

Government of Canada Credential Federation IDP Simulator Installation Guide

**Identity, Authentication & Authorization Services
Shared Services Canada**

**Version 1.4
EDRM# 1483763**



Shared Services
Canada

Services partagés
Canada

Canada

Revision History

Date	Version	Description
Nov 30, 2011	1.0	First version
May 10, 2012	1.1	Updates for new simulator version
May 24, 2012	1.2	Added Load testing tips
April 19, 2013	1.3	Added Instructions for enabling SHA-256
July 5, 2017	1.4	Added instructions to disable dynamic IPs for the virtual box setting



Table of Contents

1.	Introduction	4
1.1	Purpose	4
1.2	Audience	4
1.3	References	4
2.	The IDP Simulator	5
2.1	Virtual Hardware Requirements	5
2.2	Networking Requirements	5
2.3	Installation	5
2.4	Configuring a Service Provider	15
2.5	Creating Additional Test Users	24
2.6	Enabling Signature Algorithm (SHA-256)	30
3.	Load and Performance Testing Tips	34
4.	Other Testing Tools	34



1. Introduction

1.1 Purpose

Shared Services Canada maintains and provides an Identity Provider Simulator that GC Departments and Agencies can use to develop and test their SAML implementations. The purpose of this document is to provide information to assist departments and agencies with installing and using the IDP Simulator.

1.2 Audience

This document is primarily targeted toward system administrators and testers who are responsible for managing development and testing environments.

1.3 References

[CATS]	Cyber Authentication Interface Architecture and Specification Version 2.0: Deployment Requirements
--------	---

2. The IDP Simulator

Shared Services Canada maintains and provides an Identity Provider Simulator that GC Departments and Agencies can use to develop and test their SAML implementations. The IDP Simulator is a virtual machine appliance that has been packaged using the Open Virtualization Format (OVF) and can be deployed on popular virtualization platforms including VMWare Player and Oracle VirtualBox.

The IDP Simulator virtual machine comes with the Open Source ForgeRock Open AM SAML product pre-installed on Apache Tomcat and Linux. The first time the virtual machine is started an automated script is executed that quickly and easily configures the IDP simulator to work within the host network environment.

2.1 Virtual Hardware Requirements

The minimum virtual hardware requirements of the IDP simulator are quite modest:

- 1 Virtual CPU (32 bit)
- 1GB of virtual memory
- 6GB of virtual disk space
- 1 virtual network interface

Additional virtual hardware (for example a virtual CD-ROM drive) is also supported should you wish to install additional software or paravirtualized drivers. If you intend to use the IDP Simulator to support load testing of your RP application then 2GB of memory and additional CPUs are recommended.

2.2 Networking Requirements

The IDP simulator requires one static IP address in your environment. For best results the host name of the simulator should be registered with a Domain Name Service. The IDP simulator supports the IDP discovery profile and would normally have an additional separate DNS entry in a common domain for exchanging the IDP discovery common domain cookie. The host name and domain names of the simulator are fully configurable in order to work within the target network environment.

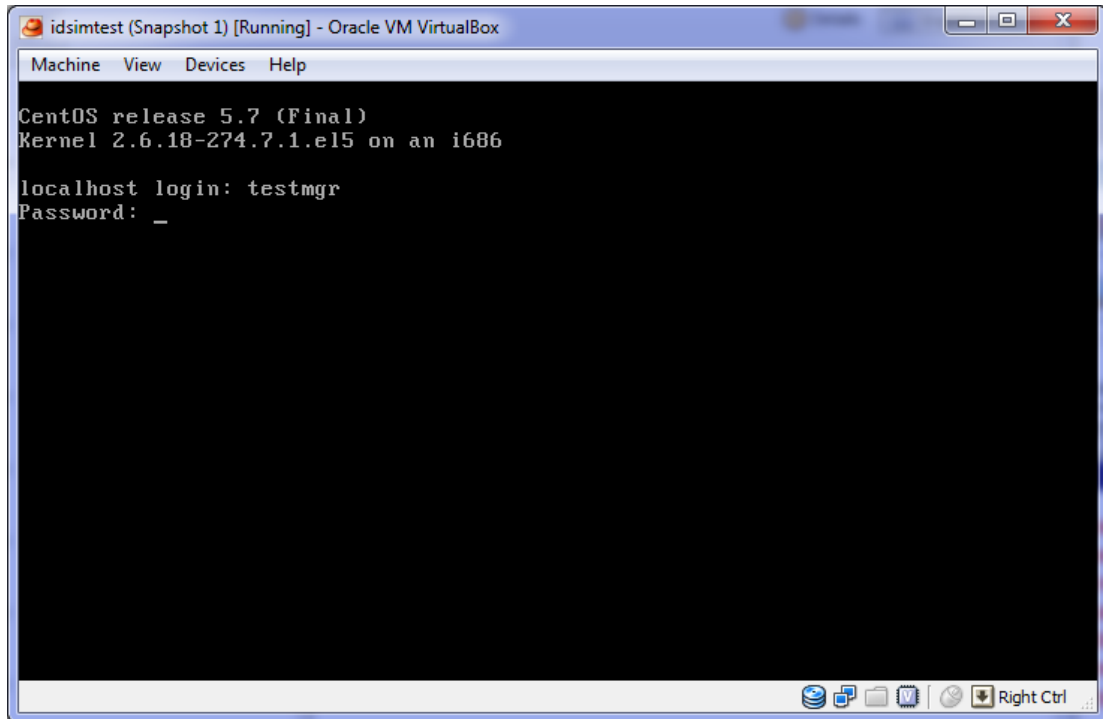
If a Domain Name Service is not available then the simulator also supports the use of host files for name resolution. Note that if host files are to be used then every server or client PC that accesses the IDP simulator must have an entry added to its host file. If an attempt is made to access the simulator by IP address or some other means then the secure nature of SAML and HTTPS will prevent it from functioning.

2.3 Installation

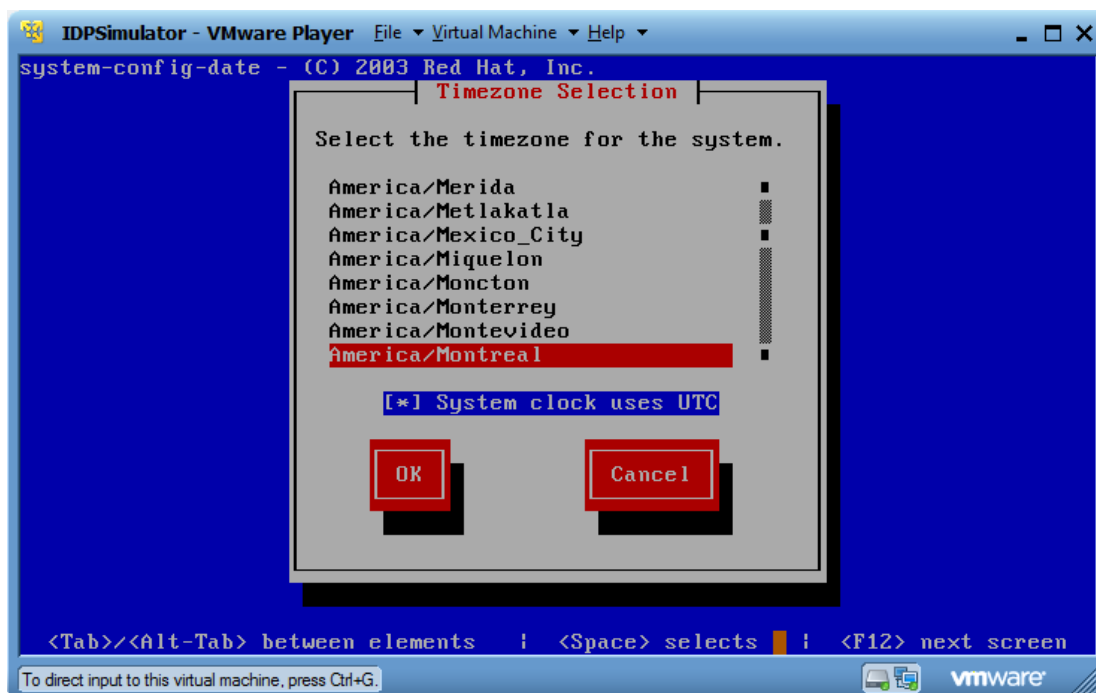
The generic process for installing and configuring the appliance is as follows:

1. Import the VM image into your virtualization product. (Consult your product documentation for details on how to do this)

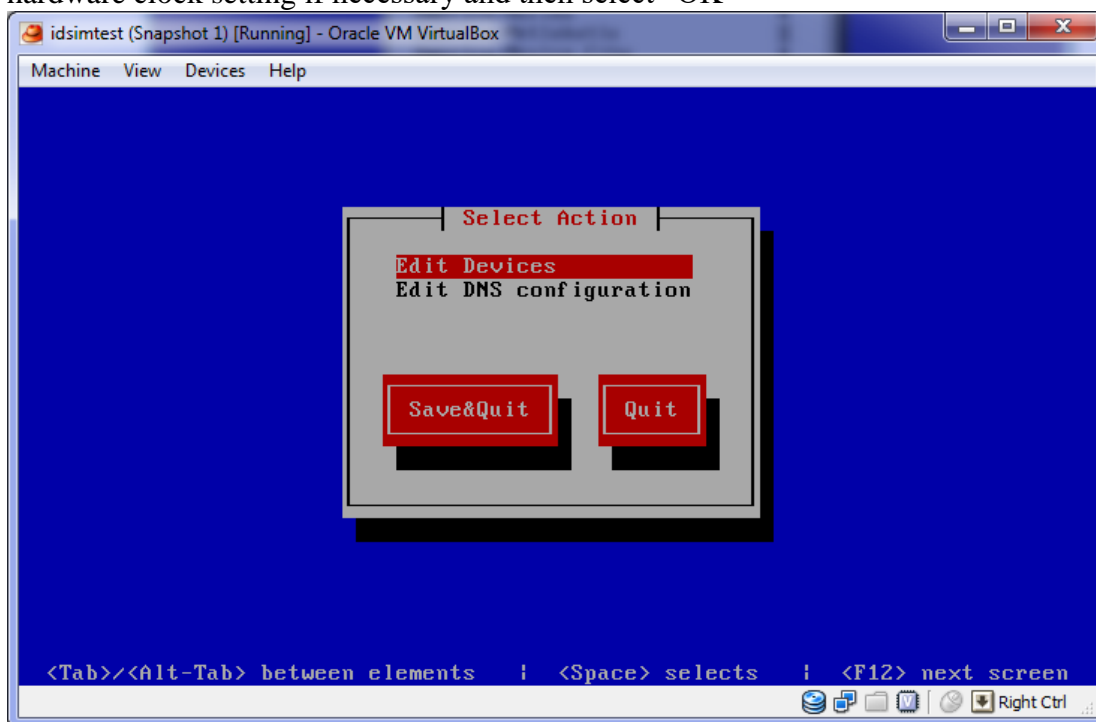
2. Please note: Do not use Dynamic IPs when configuring the virtual box; For instance, when setting up the virtual box network adapter for 'host only network', uncheck 'enable dhcp' Take down the IP
3. Configure the virtual network card for bridged or host only networking as required (most installations will use bridged networking)
4. Optionally configure a virtual CD-ROM drive if you wish to install any hypervisor specific guest tools (such as VMWare tools or VirtualBox guest additions)
5. Start the VM for the first time
6. Optionally log in to the VM as root (the password is "SAMLTest1"), install any hypervisor specific guest tools (such as VMWare tools or VirtualBox guest additions) and reboot the VM.



