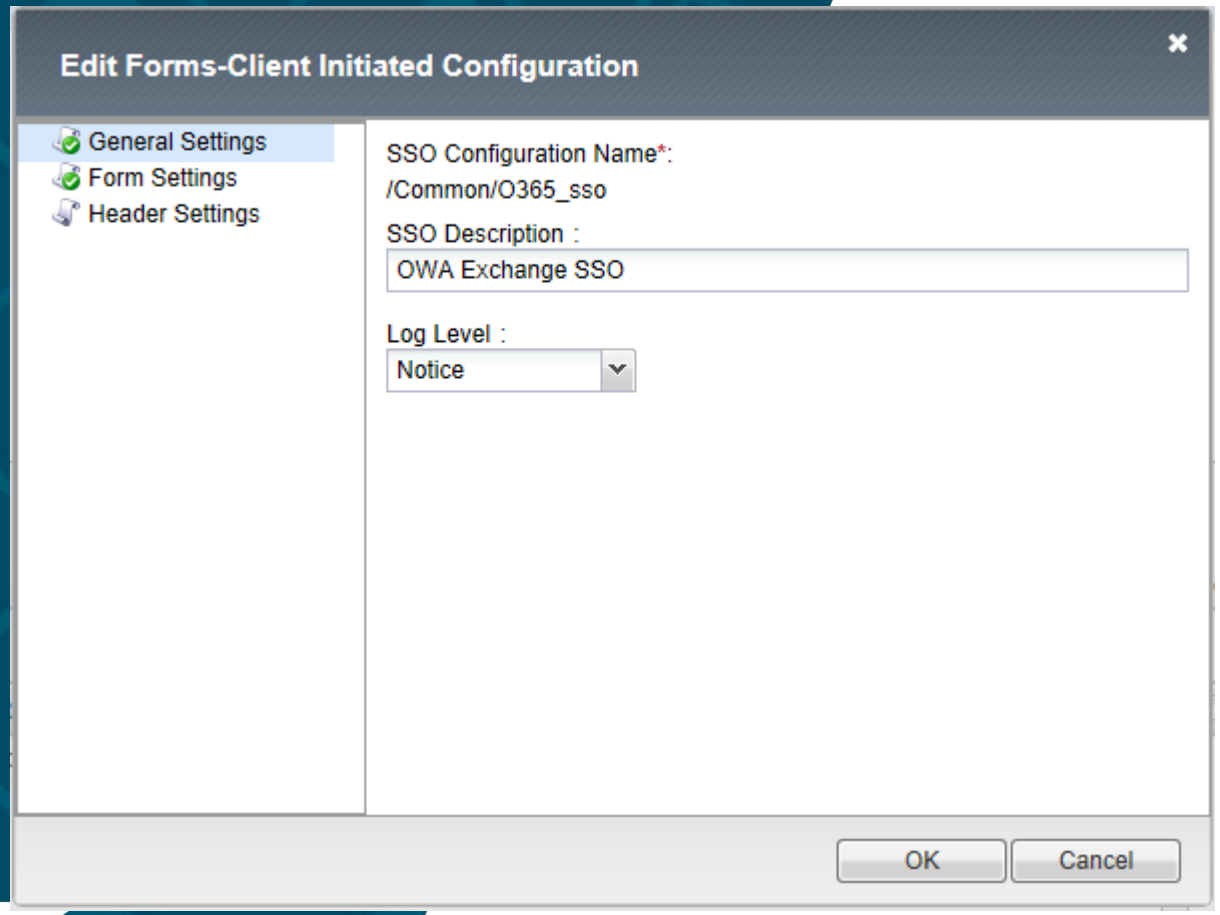
Our SSO Configuration calls O365_sso. See below.



