Single Sign-on to Google Apps with CA Federation Manager

TOM GODFREY SOFTWARE ENGINEERING MANAGER, CA

NOTICES

This publication is based on current information and resource allocations as of its date of publication and is subject to change or withdrawal by CA at any time without notice. The information in this publication could include typographical errors or technical inaccuracies. CA may make modifications to any CA product, software program, method or procedure described in this publication at any time without notice.

Any reference in this publication to non-CA products and non-CA websites are provided for convenience only and shall not serve as CA's endorsement of such products or websites. Your use of such products, websites, any information regarding such products or any materials provided with such products or at such websites shall be at your own risk.

Notwithstanding anything in this publication to the contrary, this publication shall not (i) constitute product documentation or specifications under any existing or future written license agreement or services agreement relating to any CA software product, or be subject to any warranty set forth in any such written agreement; (ii) serve to affect the rights and/or obligations of CA or its licensees under any existing or future written license agreement or services agreement relating to any CA software product; or (iii) serve to amend any product documentation or specifications for any CA software product. The development, release and timing of any features or functionality described in this publication remain at CA's sole discretion.

The information in this publication is based upon CA's experiences with the referenced software products in a variety of development and customer environments. Past performance of the software products in such development and customer environments is not indicative of the future performance of such software products in identical, similar or different environments. CA does not warrant that the software products will operate as specifically set forth in this publication. CA will support only the referenced products in accordance with (i) the documentation and specifications provided with the referenced product, and (ii) CA's then-current maintenance and support policy for the referenced product.

Certain information in this publication may outline CA's general product direction. All information in this publication is for your informational purposes only and may not be incorporated into any contract. CA assumes no responsibility for the accuracy or

completeness of the information. 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, 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, lost investment, business interruption, goodwill or lost data, even if CA is expressly advised of the possibility of such damages.

Single Sign-on to Google Apps with CA Federation Manager

Summary

This document shows the steps to configure CA Federation Manager for your organization to allow your authorized users to single sign-on to Google Docs, Calendar and Mail.

GMail
Google Calendar
Google Docs

Identity Federation for Single Sign-on

Application developers and IT security people are becoming increasingly aware of the value of using standards-based identity federation to achieve single-sign on to SaaS applications, such as Google Apps. This document gives standards-based SAML 2.0 examples of how CA Federation Manager is configured to allow an organization's authorized users to single sign-on to the Google Apps, specifically Docs, Calendar and Mail.

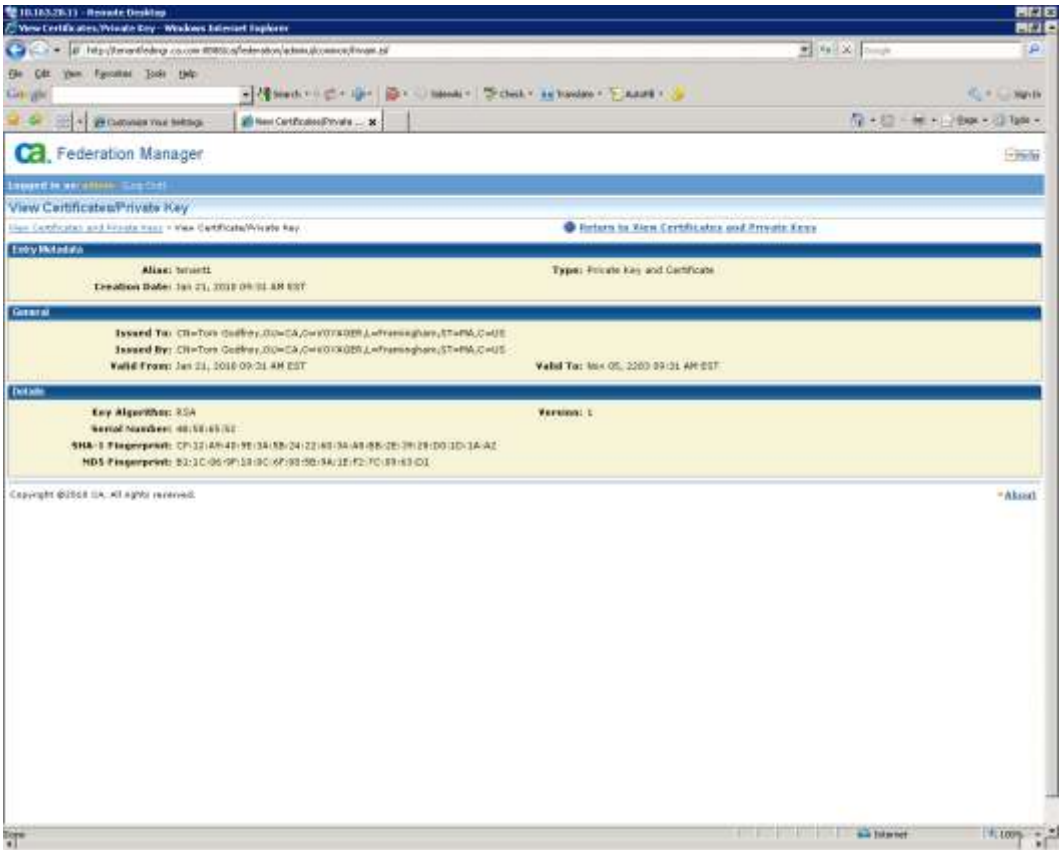
Federated Single Sign-on offers significant benefits, including:

- **Cost Reduction -** IT organizations are looking to control IT costs and gain efficiencies. Federated Single Sign-on targets areas that traditionally require lots of manual processes, including user account management, entitlements management, password management, and access management are a focus of these cost control efforts.
- **Easier Regulatory Compliance** - Expanding regulatory requirements and the increasing rate of compromise of personal information via various types of security breaches have led organizations to place a greater emphasis on data security, and the people, process, and technology that make it up. Standards-based identity federation can increase security enabling an organization to identify and authenticate a user once, and then use that identity information across multiple systems, including external partner websites.