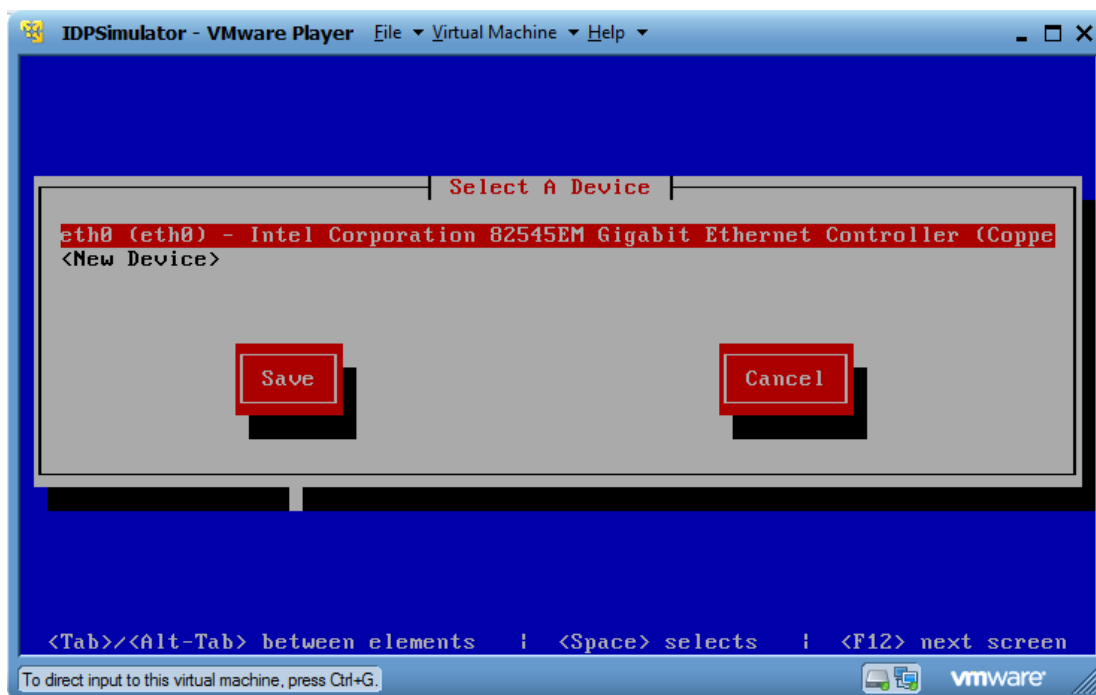
7. Once booting is complete, login as "testmgr". The password is "SAMLTest1".



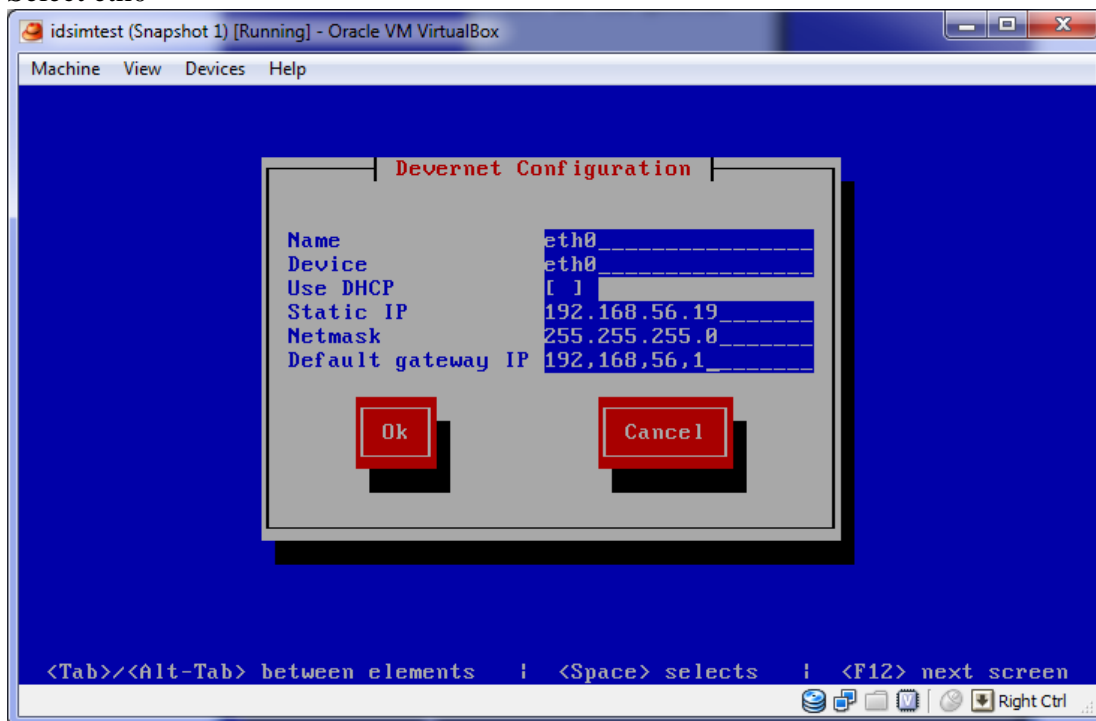
8. The Timezone configuration tool will automatically appear. Modify the timezone and hardware clock setting if necessary and then select "OK"



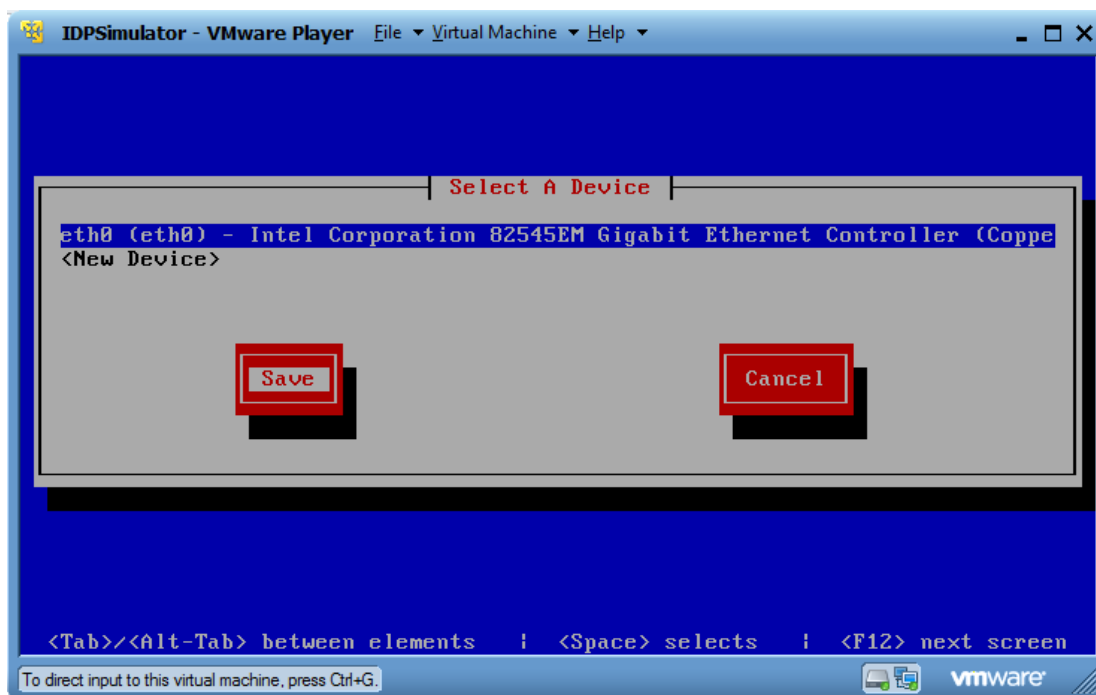
9. The Network configuration tool will automatically appear. Select "Edit Devices"



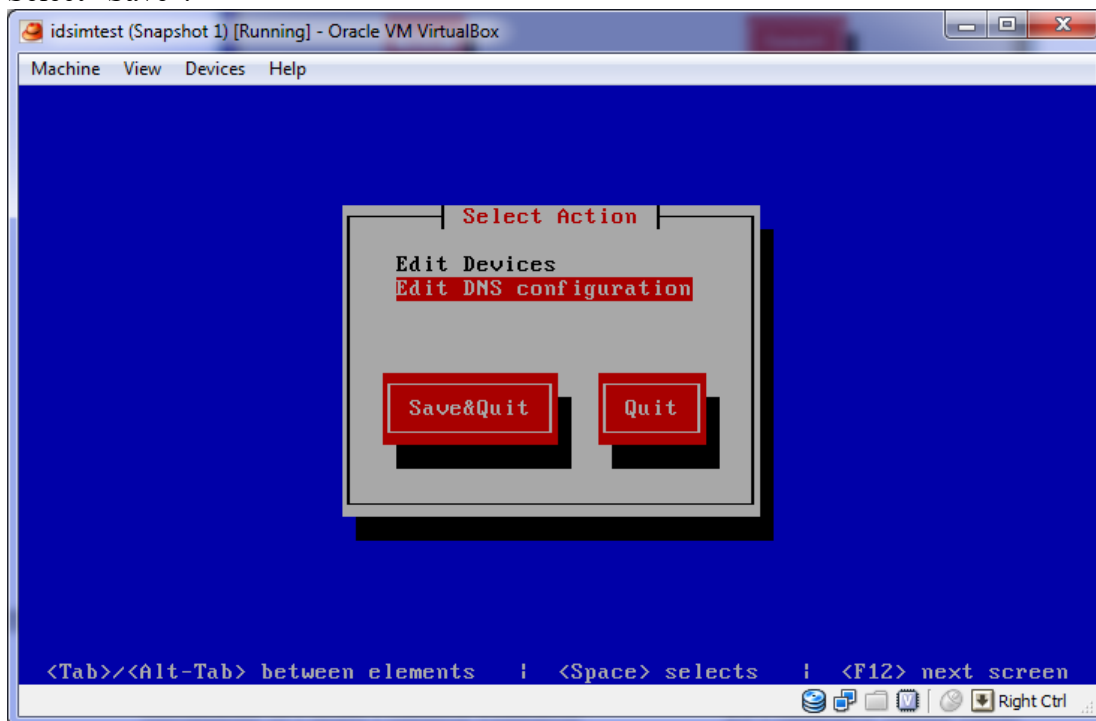
10. Select eth0



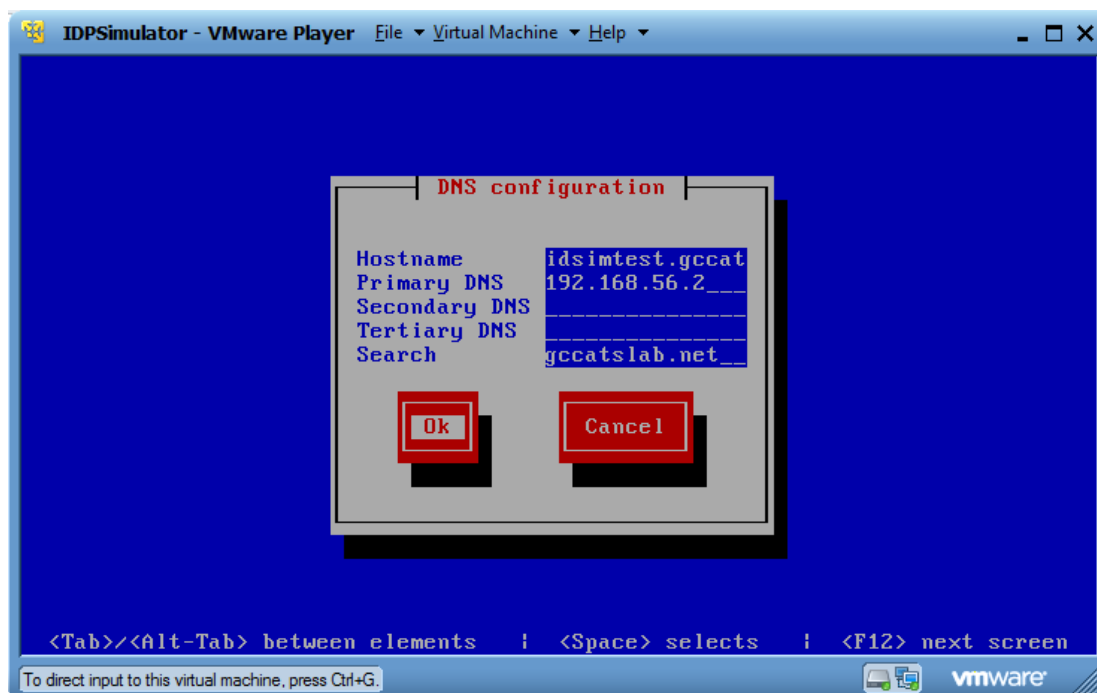
11. Configure the static IP address, netmask and default gateway for your network and select "OK".