BCNET 2019

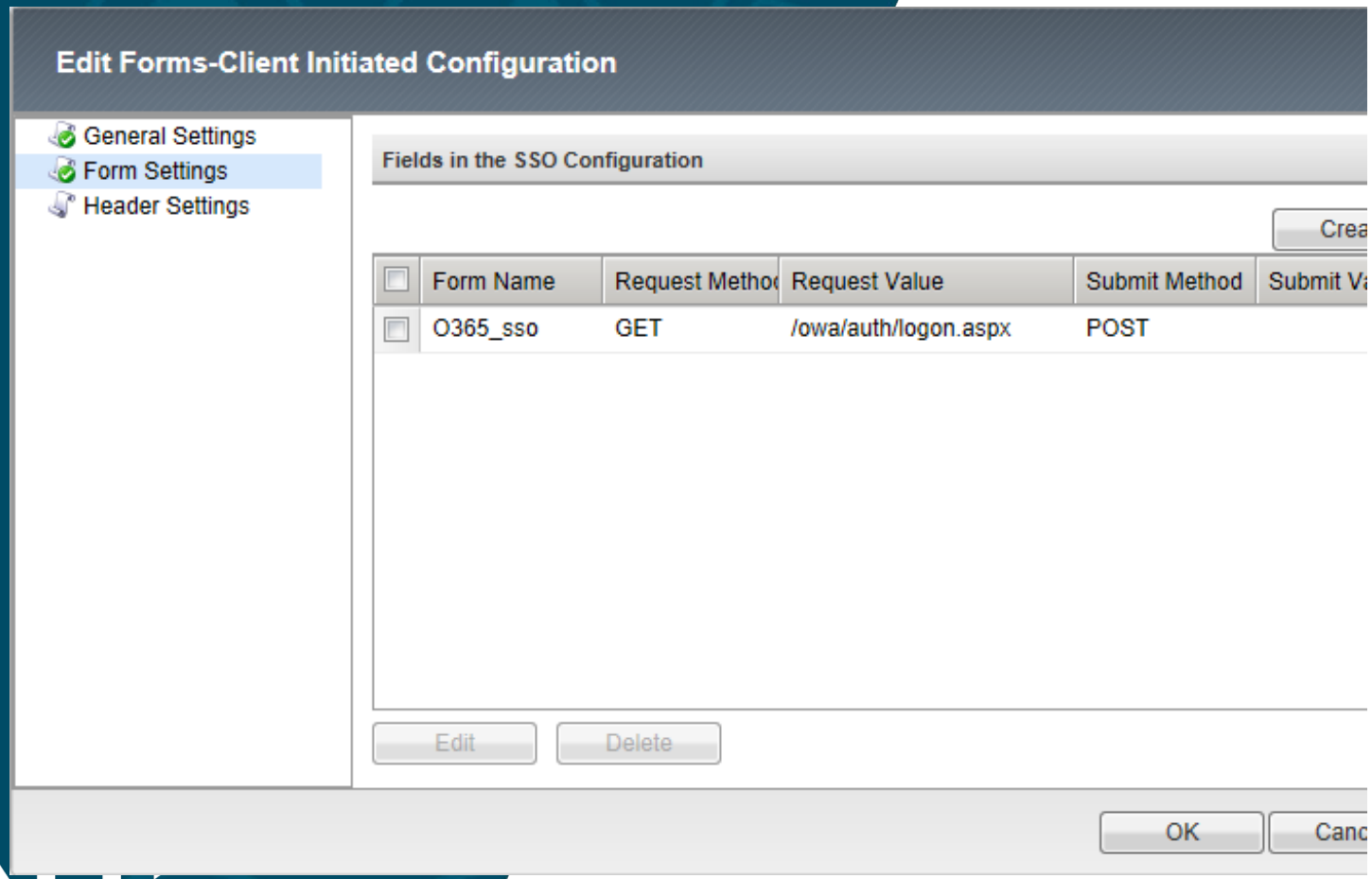
Implementing Office 365 and MS Exchange 2013 user access with BIGIP Access Policy Manager

Let's walk through O365_sso configuration.



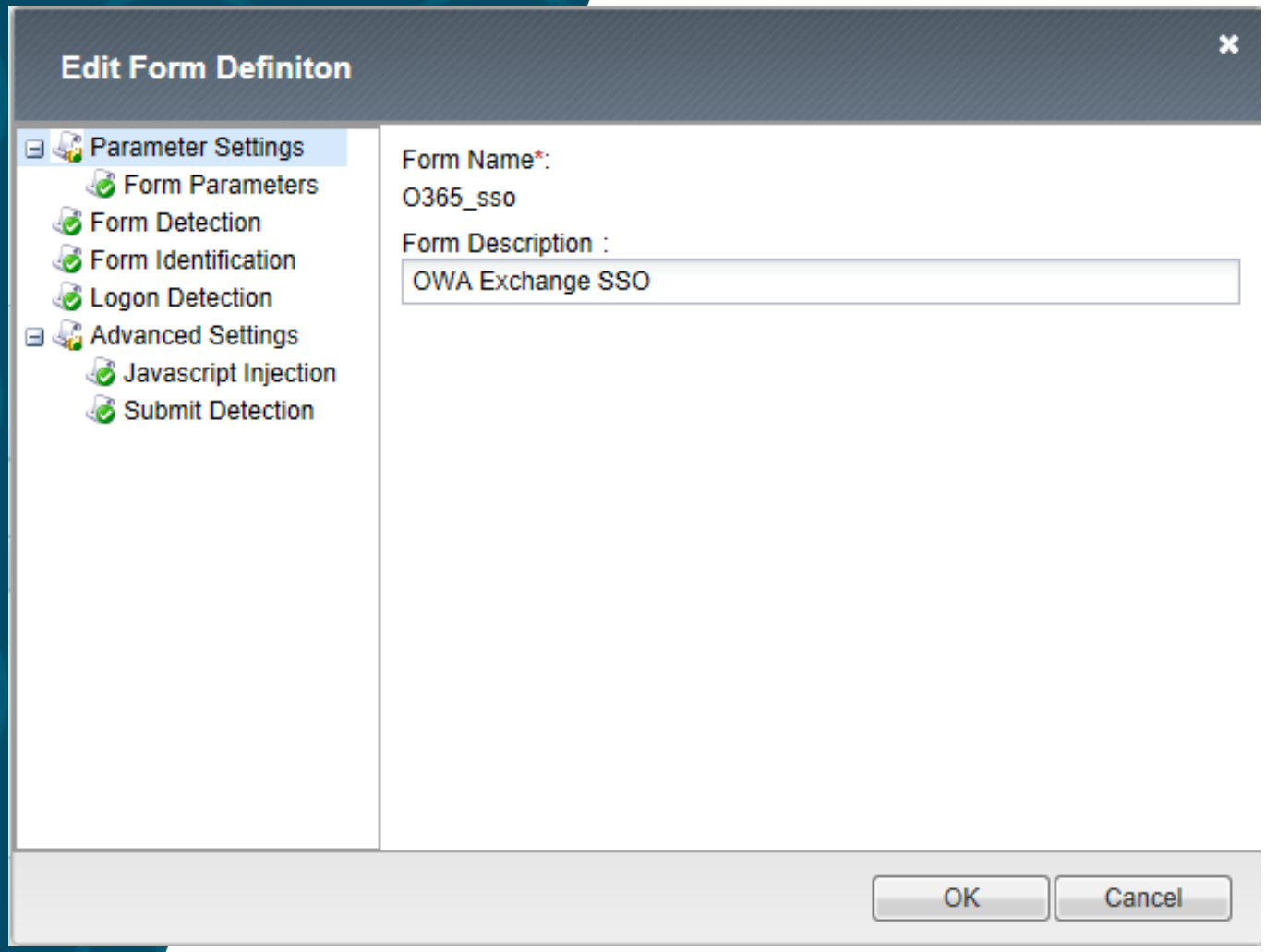
Implementing Office 365 and MS Exchange 2013 user access with BIGIP Access Policy Manager

O365_sso configuration continue.