CA Federation Manager Federation

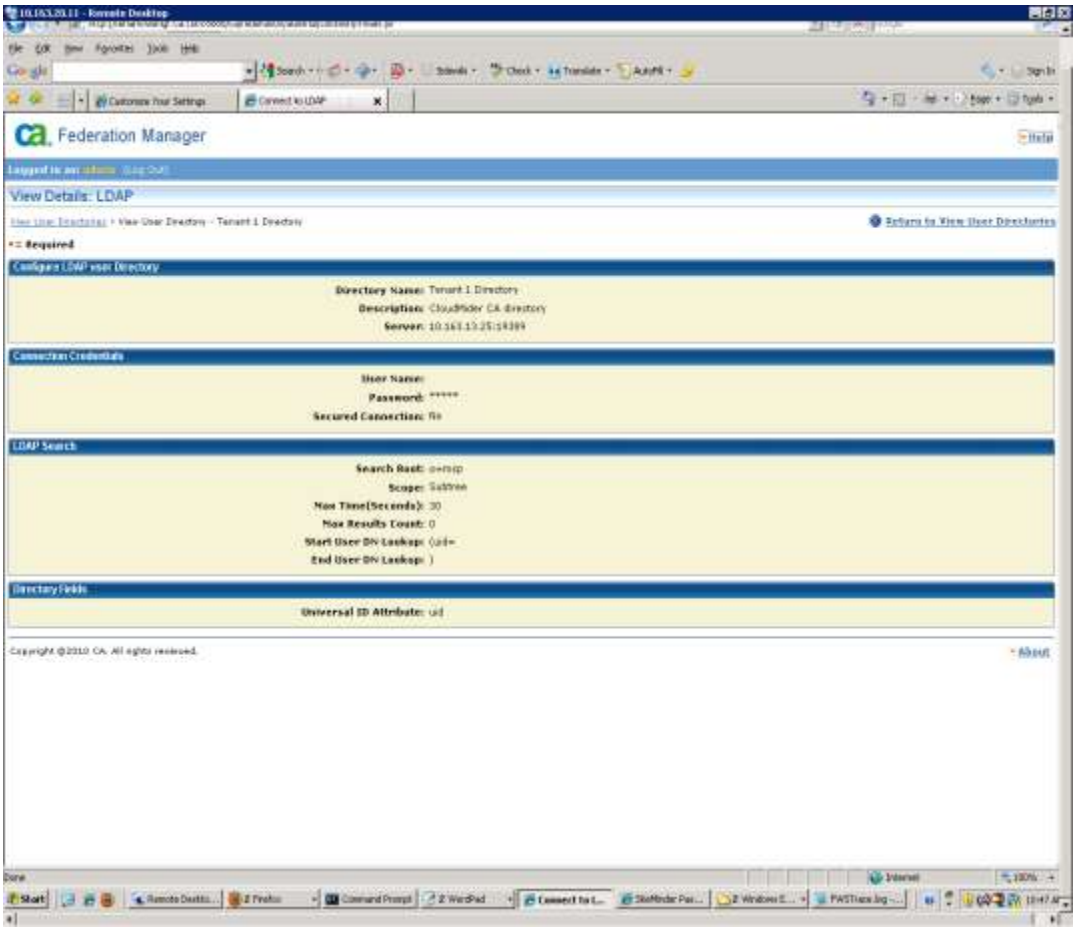
Single Sign-On Settings for Google Apps

Create a Certificate for Identity Provider (IDP) side of the federation. In this example the certificate name is tenant1. You will need to import this certificate into Google and use it on the entities and partnerships you create in Federation Manager.