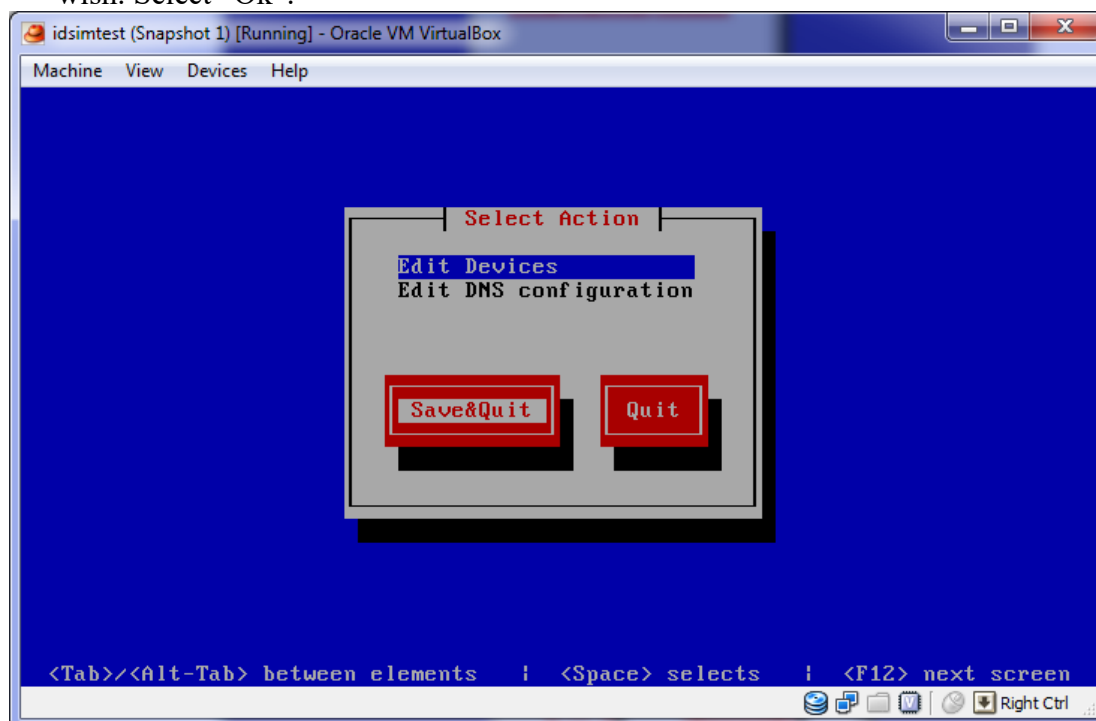
12. Select "Save".



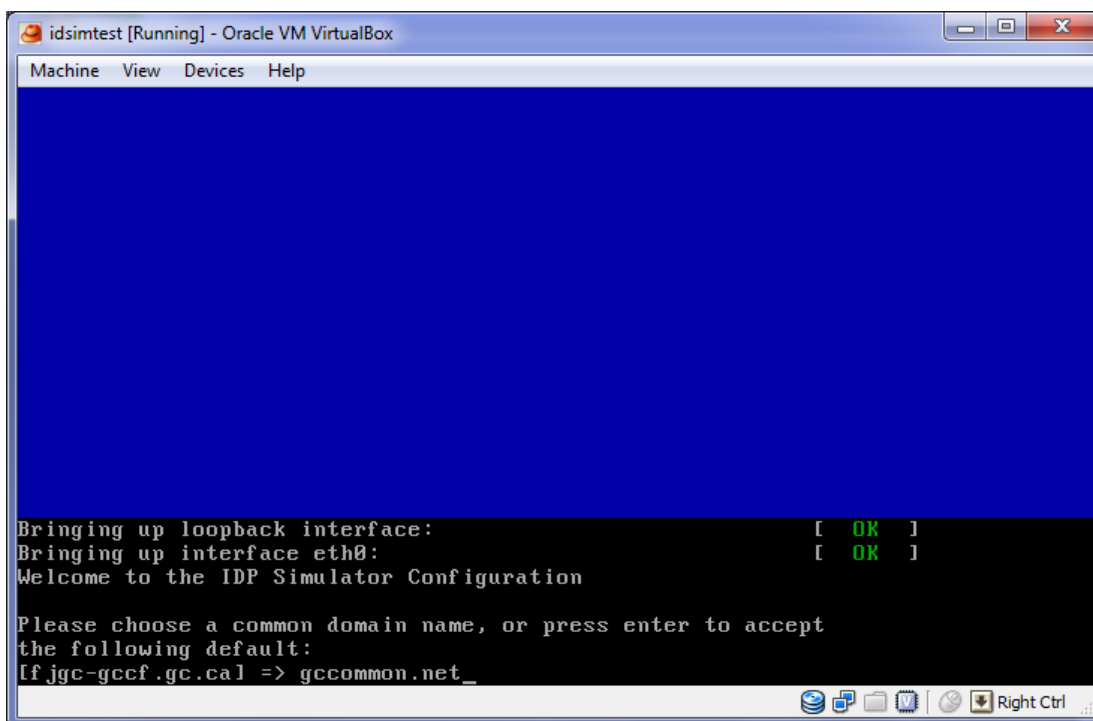
13. Select "Edit DNS Configuration".



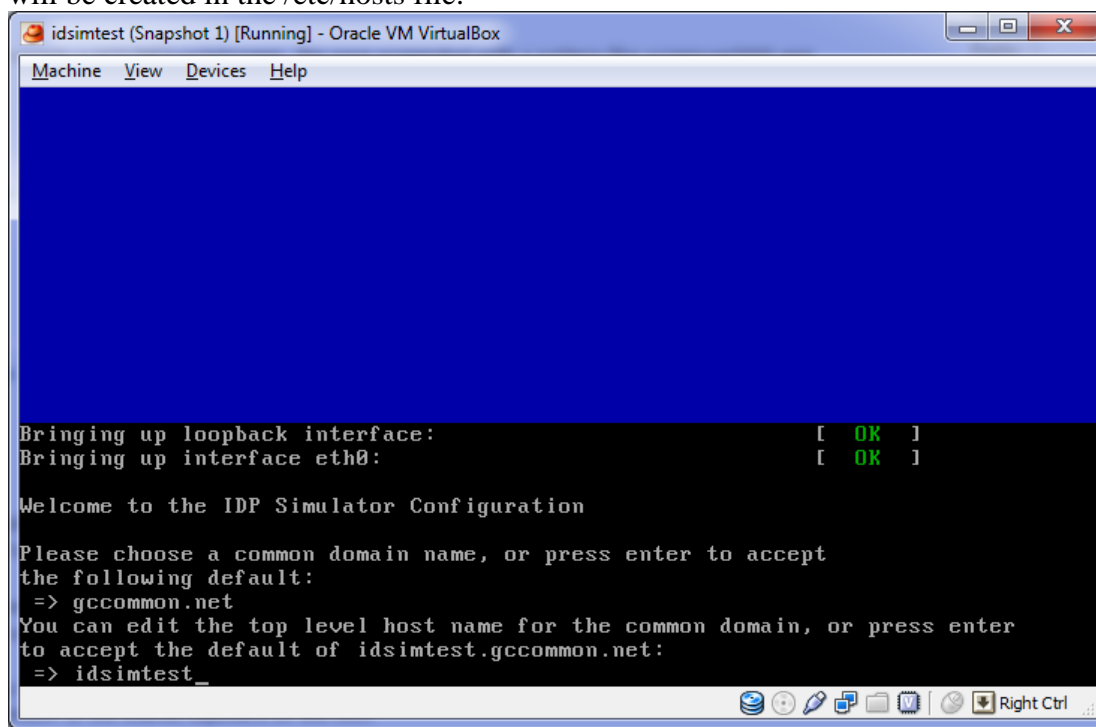
14. Enter a fully qualified host name (e.g. idsim.test.dept.gc.ca) for the IDP Simulator and the address(es) of your DNS servers. You may also specify a DNS search default if you wish. Select "Ok".



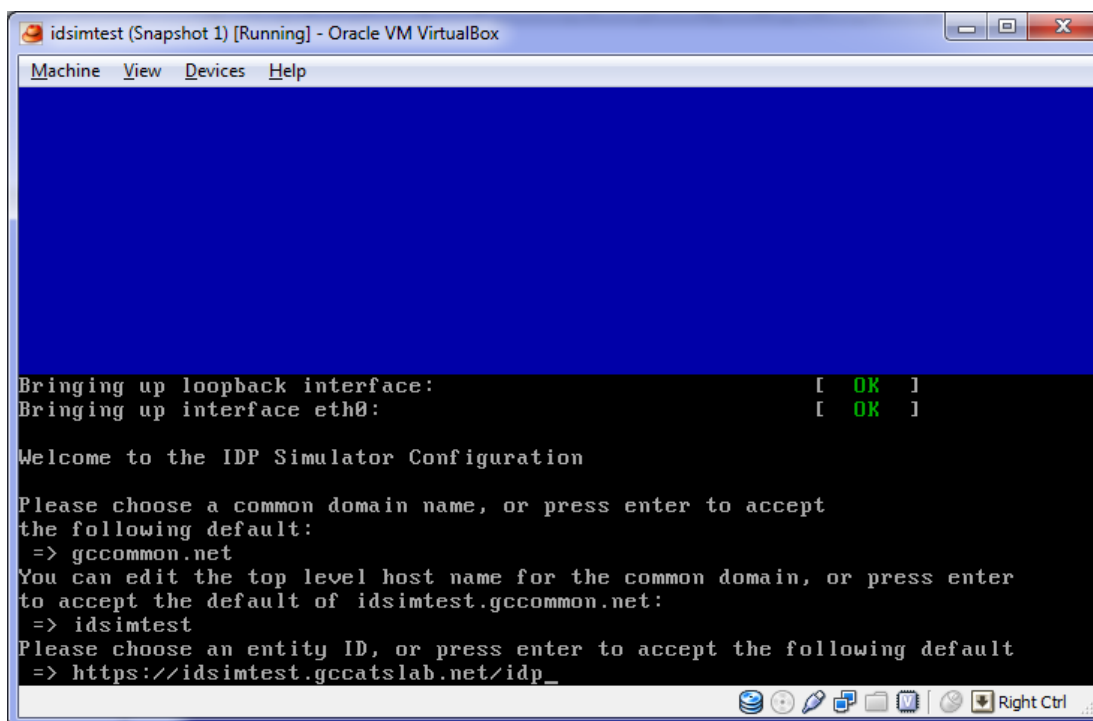
15. Select "Save & Quit".