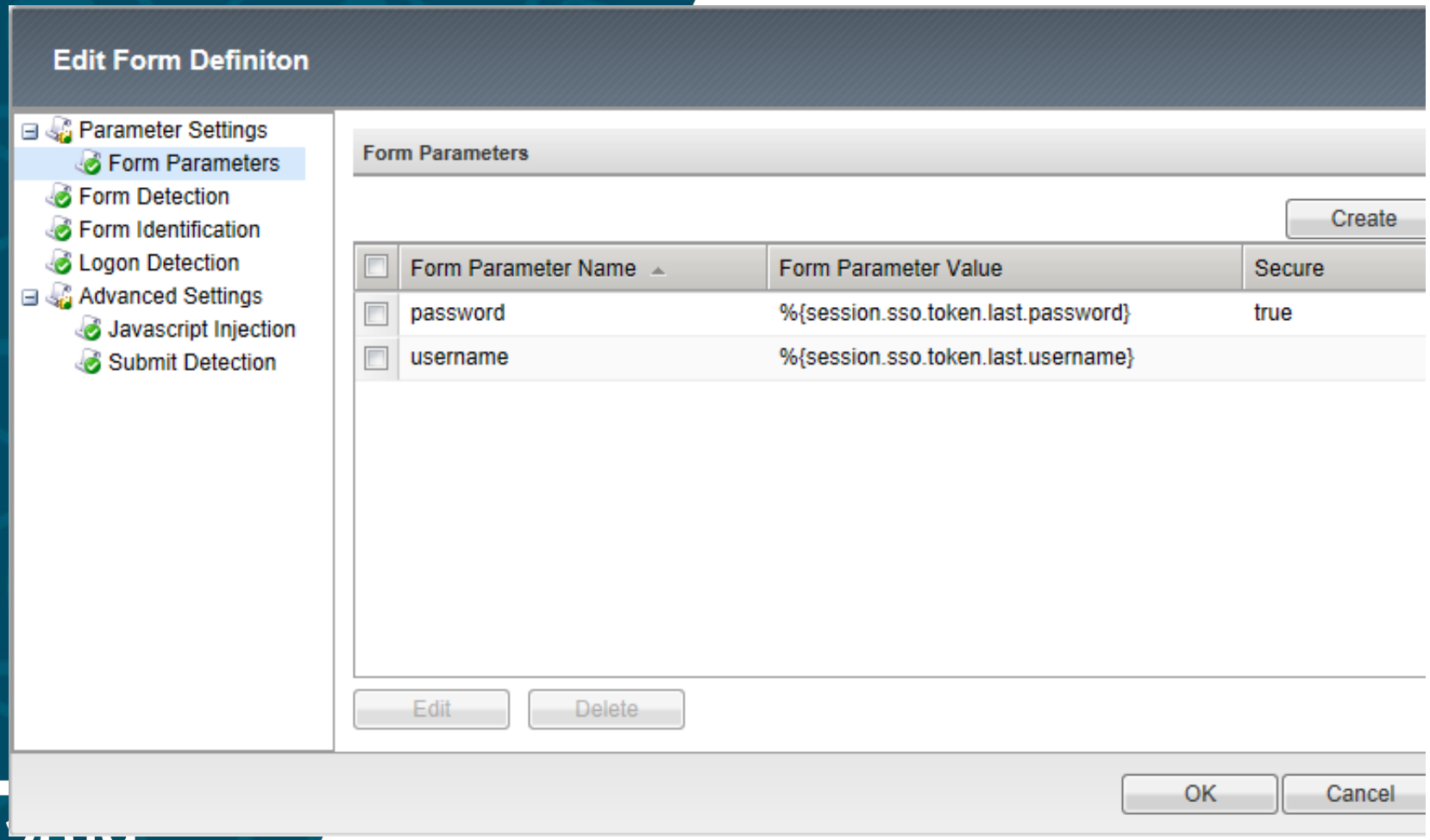
Implementing Office 365 and MS Exchange 2013 user access with BIGIP Access Policy Manager

O365_sso configuration continue.