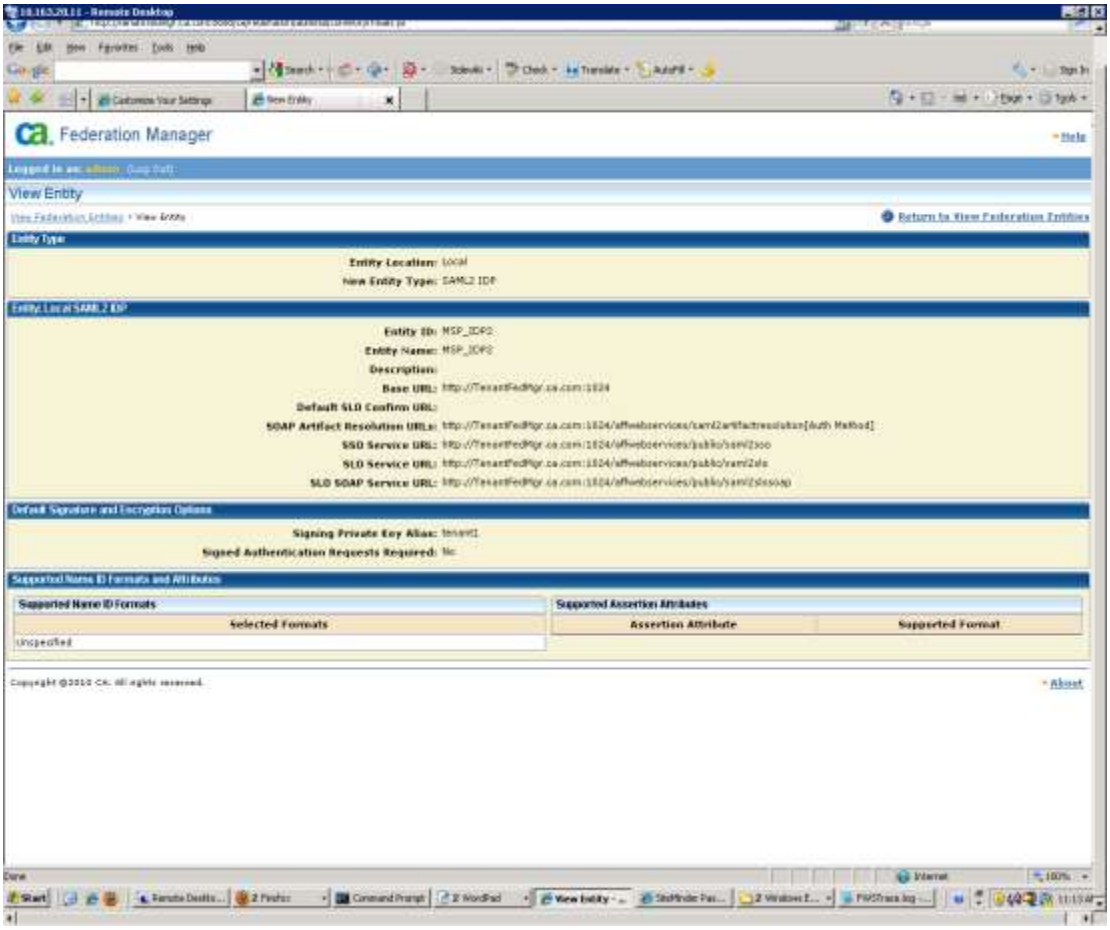


Export the certificate as x590 certificate.

Create User Directory; in this example the directory name is Tenant1 directory.

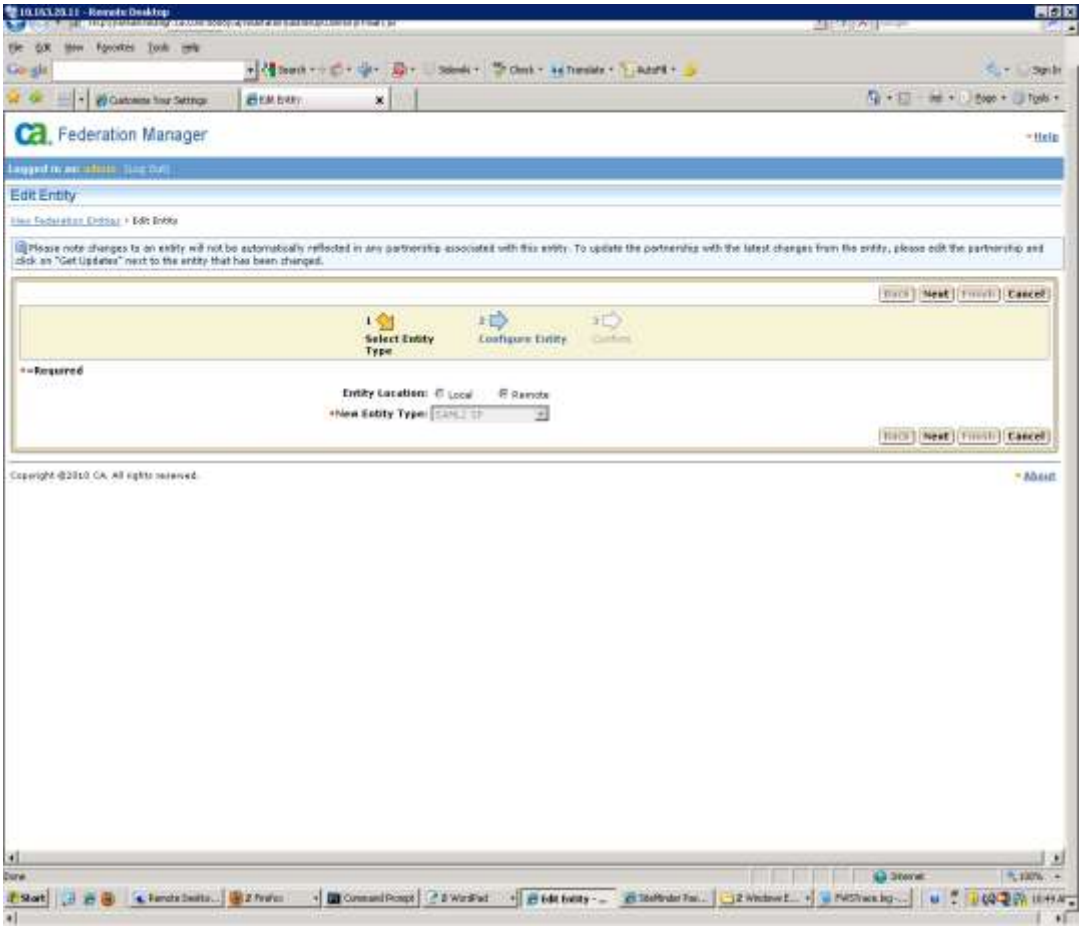

Federation Manager
View Details: LDAP
Configure LDAP user Directory
Directory Name: Tenant 1 Directory
Description: CloudRider CA directory
Server: 10.163.13.25:19389
Connection Credentials
User Name:
Password: *****
Secured Connection: No
LDAP Search
Search Root: o=ntp
Scope: Subtree
Max Time(Seconds): 30
Max Results Count: 0
Start User DN Lookup: (uid=
End User DN Lookup:)
Directory Fields
Universal ID Attribute: uid
Copyright ©2010 CA. All rights reserved.
About