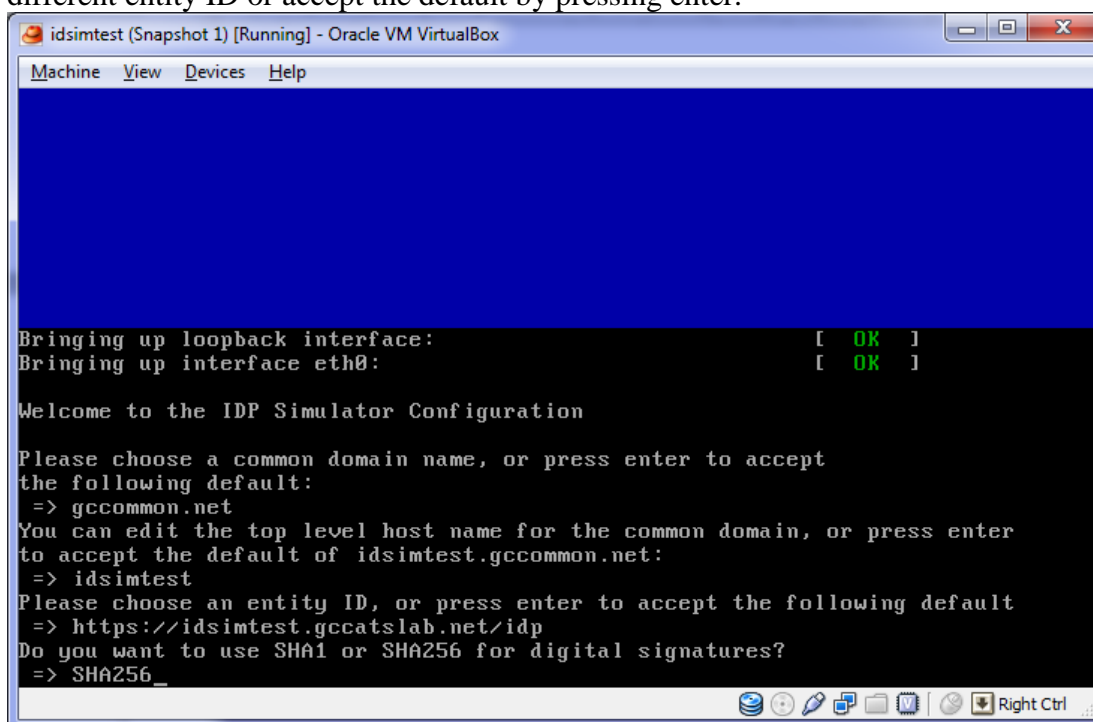
16. If you wish to use a common domain other than “fjgc-gccf.gc.ca” in your development or test environment you will be given an opportunity to specify its name. To use the default press enter.
17. At this point, the configuration script will attempt a DNS lookup of the host name you have specified. If no DNS entry is found (or no DNS server is configured) then an entry will be created in the /etc/hosts file.



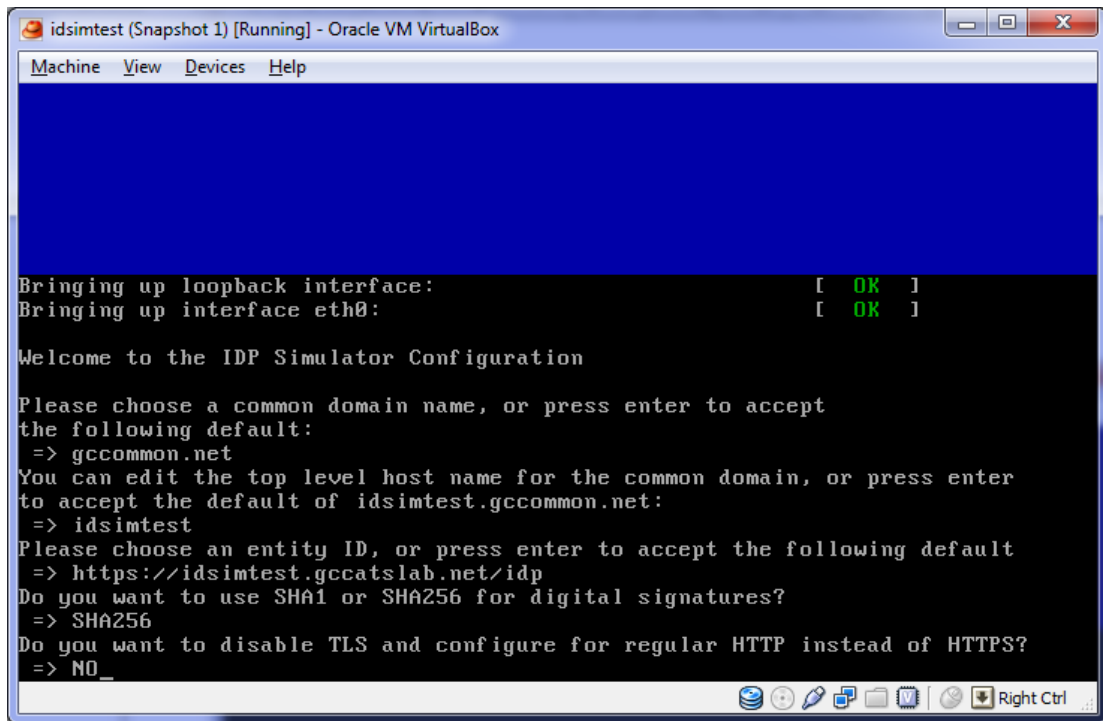
18. Next you can modify the host name to be used in the common domain if you wish.



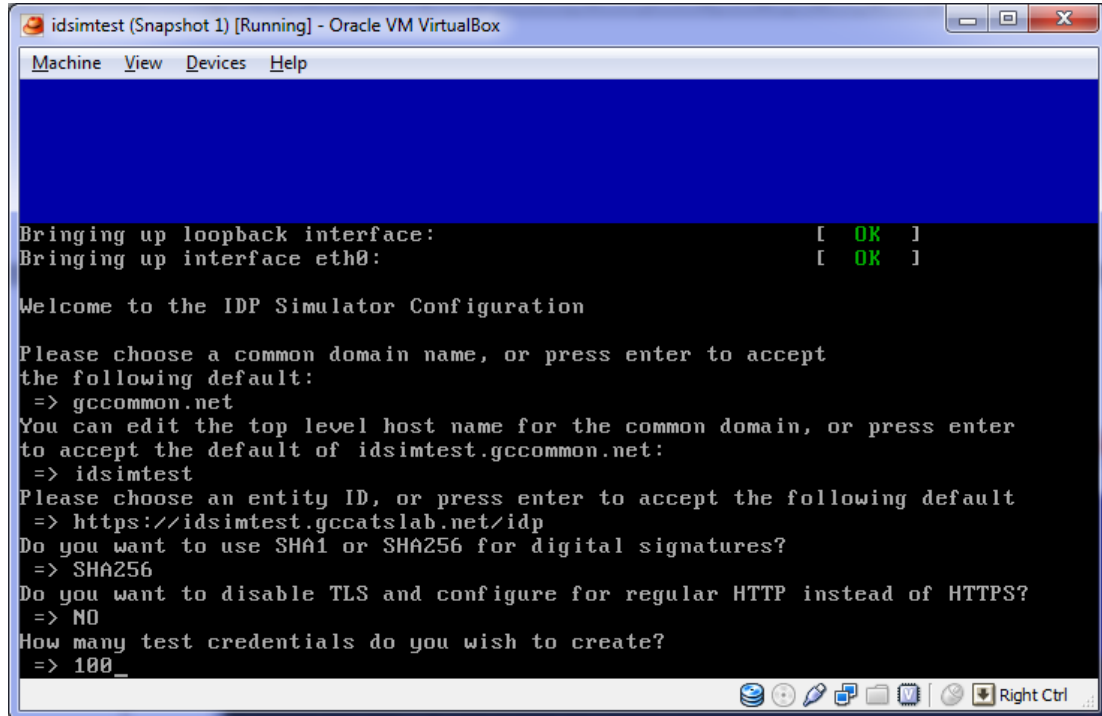
19. A default SAML entity ID will be created using the host name. You can specify a different entity ID or accept the default by pressing enter.



20. The IDP Simulator is capable of verifying both SHA-1 and SHA-256 signatures from RPs. Here you can specify which algorithm the simulator will use when signing its own SAML messages.



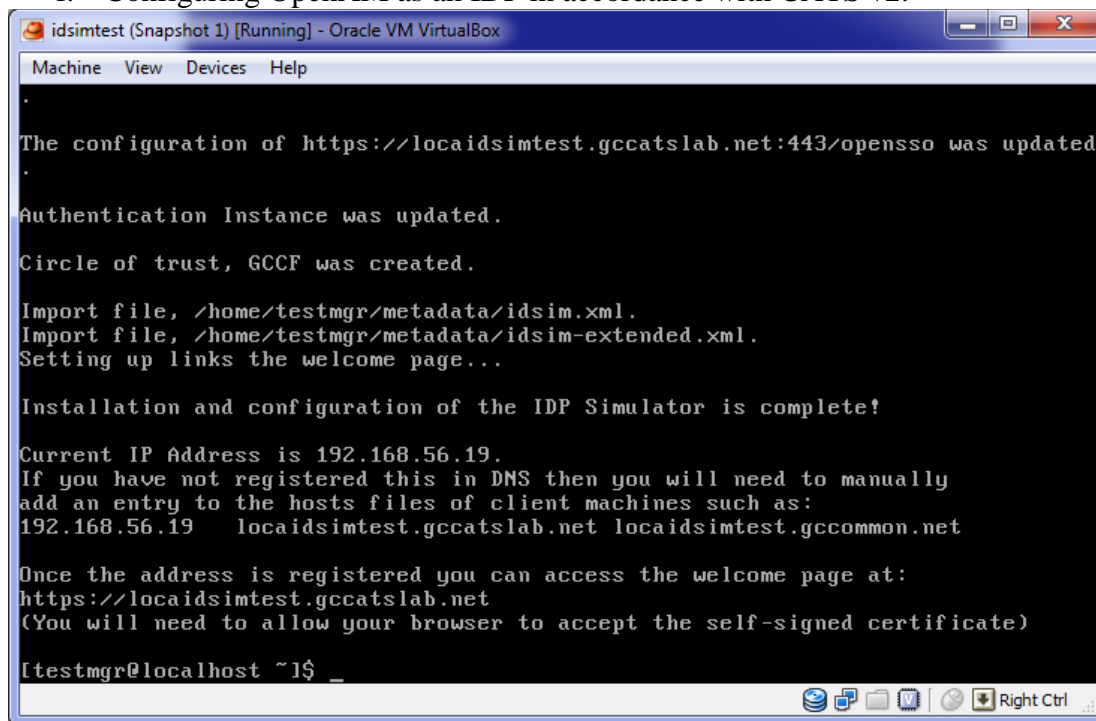
21. While CATS mandates the use of TLS it may be useful to disable it in order to perform troubleshooting in your development or test environment.



22. Next you can specify the number of test credentials that you wish to pre-load. The test userids will be of the format "user.n" where n starts at 0. All of the test credentials will

have the password “password”. Do not exceed 1 million test users as this may cause the simulator to run out of virtual disk space.

