|  |
| --- |
| CA Technologies |
| **Setting up OAuth to Authenticate against LDAP** |
| Implementation guide |

|  |
| --- |
| Christopher Waun9/18/2015 |

Copyright © 2015 CA

All rights reserved. All trademarks, trade names, service marks and logos referenced herein belong to their respective companies. No unauthorized use, copying or distribution permitted.

This document is for your informational purposes only. To the extent permitted by applicable law, CA provides this document “AS IS” without warranty of any kind, including, without limitation, any implied warranties of merchantability or fitness for a particular purpose, or non-infringement. In no event will CA be liable for any loss or damage, direct or indirect, from the use of this document including, without limitation, lost profits, business interruption, goodwill or lost data, even if CA is expressly advised of such damages.

Change History

| Date | Version | Author | Description of Change |
| --- | --- | --- | --- |
| 09/18/2015 | 0.1 | Chris Waun | Document Creation |
|  |  |  |  |
|  |  |  |  |

Table of Contents

[Document Purpose 3](#_Toc430354277)

[Assumptions 3](#_Toc430354278)

[1 Solution Requirement 3](#_Toc430354279)

[2 Changing OAuth Manager Set Valid User Fragment 3](#_Toc430354280)

[3 Changing the OTK User Authentication 4](#_Toc430354281)

[4 Changing Encapsulated Assertions Inputs. 5](#_Toc430354282)

[5 Changing OTK Client DB GET 7](#_Toc430354283)

# Document Purpose

To assist in changing the OAuth structure to use the LDAP when authenticating.

# Assumptions

This document is written based on the understanding that the reader has a good working knowledge of the CA Gateway, Policy Manager, and Policy Development. Also that the LDAP is configured and the user has basic knowledge on how to query the LDAP.

# Solution Requirement

1. User needs access to all the OAuth Policies.

# Changing OAuth Manager Set Valid User Fragment

1. There is a Fragment called IsAdmin Fragment.xml, this fragment contains all the logic to see if a user from the LDAP is contained in the Administrators group. If the User part of the admin group he/she will set the admin flag to true which will be used later in the OAuth flow.
	1. First open the oauth manager set valid user fragment in the policy manager and click show line numbers at the top.
	2. Disable the At Least one folder at line 15
	3. Add an Include Policy fragment folder, using the IsAdmin Fragment.
	4. Add an Export Variables from Fragment at the end of the policy and ensure the isAdmin variable is exported from the fragment

Before:



After:



Optional: turn the isAdmin fragment into an encapsulated assertion, but be sure to export the isAdmin variable.

This is the final change that needs to be made to this fragment.

# Changing the OTK User Authentication

1. There is a small change that needs to be made to this fragment to ensure that this is able to authenticate against the LDAP, and not the Internal Identify Provider.
	1. On line 20 directly under the Request: Require XPath Credentials assertion add an At Least One Folder
	2. Inside of the At Least One folder add two (2) All Assertions Must Evaluate True.
	3. Inside of the first All folder drag the Authenticate against Internal Identity Provider assertion that was already in policy.
	4. Inside of the second folder drag a new Authenticate against Identity Provider that is in the assertions pallet. Choose to authenticate against the LDAP that is configured on the Gateway.

Before:



After:



# Changing Encapsulated Assertions Inputs.

1. There are two encapsulated assertions that will now need to pass the value of isAdmin though in order to get the correct information.
	1. First the OTK Client GET needs to be changed.
	2. Find the policy in the policy pallet (bottom left in policy manager)
	3. Right click on the OTK Client Get Policy and click on the Encapsulated Assertion Properties.



* 1. The Encapsulated Assertion Configuration properties appears



* 1. To the left of the inputs panel click add and the argument properties box will appear 

Fill out the box as shown and click Ok on both boxes

* 1. Do steps A-E to the fragment OTK Client DB GET

# Changing OTK Client DB GET

1. This will more of a challenge as there is no easy way to simplify this to a fragment. This is to list everything on the OAuth clients when the user that logs in is an admin.
	1. Navigate and open OTK Client DB GET if not already open.
	2. Expand all folders.
	3. Navigate down to line 193.
	4. Replace lines 193 to 201 with the below code

Before:



After:



* 1. After this last edit there should be a list of all clients that are registered when an administrator logs in.