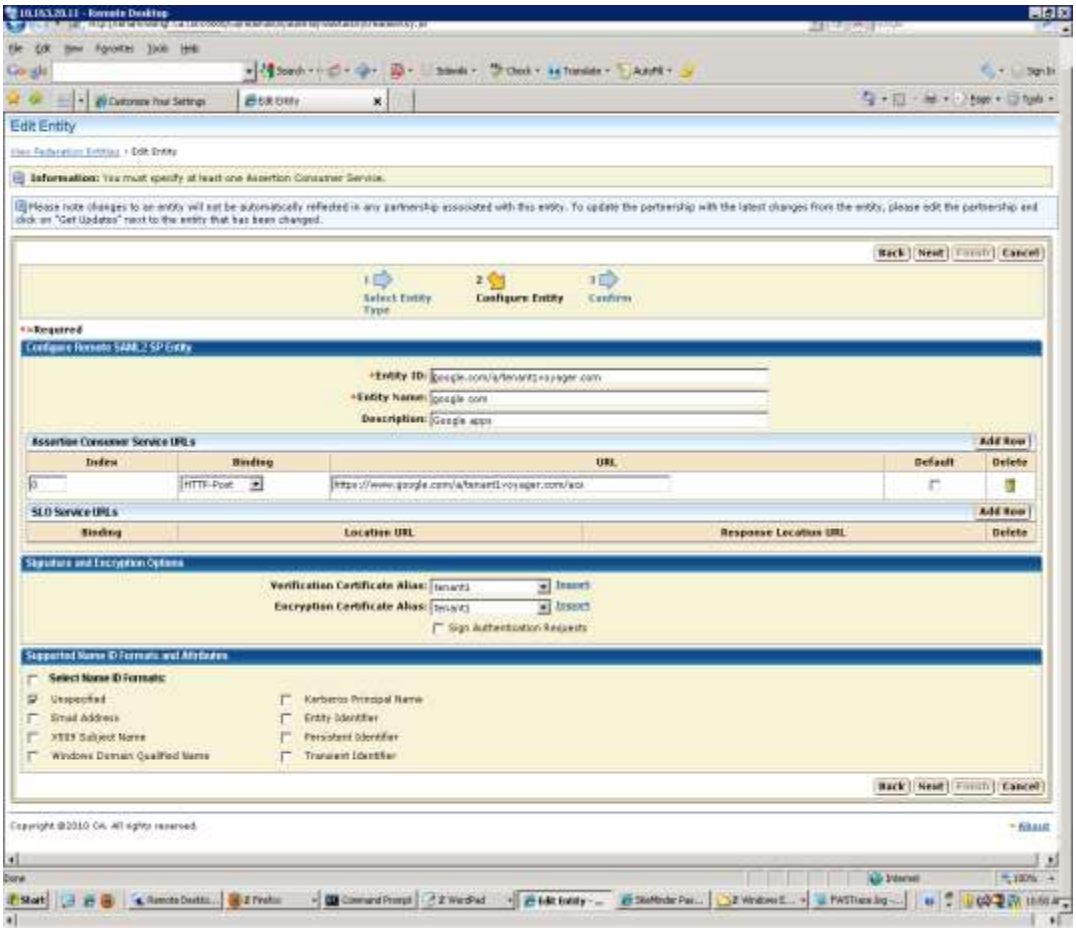
Create IdP: in this example the MSP_IDP2. Type=Local and SAML 2 IDP. Note the SSO and SLO URL's. You will need to configure these on Google.



Use the certificate created.