23. At this point, the configuration script has all of the information it needs. It will proceed to complete the installation and configuration process by:
- Generating and installing a self-signed SSL certificate for the web server,
 - Installing and starting an OpenDJ directory server,
 - Starting Apache Tomcat and installing OpenAM,
 - Configuring OpenAM for the selected host name,
 - Generating CATS-compliant SAML metadata for the IDP, and
 - Configuring OpenAM as an IDP in accordance with CATS v2.



```
idsimtest (Snapshot 1) [Running] - Oracle VM VirtualBox
Machine View Devices Help

The configuration of https://locaidsimtest.gccatslab.net:443/opensso was updated.
Authentication Instance was updated.
Circle of trust, GCCF was created.
Import file, /home/testmgr/metadata/idsim.xml.
Import file, /home/testmgr/metadata/idsim-extended.xml.
Setting up links the welcome page...

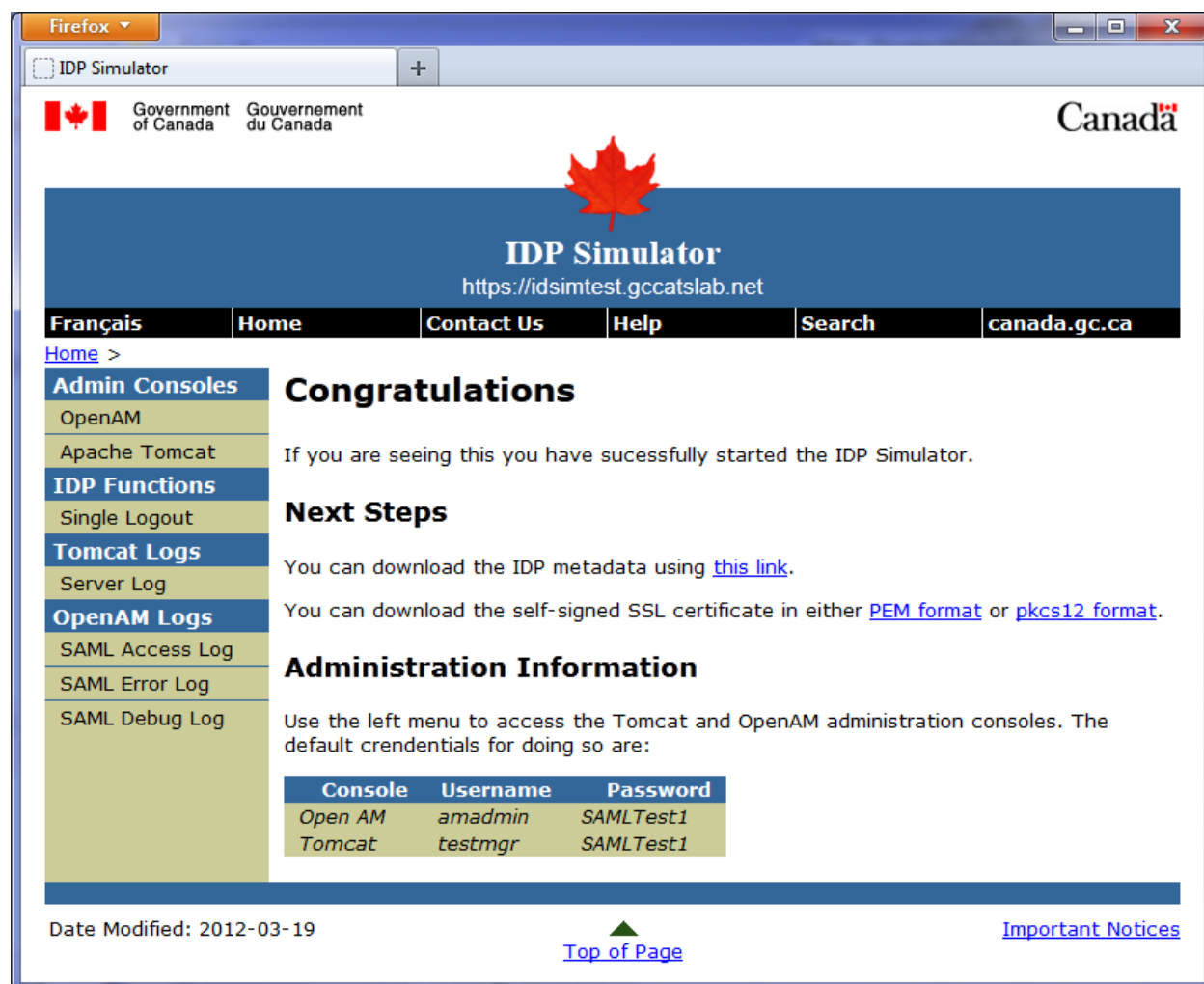
Installation and configuration of the IDP Simulator is complete!

Current IP Address is 192.168.56.19.
If you have not registered this in DNS then you will need to manually
add an entry to the hosts files of client machines such as:
192.168.56.19 locaidsimtest.gccatslab.net locaidsimtest.gcccommon.net

Once the address is registered you can access the welcome page at:
https://locaidsimtest.gccatslab.net
(You will need to allow your browser to accept the self-signed certificate)

[testmgr@localhost ~]$_
```

24. Once configuration is complete, the URL to access the web server will be displayed. Use a web browser to confirm that the simulator is running. Note that if the IDP Simulator is not registered in DNS then every server or client PC that accesses the IDP simulator must have an entry added to its host file. If an attempt is made to access the simulator by IP address or some other means then the secure nature of SAML and HTTPS will prevent it from functioning.



The IDP Simulator home page provides quick links to access the Tomcat and Open AM administration consoles. The Single Logout link can be used to initiate single logout from the IDP. Links are also provided to download the IDP's SAML metadata as well as the self-signed SSL certificate. Both of these will be required to configure your application's SAML interface to use the IDP Simulator. To assist in testing and debugging, links to download the Tomcat server log and the OpenAM SAML logs are also available.

2.4 Configuring a Service Provider

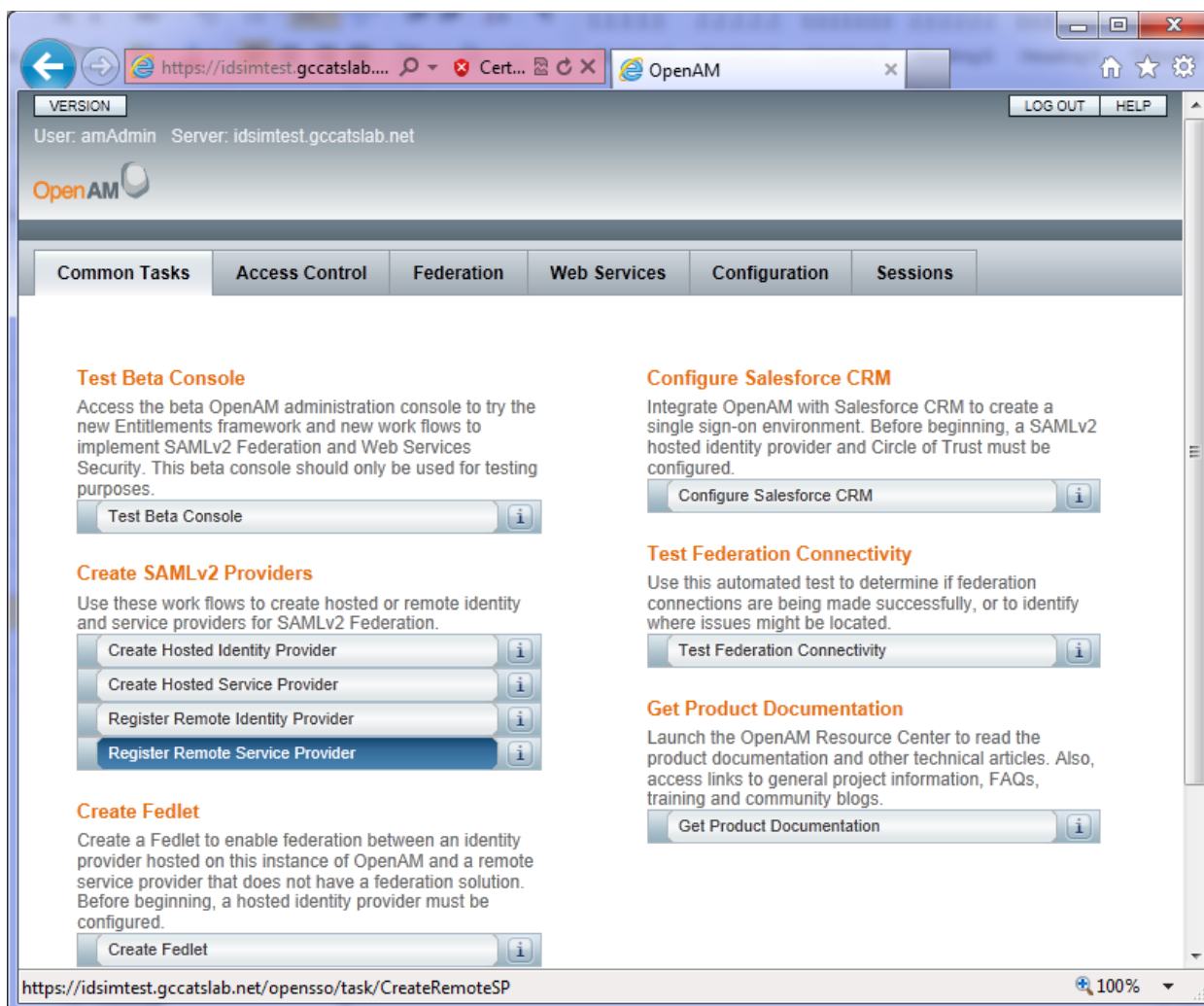
To configure the IDP Simulator to work with your application, proceed as follows.

1. From the IDP Simulator home page, launch the OpenAM admin console.



The screenshot shows a web browser window titled "Firefox" with a tab labeled "OpenAM (Login)". The page header includes the Government of Canada logo and text in English and French, along with navigation links for "Canada.gc.ca", "Services", "Departments", and "Français". The main heading is "IDP Simulator" with a large red maple leaf graphic and the "Canada" wordmark. A central "Login" form contains fields for "Username:" (with "amadmin" entered) and "Password:" (with masked characters). Below the fields are "Login" and "Clear" buttons. The footer includes links for "Terms and conditions" and "Transparency", a small maple leaf icon, and a list of government services: HEALTH (healthycanadians.gc.ca), TRAVEL (travel.gc.ca), SERVICE CANADA (servicecanada.gc.ca), JOBS (jobbank.gc.ca), and ECONOMY (actionplan.gc.ca), followed by the "Canada.gc.ca" logo. The version "Version: 0.0" is displayed in the bottom right corner of the main content area.

2. Log in as “amadmin” (the password is “SAMLTest1”).



3. Select “Register Remote Service Provider”.

The screenshot shows the OpenAM web interface in a browser window. The address bar shows the URL <https://idsimtest.gccatslab.net>. The page title is "Create a SAMLv2 Remote Service Provider". The user is logged in as "amAdmin" and the server is "idsimtest.gccatslab.net". The page contains the following sections:

- Create a SAMLv2 Remote Service Provider**: Includes a "Configure" button and a "Cancel" button. A description states: "This page allows you to register a remote Service Provider (SP). You need two things: Circle of Trust (COT) and metadata of the provider. A COT is a group of Identity Providers (IDPs) and SPs that trust each other and in effect represents the confines within which all federation communications are performed. Metadata represents the configuration necessary to execute federation protocols (eg SAMLv2) as well as the mechanism to communicate this configuration to other entities (eg IDPs) in a COT." A note indicates that an asterisk (*) denotes a required field.
- Where does the metadata file reside?:** Two radio buttons are present: "URL" and "File". The "File" radio button is selected.
- URL where metadata is located:** A text input field is empty, and an "Upload..." button is next to it.
- Circle of Trust**: Two radio buttons are present: "Add to existing" and "Add to new". The "Add to existing" radio button is selected.
- Existing Circle of Trust:** A dropdown menu shows "GCCF" as the selected option.
- Attribute Mapping**: A section with a "Delete" button and a table with two columns: "Name in Assertion" and "Local Attribute Name".

4. Select the "File" radio button next to "Where does the metadata file reside?", then select the "Upload" Button.

The screenshot shows a "Select File to Upload" dialog box. The title bar says "OpenAM - Windows Internet Explorer". The address bar shows the URL <https://idsimtest.gccatslab.net/opensso/federation/FileUploader>. The dialog box contains the following elements:

- Select File to Upload**: A title for the dialog box.
- Upload File** and **Cancel**: Two buttons at the top right.
- File Path**: A text input field showing "L:\CATSLab\Metadata\vp:" and a "Browse..." button next to it.