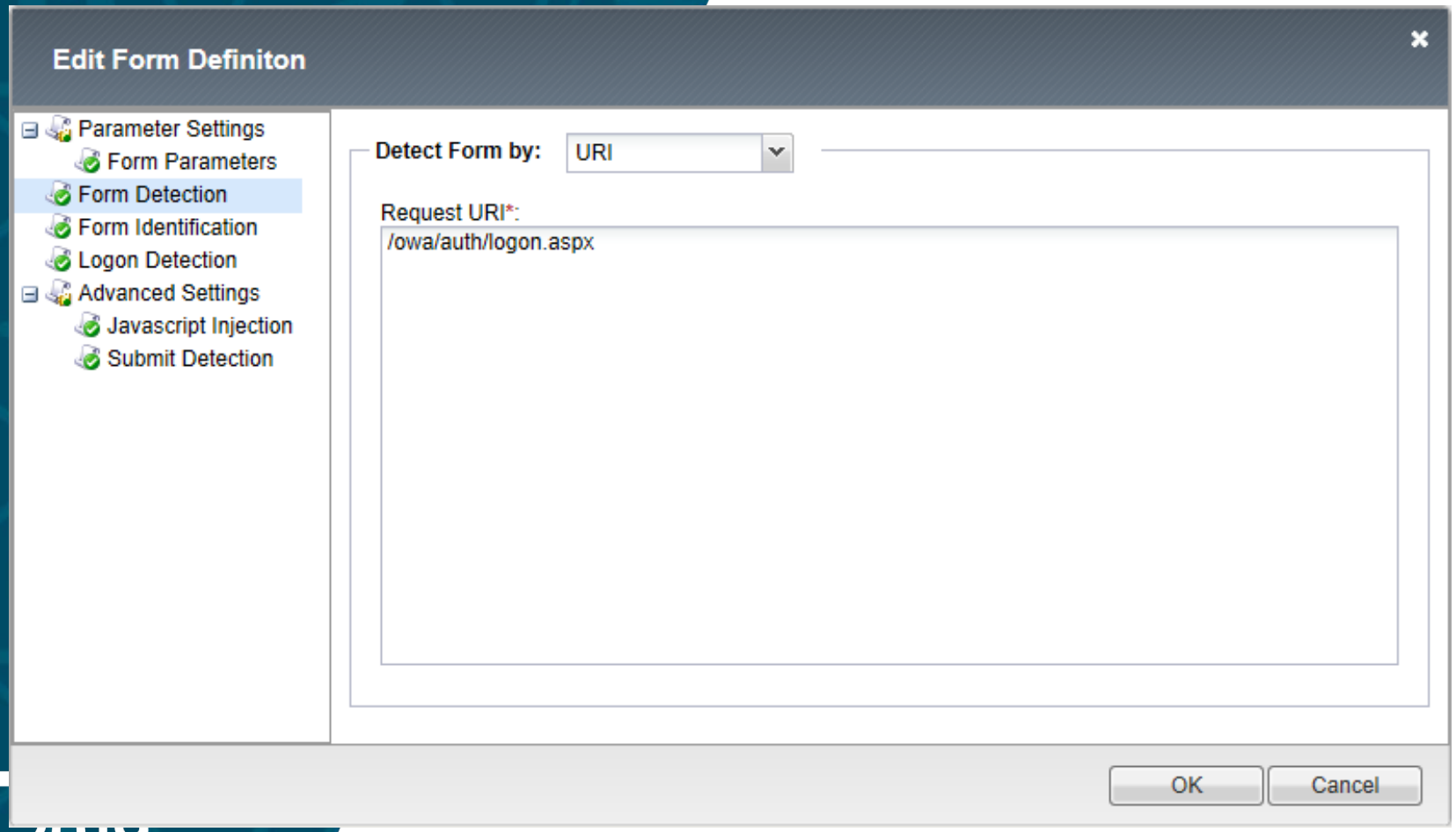
Implementing Office 365 and MS Exchange 2013 user access with BIGIP Access Policy Manager

O365_sso configuration continue.



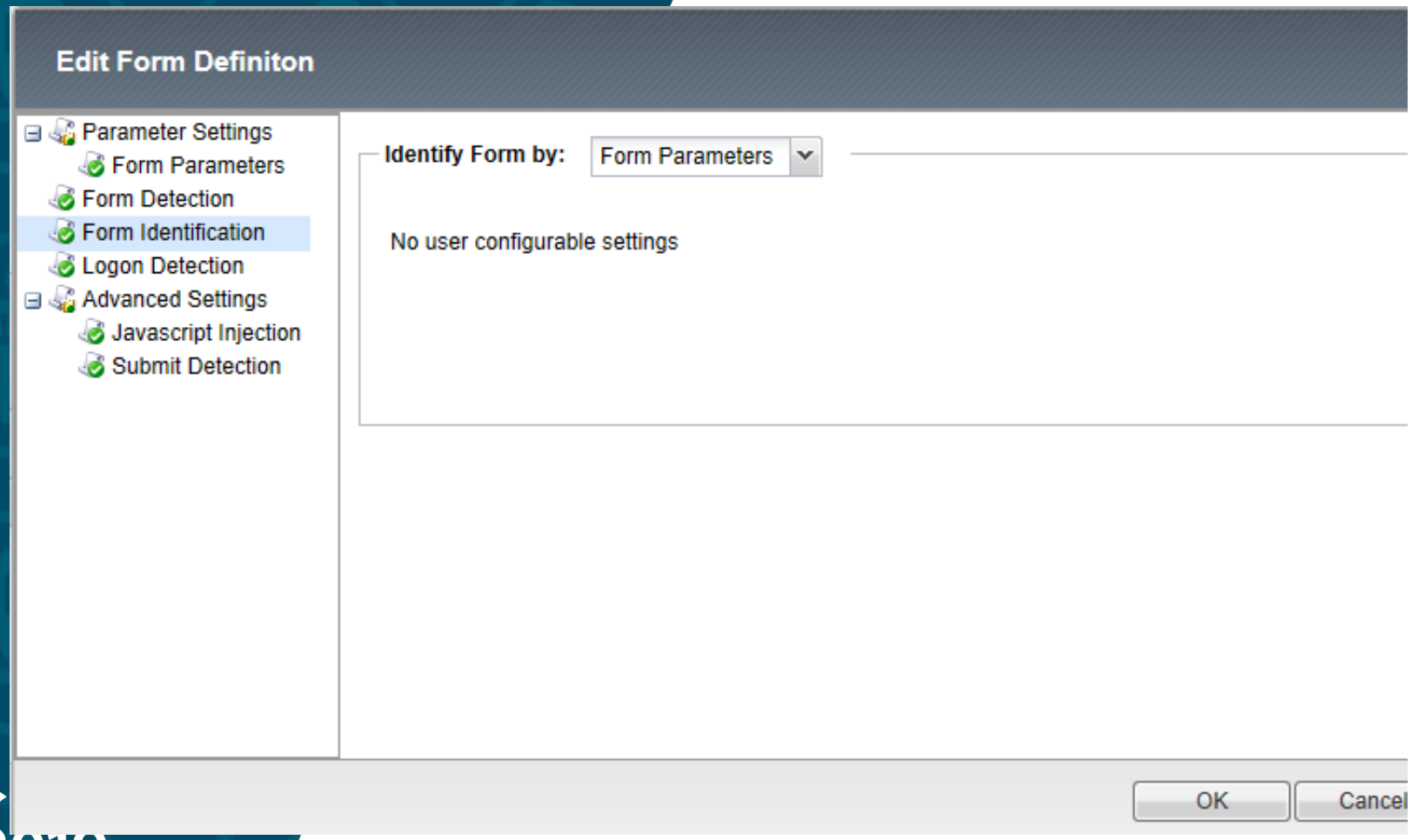
Implementing Office 365 and MS Exchange 2013 user access with BIGIP Access Policy Manager