Create SP – Type=Remote and SAML2



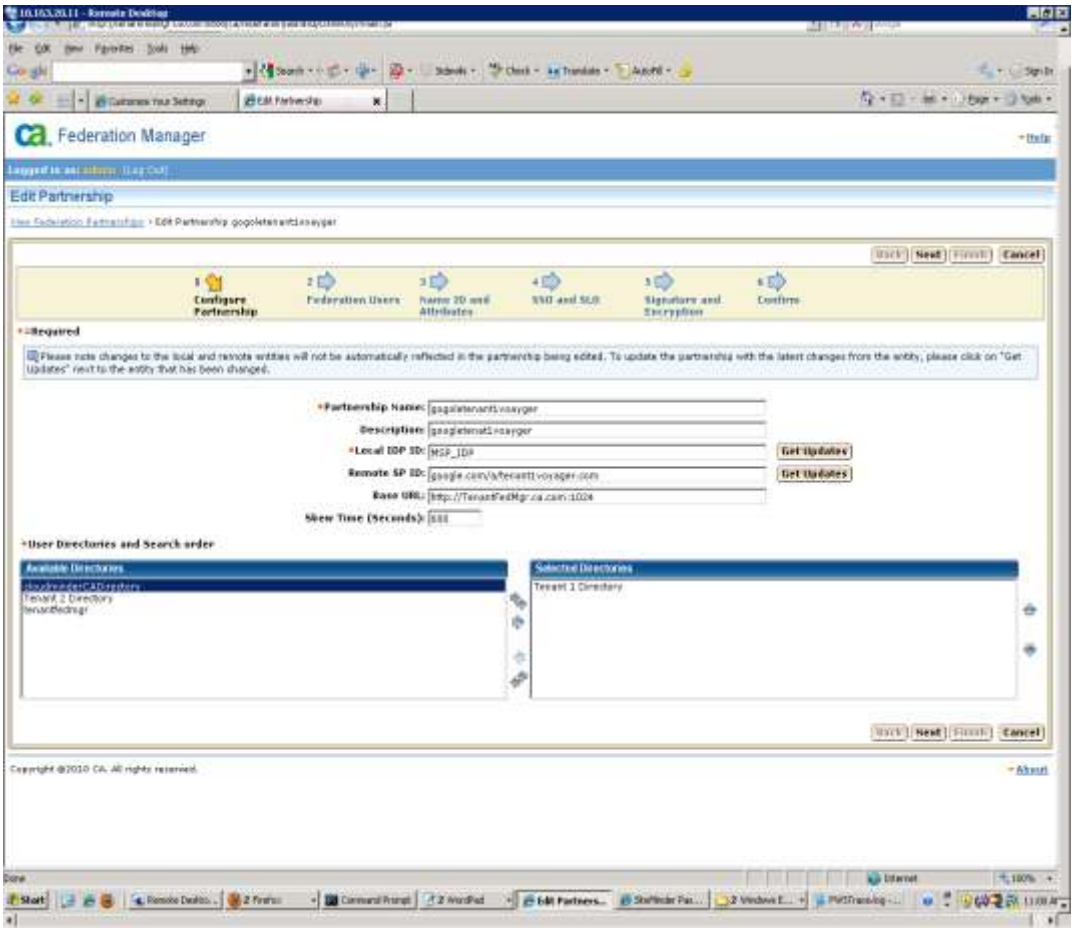


Entity Id must be google.com/<domain>. I

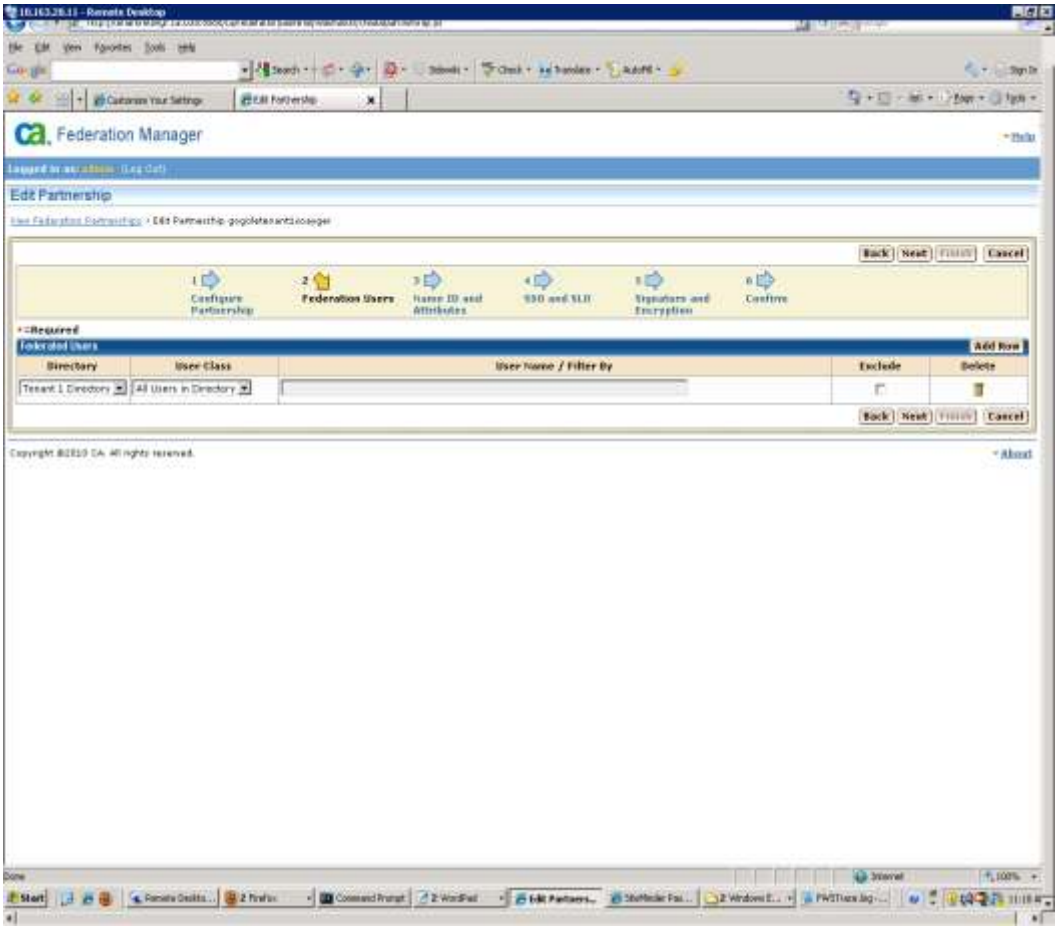
n this example the domain is tenant1voyager.com.
ACS is https://www.google.com/a/<domain>/acs in this example it's https://www.google.com/a/tenant1voyager.com/acs - use http post.

Use the certificate you created.