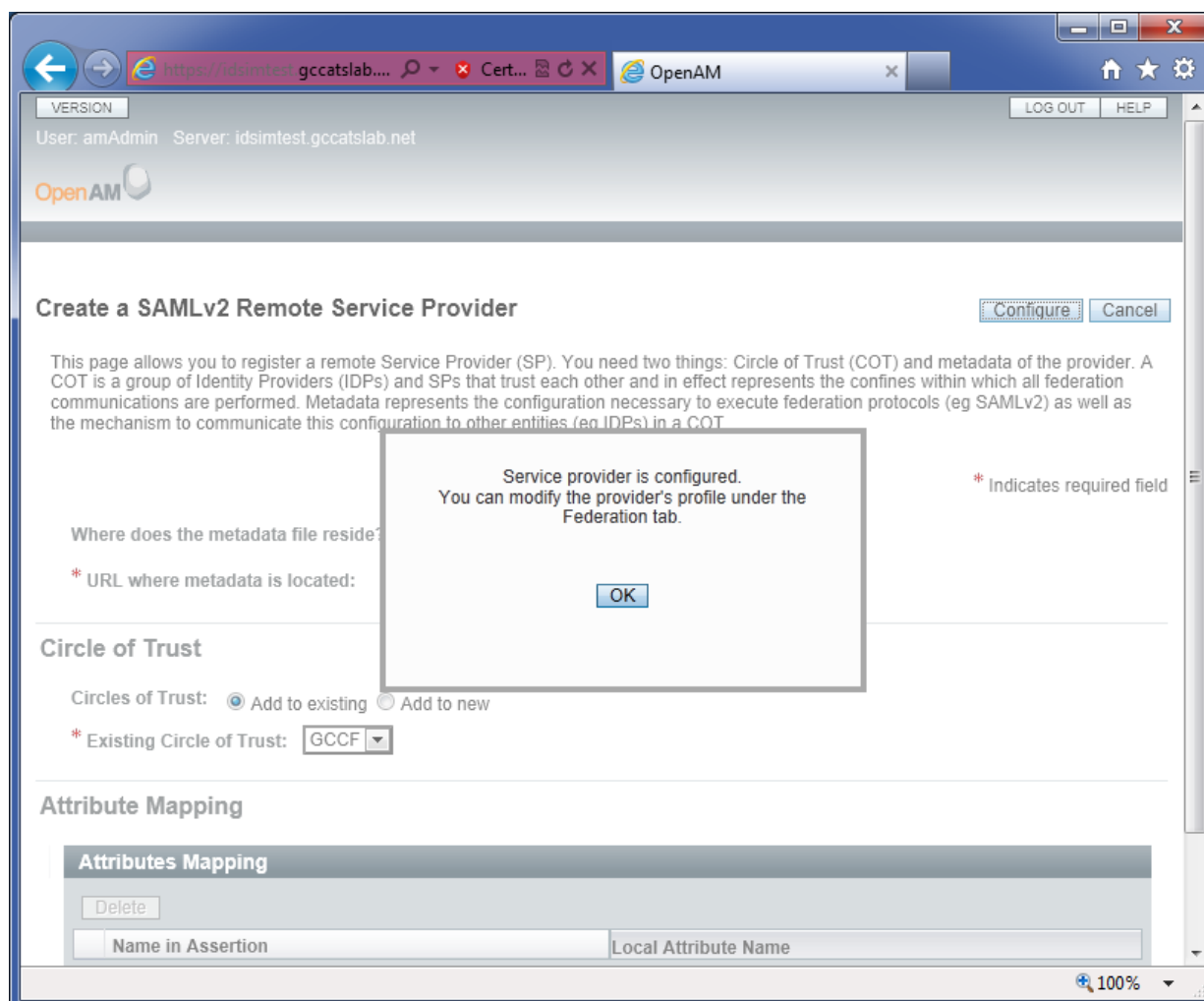
5. Browse to the location of your CATS2 compliant metadata and select "Upload File".

The screenshot shows a web browser window with the URL `https://idsimtest.gccatslab.net`. The page title is "Create a SAMLv2 Remote Service Provider". The user is logged in as "amAdmin" on the server "idsimtest.gccatslab.net". The page contains the following sections:

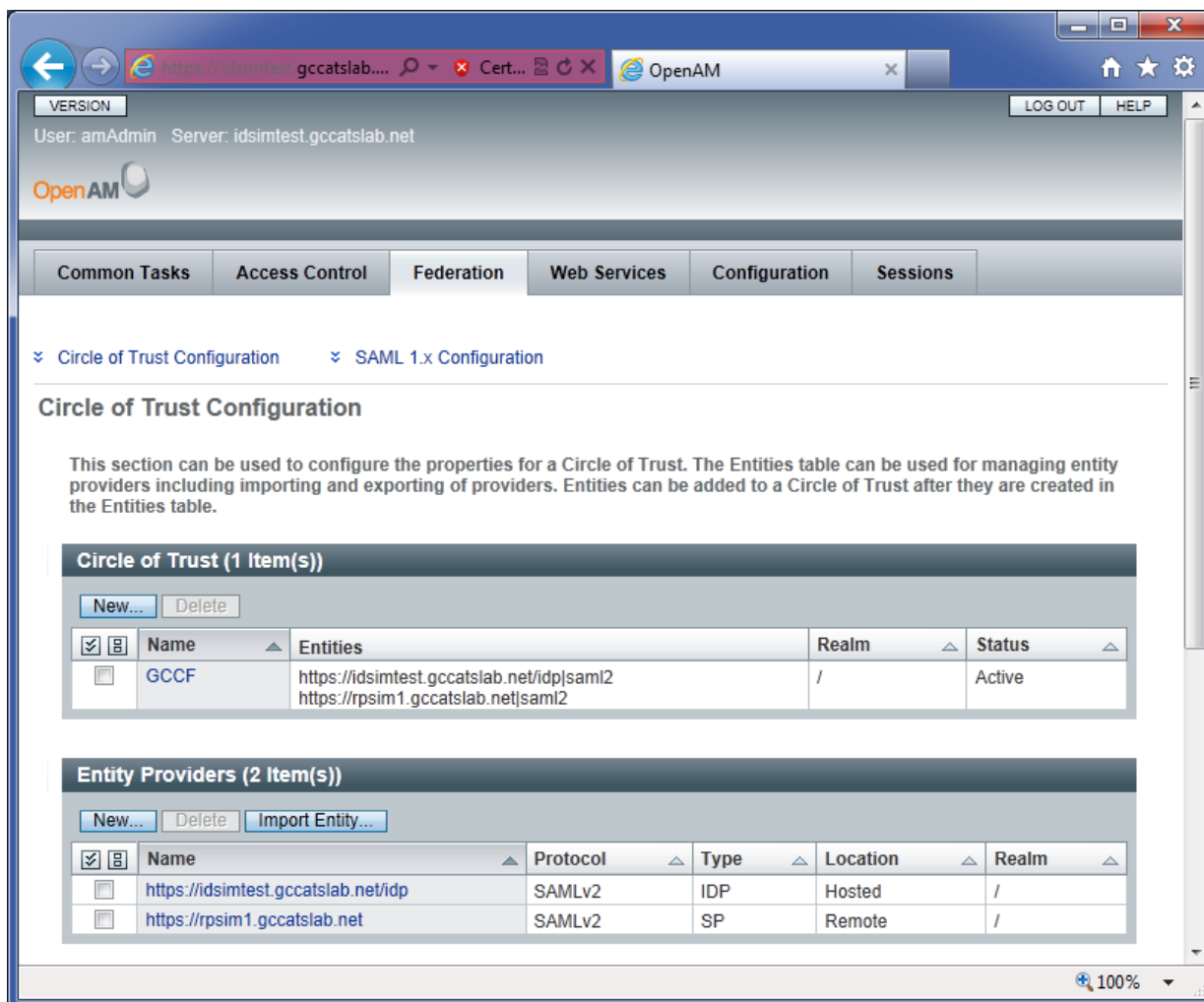
- Header:** Includes "LOG OUT" and "HELP" buttons.
- Instructions:** A paragraph explaining that a remote Service Provider (SP) can be registered by providing a Circle of Trust (COT) and metadata. It defines COT as a group of Identity Providers (IDPs) and SPs that trust each other, and metadata as configuration for federation protocols like SAMLv2.
- Metadata Location:** A section titled "Where does the metadata file reside?:" with radio buttons for "URL" and "File". The "File" option is selected. Below it, a text field labeled "* URL where metadata is located:" contains the path `C:\fakepath\rpsim1-cats2.xml`. An "Upload..." button is next to the field.
- Circle of Trust:** A section titled "Circle of Trust" with radio buttons for "Add to existing" and "Add to new". The "Add to existing" option is selected. Below it, a text field labeled "* Existing Circle of Trust:" contains the value "GCCF".
- Attribute Mapping:** A section titled "Attribute Mapping" containing a table with the following structure:

Attributes Mapping	
<input type="button" value="Delete"/>	
Name in Assertion	Local Attribute Name

6. Select the "Configure" Button at the top-right of the page.



7. Click on "OK" to return to the admin console home page.



The screenshot shows the OpenAM web interface. The browser address bar displays <https://idsimtest.gccatslab.net>. The page header includes the OpenAM logo and navigation links for LOG OUT and HELP. The main navigation menu has tabs for Common Tasks, Access Control, Federation, Web Services, Configuration, and Sessions. The Federation tab is selected, and the sub-tab Circle of Trust Configuration is active. Below the sub-tab, there is a description of the Circle of Trust configuration and two tables.

Circle of Trust Configuration

This section can be used to configure the properties for a Circle of Trust. The Entities table can be used for managing entity providers including importing and exporting of providers. Entities can be added to a Circle of Trust after they are created in the Entities table.

Circle of Trust (1 Item(s))

New... Delete

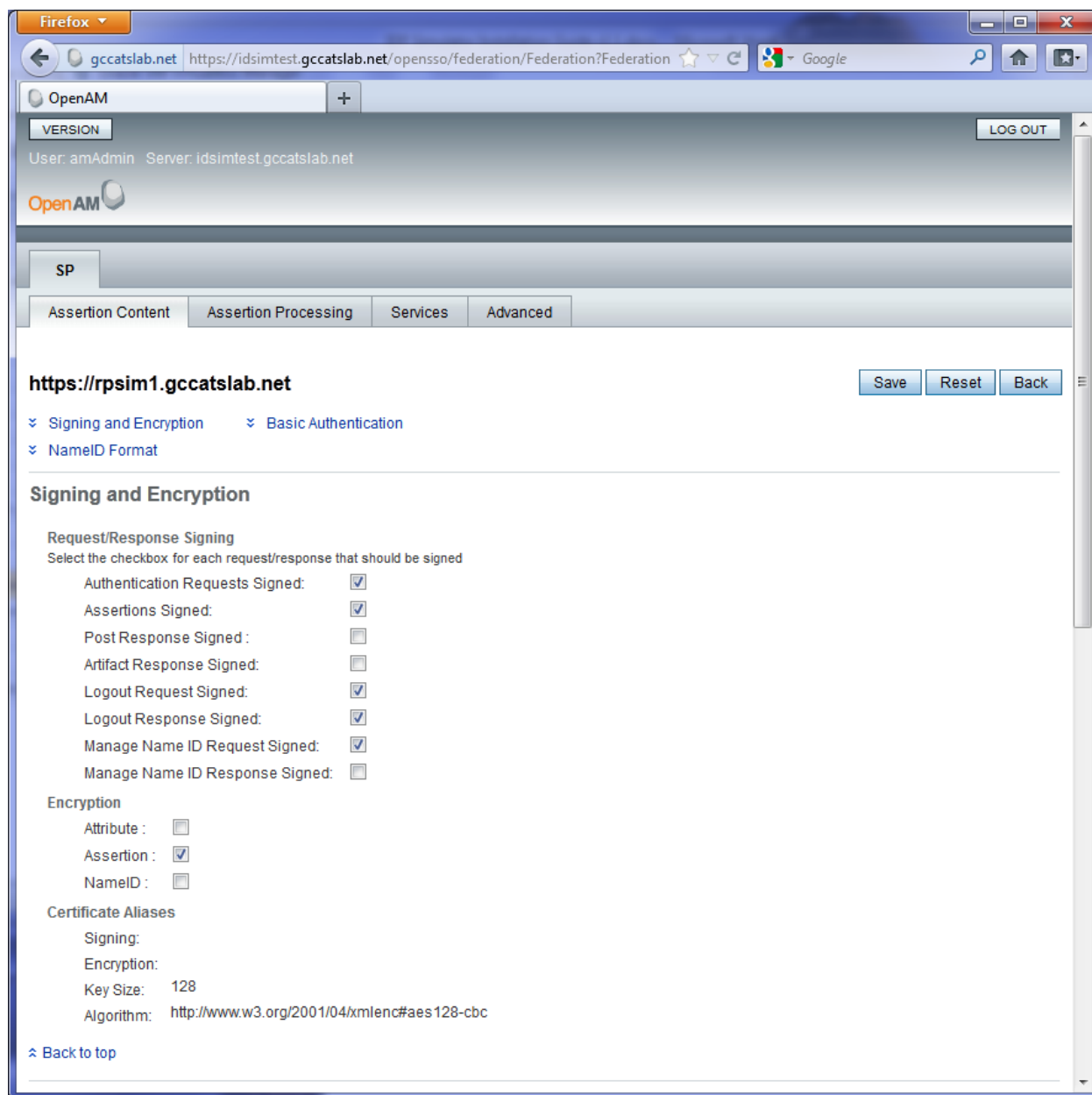
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Name	Entities	Realm	Status
<input type="checkbox"/>		GCCF	https://idsimtest.gccatslab.net/idp/saml2 https://rpsim1.gccatslab.net/saml2	/	Active