O365_sso configuration continue.



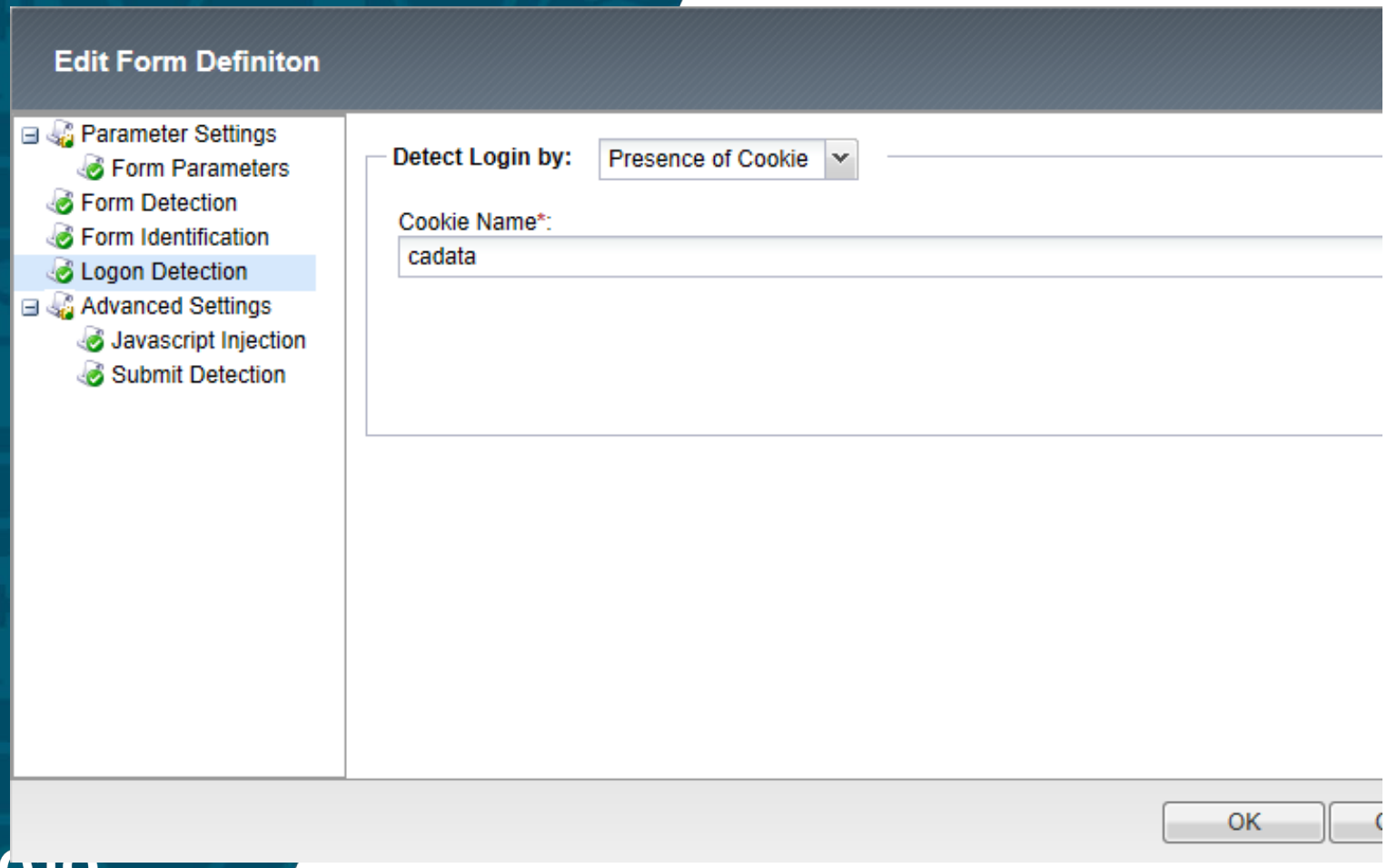
Implementing Office 365 and MS Exchange 2013 user access with BIGIP Access Policy Manager

O365_sso configuration continue.