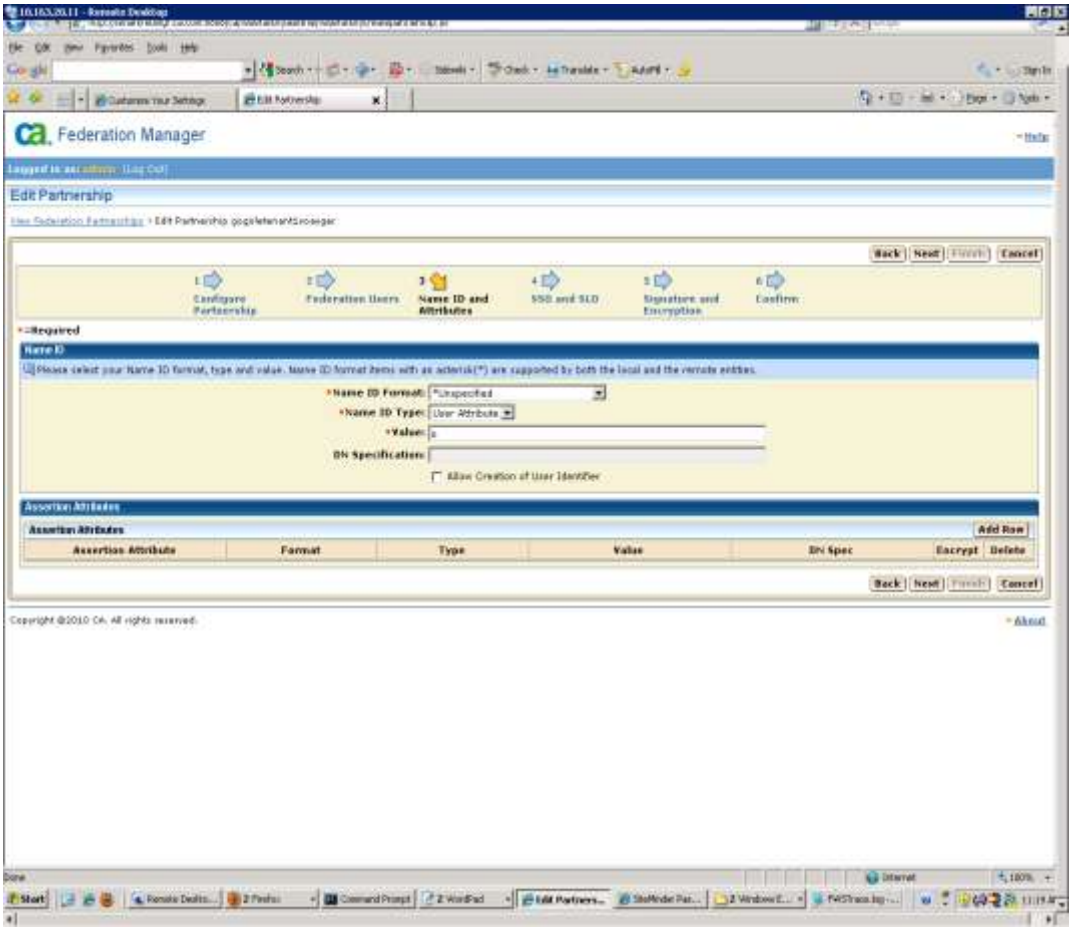
Create Partnership - in this example the partnership is gogoletenant1voayger. Select the IDP (MSP_IDP2) and SP (google.com/a/tenant1voyager.com)created above. Add you user directory from above (Tenant 1 directory)



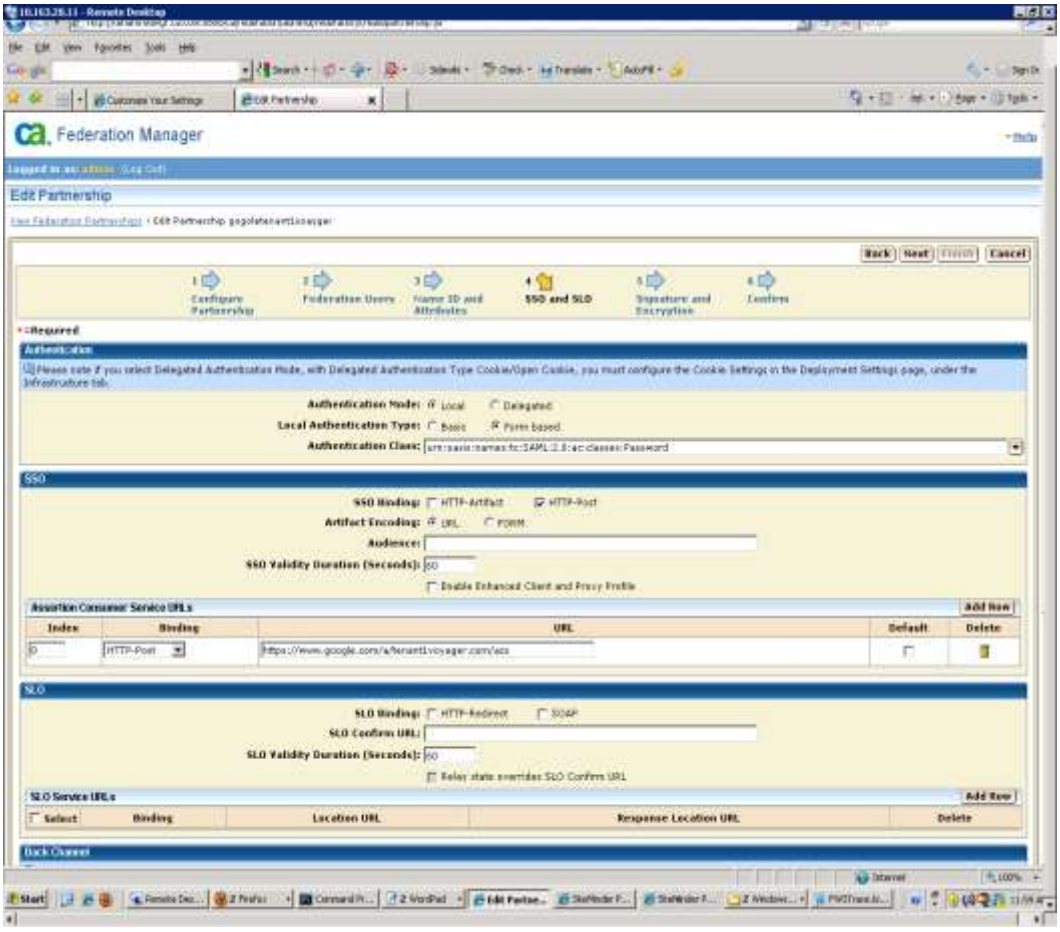
You do not need to do anything on the user screen.