Entity Providers (2 Item(s))

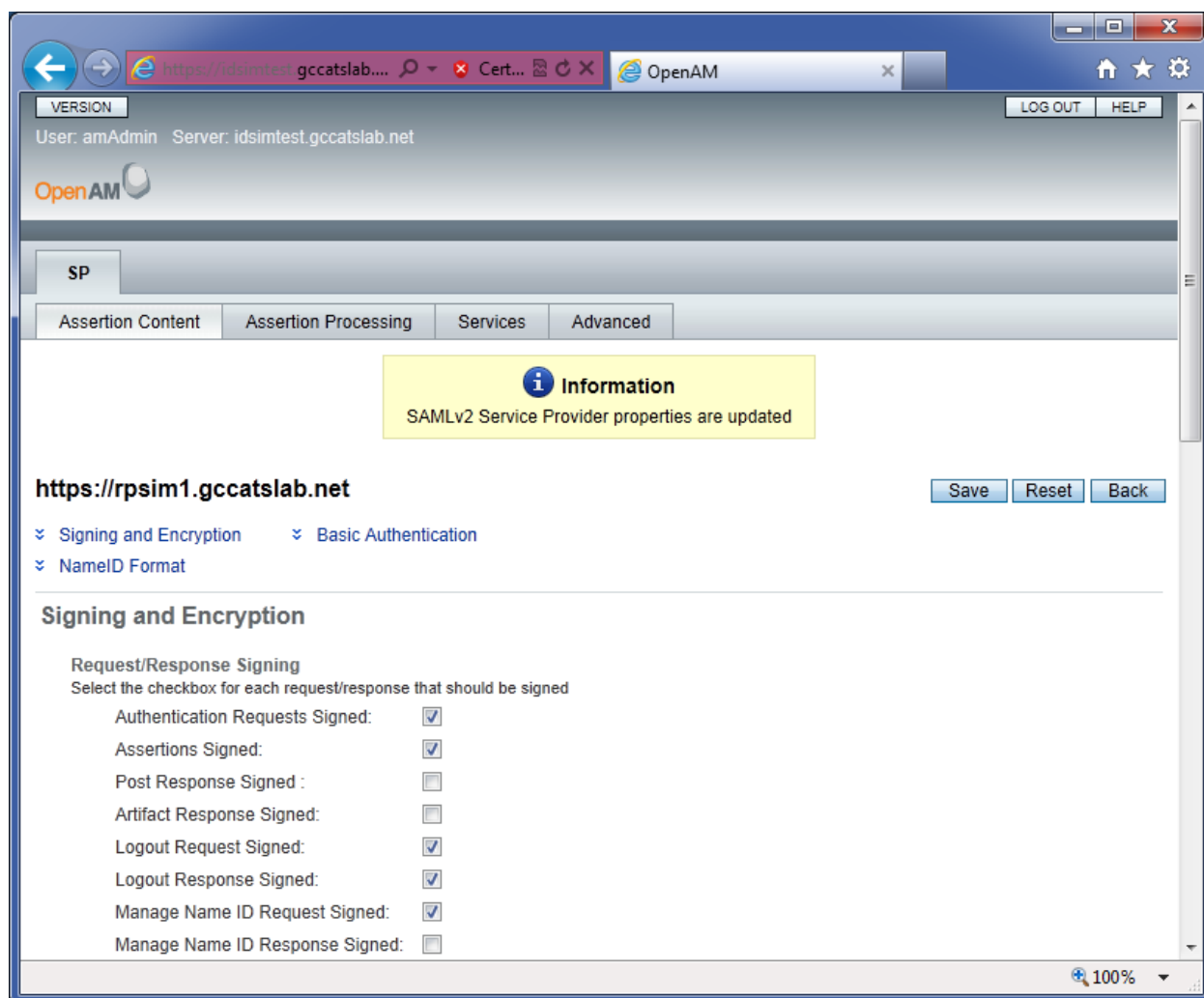
New... Delete Import Entity...

<input checked="" type="checkbox"/>	<input type="checkbox"/>	Name	Protocol	Type	Location	Realm
<input type="checkbox"/>		https://idsimtest.gccatslab.net/idp	SAMLv2	IDP	Hosted	/
<input type="checkbox"/>		https://rpsim1.gccatslab.net	SAMLv2	SP	Remote	/

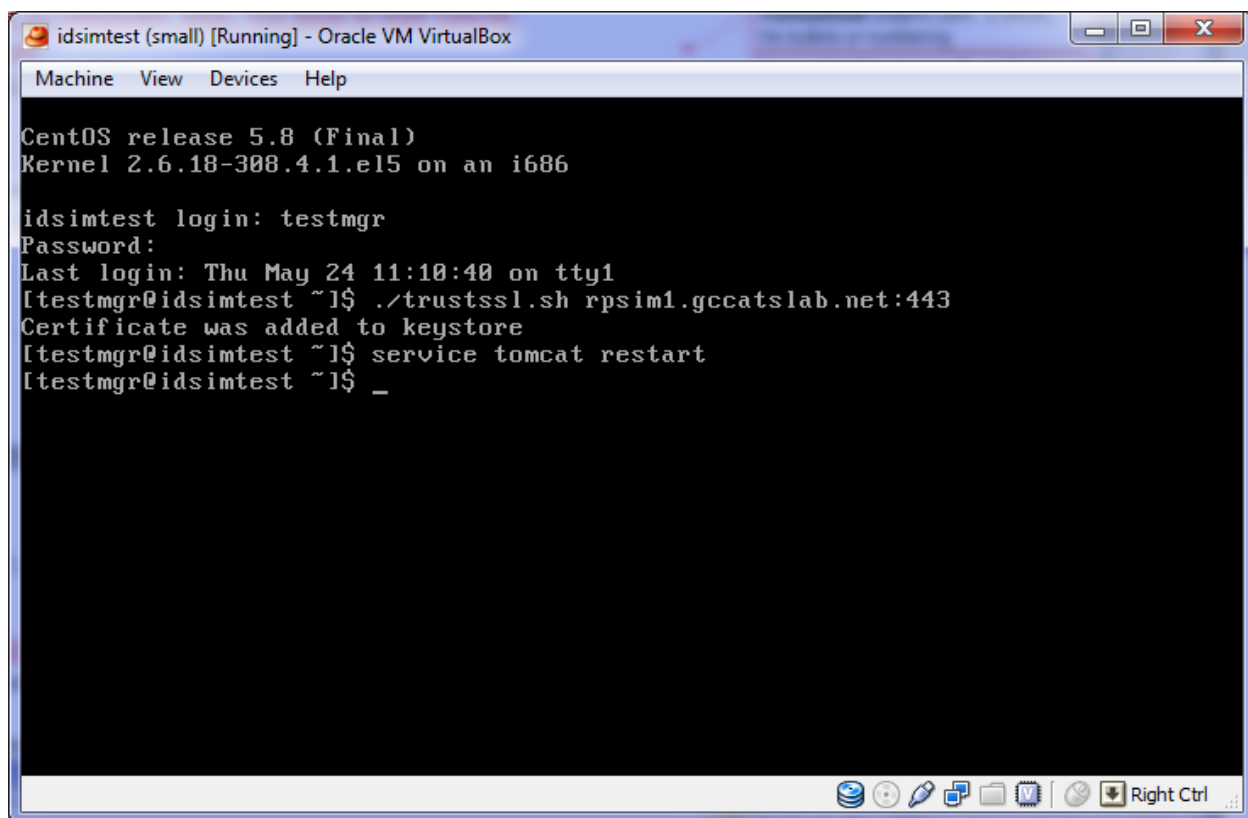
8. Select the “Federation Tab” to display the Circle of Trust configuration page.



9. Select the entity ID of your service provider at the bottom of the page to bring up the SP Configuration page. Under Request/Response signing select the checkboxes for "Logout Request Signed", "Logout Response Signed" and Manage Name ID Request Signed". Under Encryption, select the checkbox for "Assertion".



10. Select “Save”. OpenAM is now configured to work with your application.
11. You should log out of the admin console before attempting a test (or OpenAM will satisfy your application’s authentication request by performing a single-sign on for the “amadmin” user). For best results, close and re-open your browser before testing.
12. If your RP is not using a commercially recognized SSL certificate they you will need to add its certificate to the IDP Simulator’s trusted certificate store in order for SOAP single logout to work. This can be easily done using the trustssl.sh script in the testmgr home directory:



```
idsimtest (small) [Running] - Oracle VM VirtualBox
Machine View Devices Help

CentOS release 5.8 (Final)
Kernel 2.6.18-308.4.1.el5 on an i686

idsimtest login: testmgr
Password:
Last login: Thu May 24 11:10:40 on tty1
[testmgr@idsimtest ~]$ ./trustssl.sh rpsim1.gccatslab.net:443
Certificate was added to keystore
[testmgr@idsimtest ~]$ service tomcat restart
[testmgr@idsimtest ~]$ _
```

Note that your RP web server must be running and accessible so that the trust.ssl script can connect to it and retrieve its certificate. Also, you must re-start tomcat as shown in order for the change to take effect.