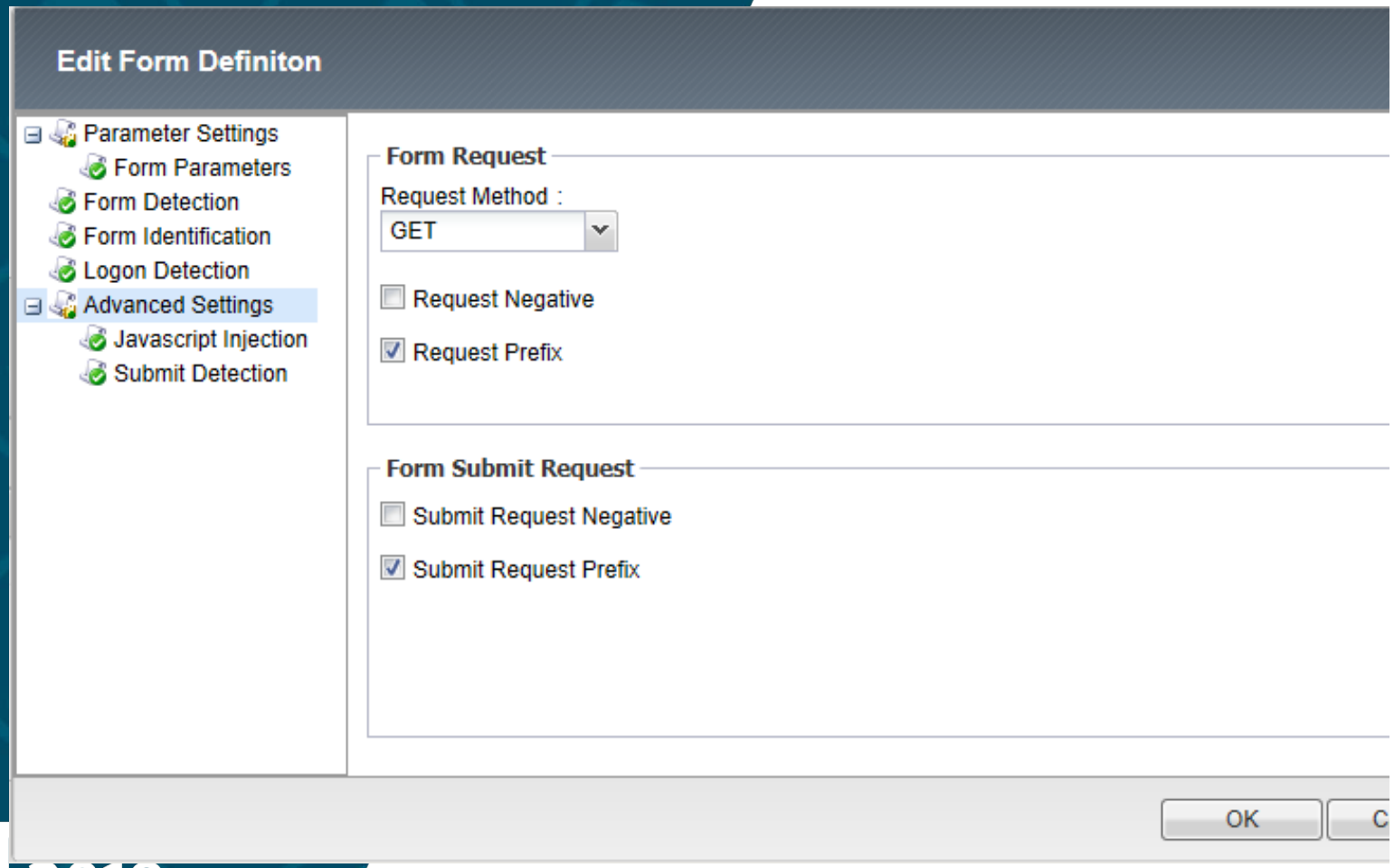
Implementing Office 365 and MS Exchange 2013 user access with BIGIP Access Policy Manager

O365_sso configuration continue.