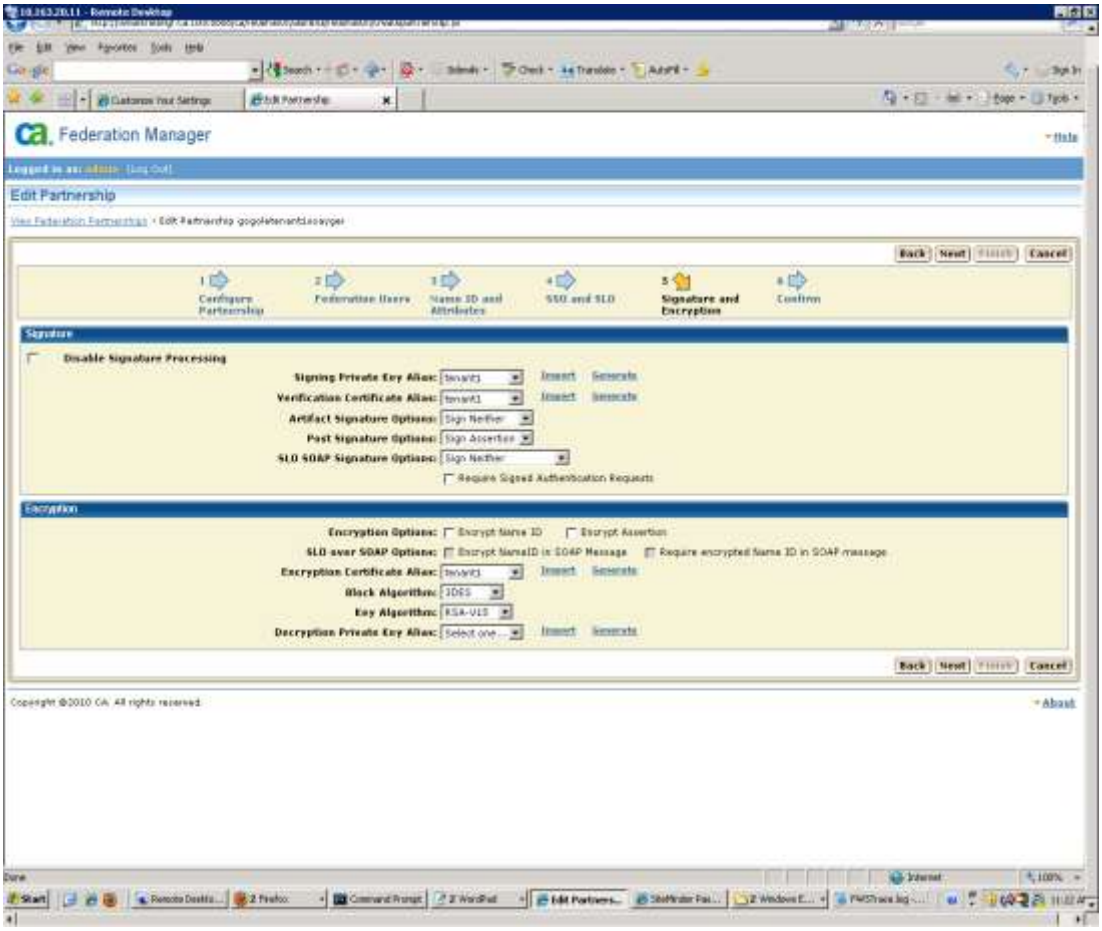
Map the user attribute from the directory which contains the Google id. In this case the attribute is o.



Leave the audience blank and use the same ACS from the SP configuration. ACS is https://www.google.com/a/<domain>/acs in this example it's https://www.google.com/a/tenant1voyager.com/acs



Use the same certificate as before. Tenant1



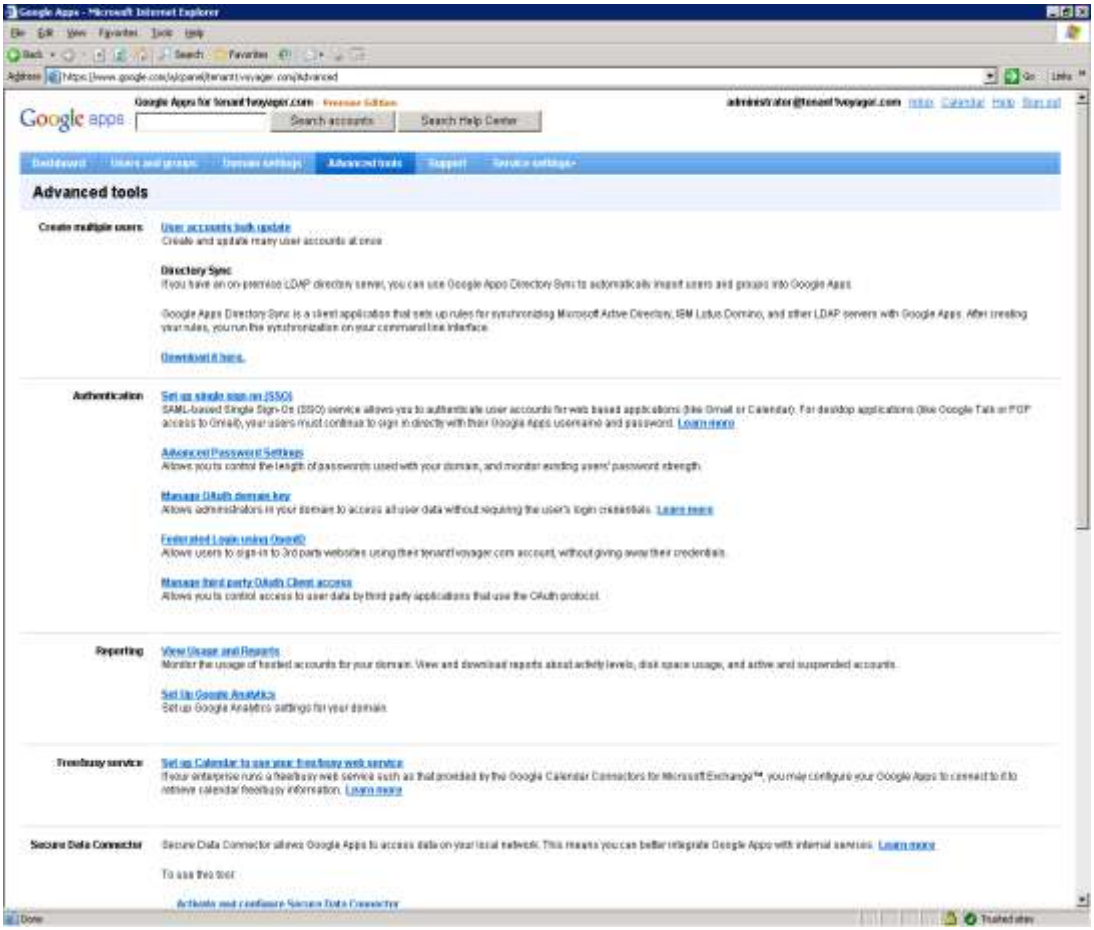
Finish, then activate the partnership

Now configure Google.

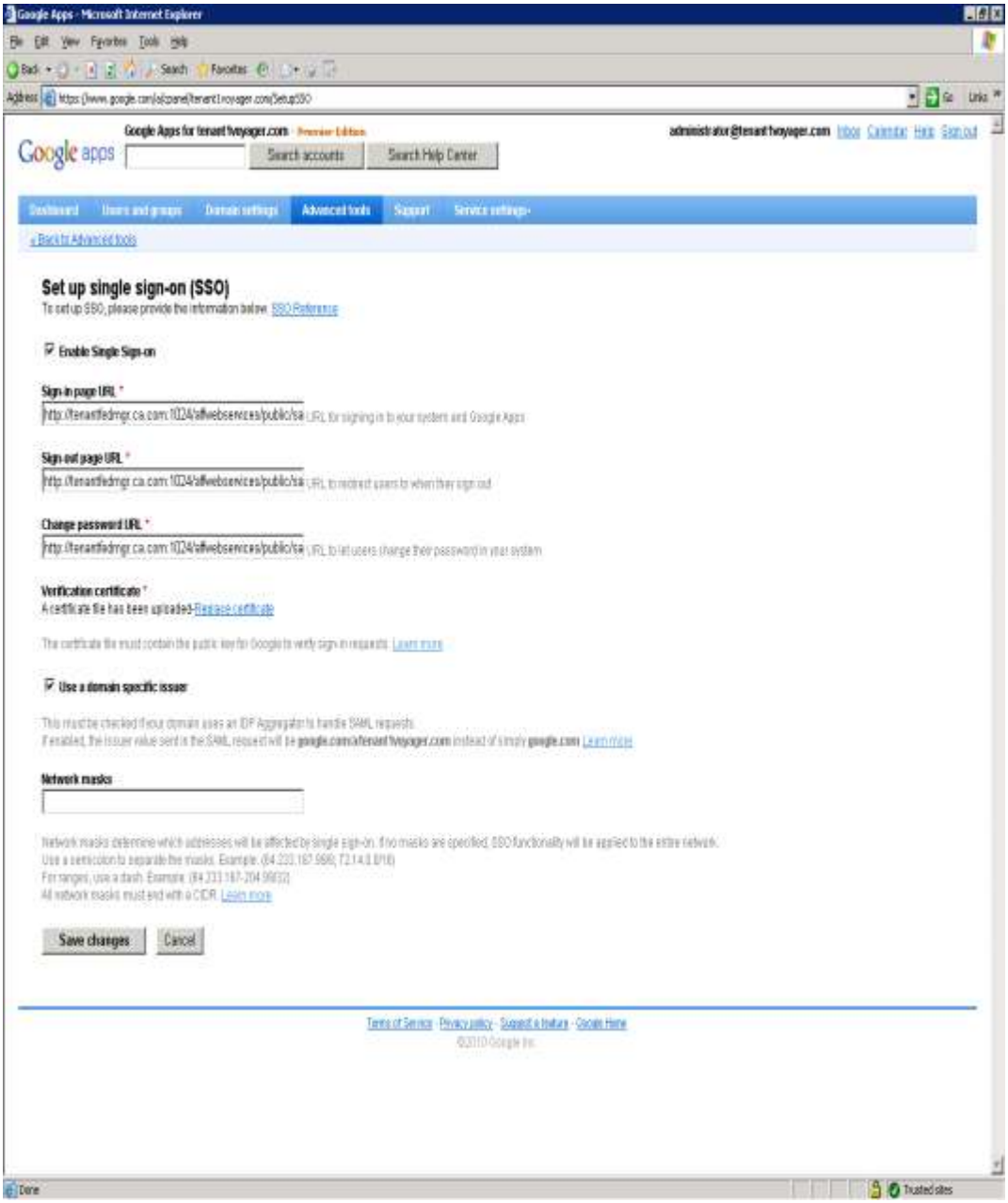
Sign on to Google with yourself as the administrator.
The URL is: https://www.google.com/a/cpanel/<domain>.com

In this example: https://www.google.com/a/cpanel/tenant1voyager.com

Go to <Advanced Tools>.



Select <Set up single sign-on (SSO)>



Check <Enable Single Sign-on>
Use the URL's form IDP
Check Use a domain specific user

Save your settings and test the federation.

Since Google Federation is SP initiated, you should use links like these below to test.

- mail.<domain>.com
- docs.<domain>.com

In this example, we used:

- mail.tenant1voyager.com
- docs.tenant1voyager.com