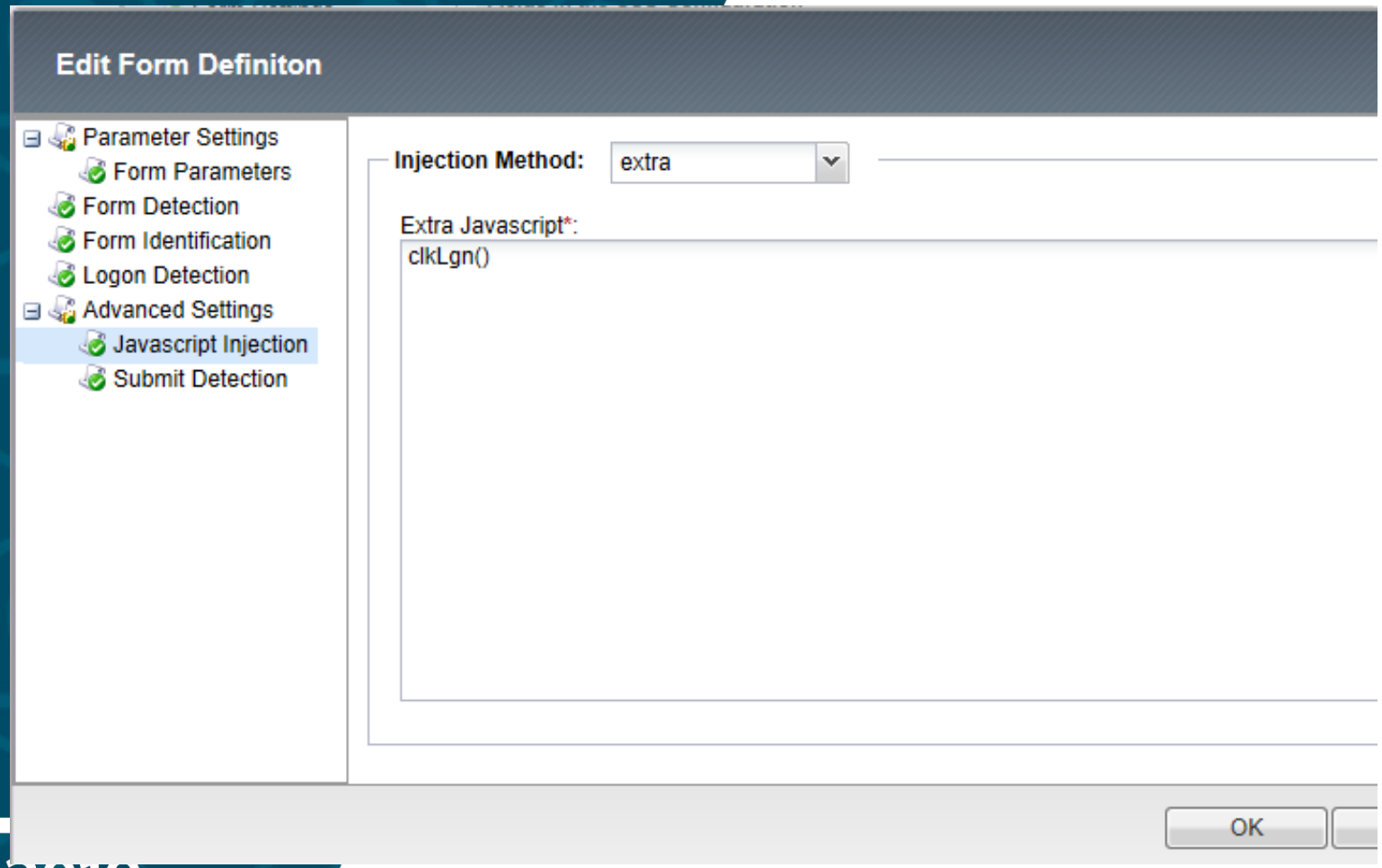
Implementing Office 365 and MS Exchange 2013 user access with BIGIP Access Policy Manager

O365_sso configuration continue.



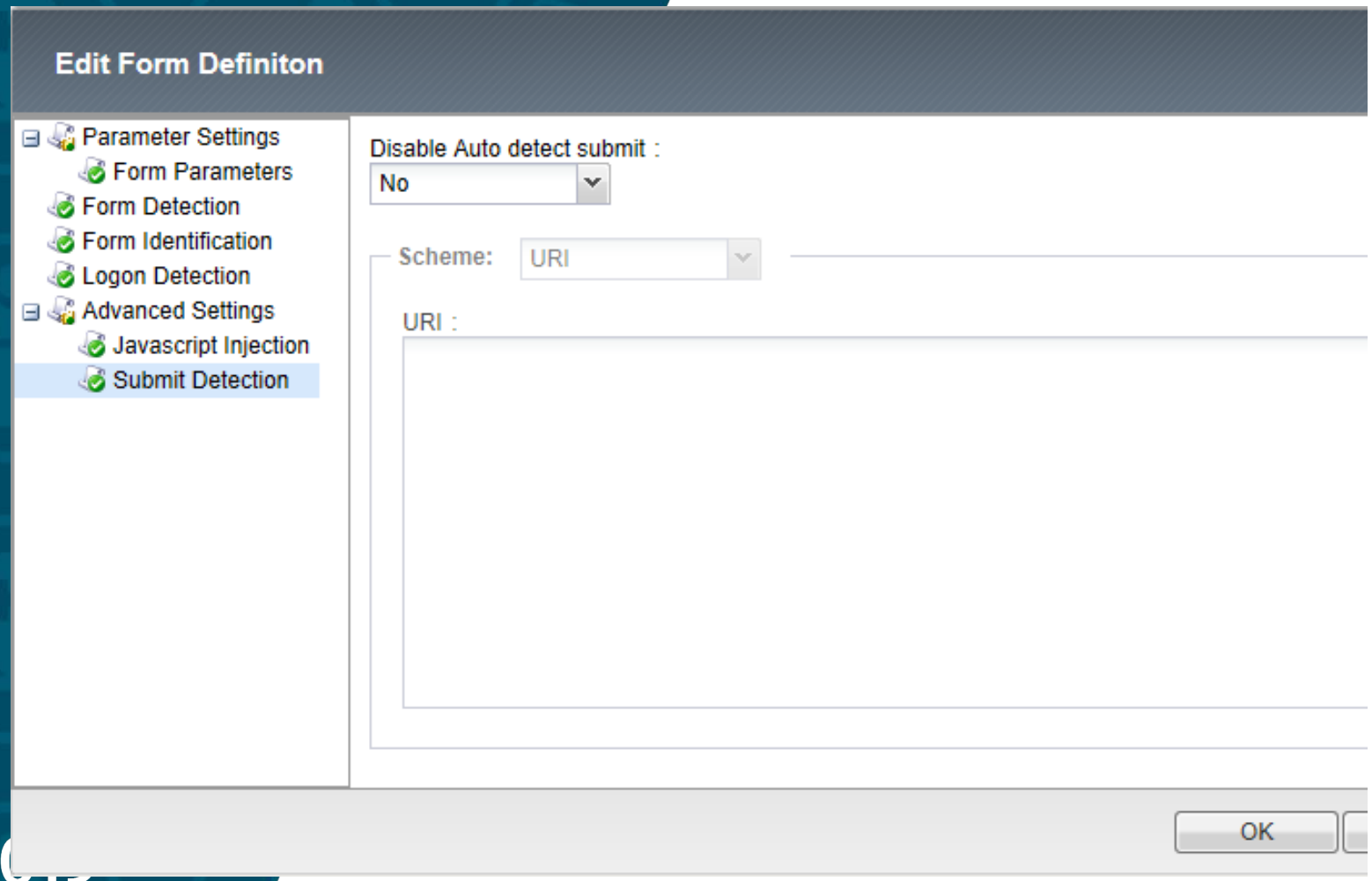
Implementing Office 365 and MS Exchange 2013 user access with BIGIP Access Policy Manager

O365_sso configuration continue.



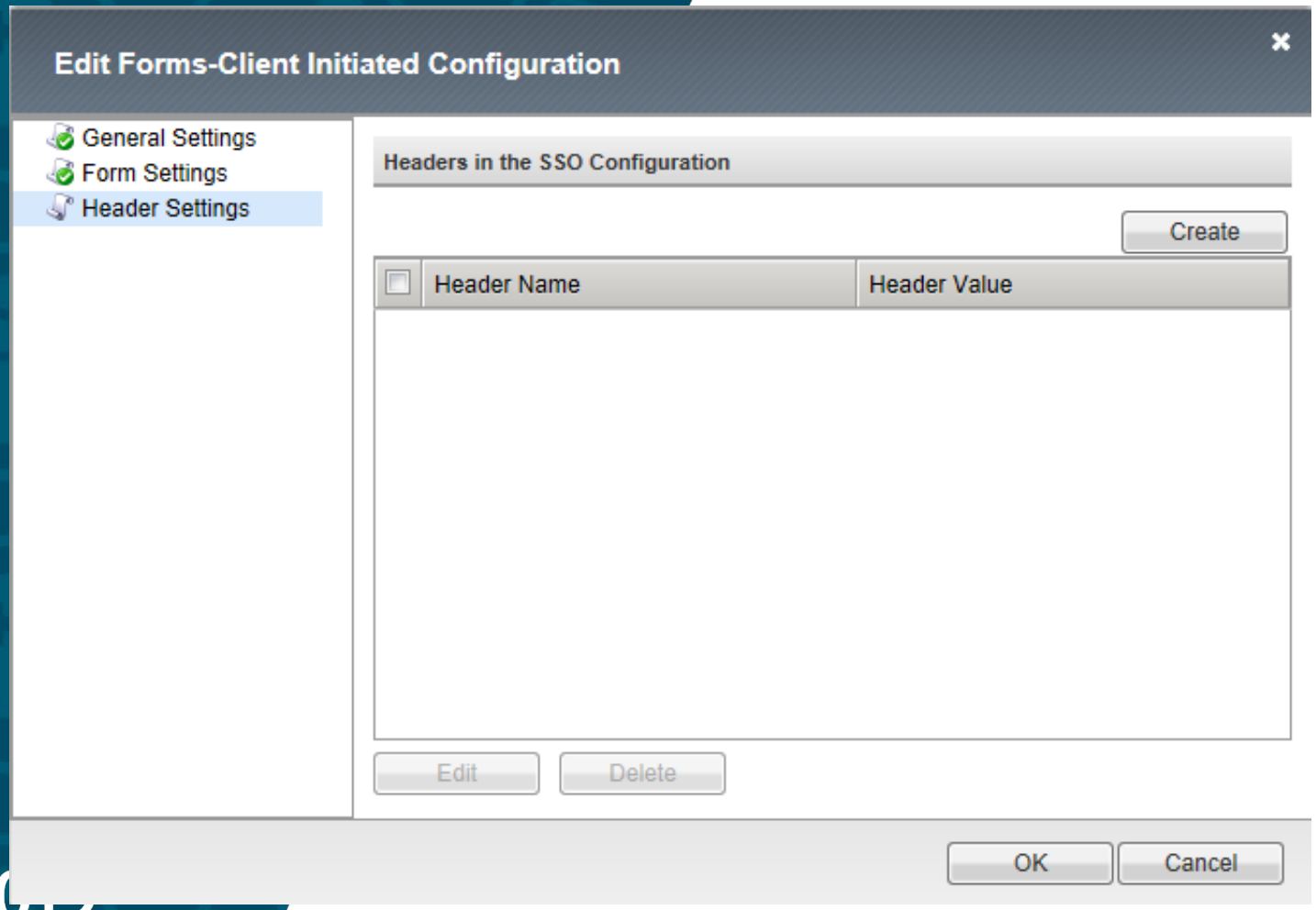
Implementing Office 365 and MS Exchange 2013 user access with BIGIP Access Policy Manager

O365_sso configuration continue.



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

O365_sso configuration continue.



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. MSExchangeCAS2013prod_owa_https_monitor was used to monitor the pool. The pool has two members, exfe1.prd.capilanou.ca (204.239.151.64) and exfe2.prd.capilanou.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 belowr. /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]
…
```

BCNET 2019

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****"
  }
}
…
```

BCNET 2019

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"

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