2.5 Creating Additional Test Users

Do not use the “amadmin” user to test your application. “amadmin” is a special user and OpenAM will not provide the same nameID (PAI) to your application from login to login. The test users created the installation will have username “user.n” (where n starts from 0) and password “password”. Additional users can be manually added as follows:

1. From the IDP Simulator home page, launch the OpenAM admin console.

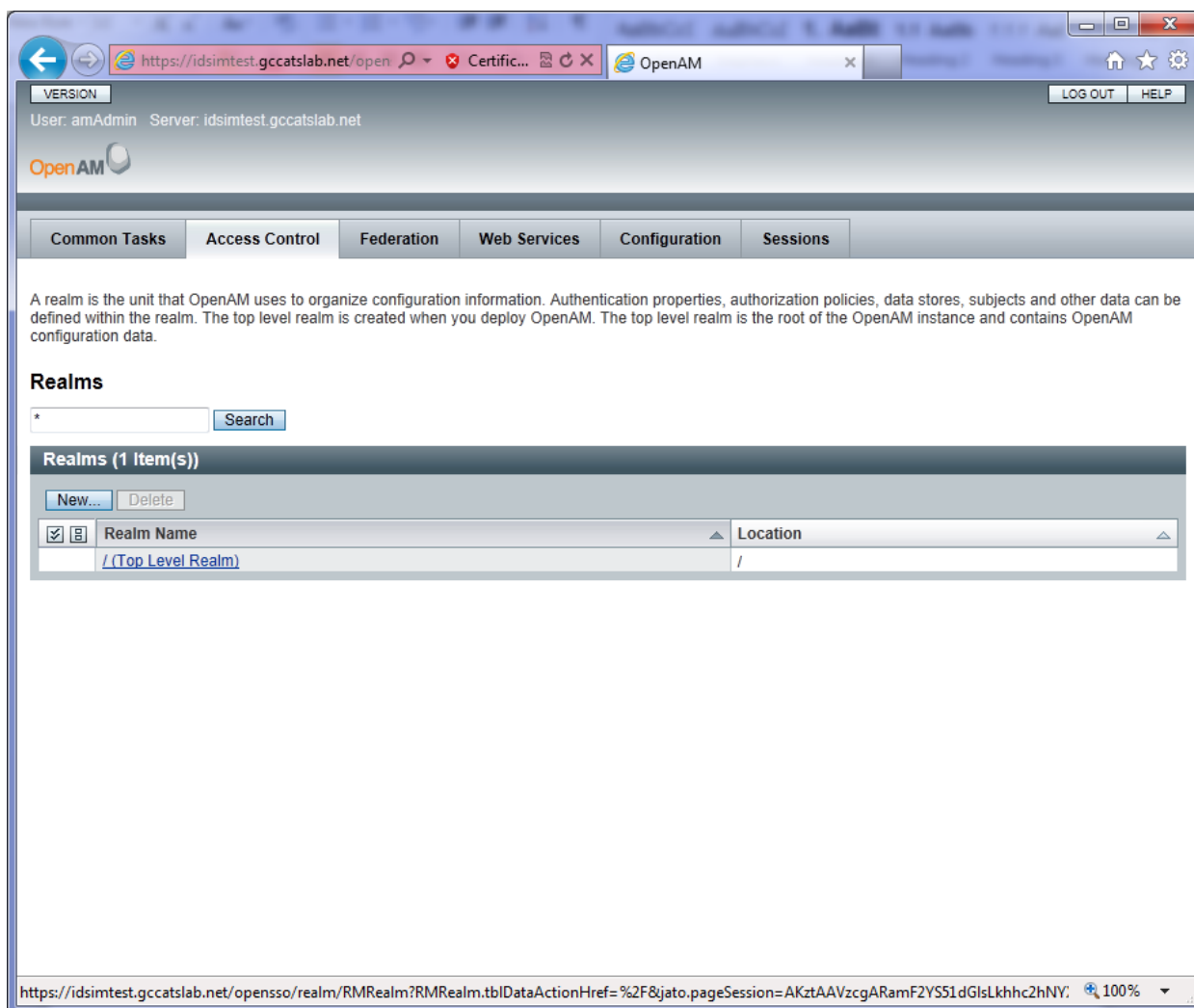


The screenshot shows a web browser window titled "Firefox" with a single tab labeled "OpenAM (Login)". The page header includes the Government of Canada logo and text in English and French, along with navigation links for "Canada.gc.ca", "Services", "Departments", and "Français". The main heading is "IDP Simulator" with a large red maple leaf graphic and the "Canada" wordmark. A central "Login" form contains fields for "Username:" (with "amadmin" entered) and "Password:" (with masked characters). Below these fields are "Login" and "Clear" buttons. The footer includes links for "Terms and conditions" and "Transparency", a small maple leaf icon, and a list of government services: HEALTH (healthycanadians.gc.ca), TRAVEL (travel.gc.ca), SERVICE CANADA (servicecanada.gc.ca), JOBS (jobbank.gc.ca), and ECONOMY (actionplan.gc.ca), followed by the "Canada.gc.ca" logo. The version "Version: 0.0" is displayed in the bottom right corner of the main content area.

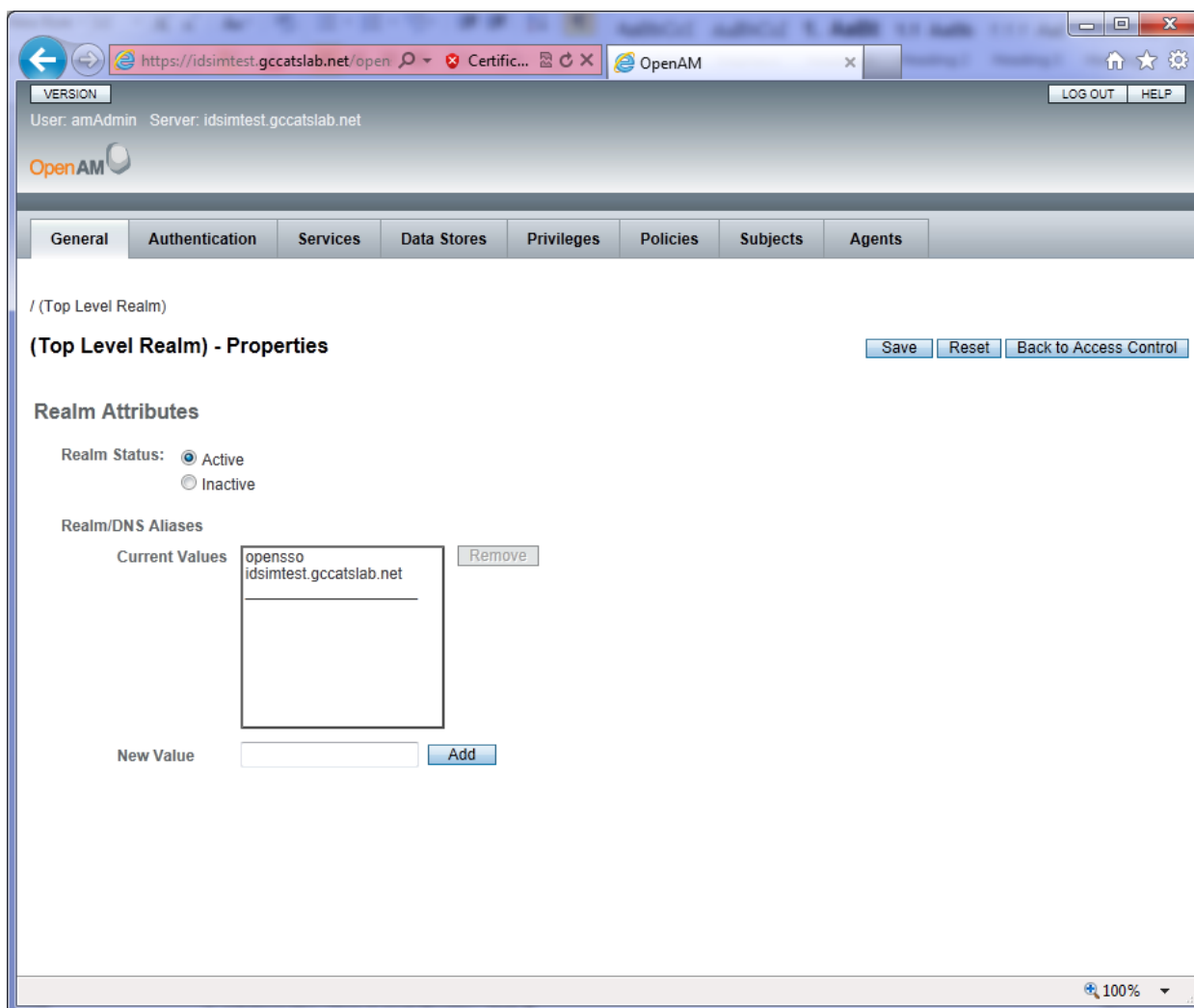
2. Log in as “amadmin” (the password is “SAMLTest1”).



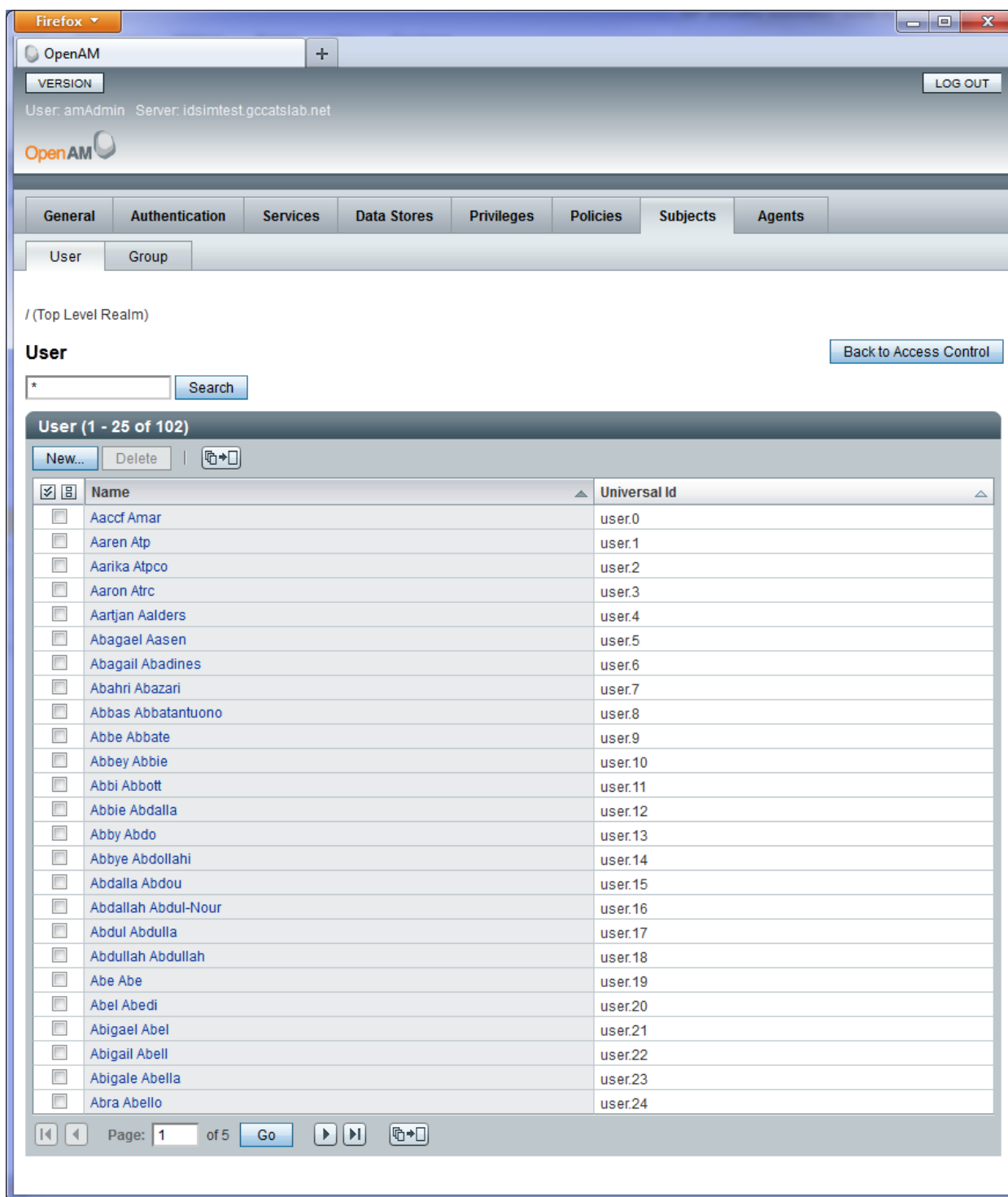
3. Select the “Access Control” tab.



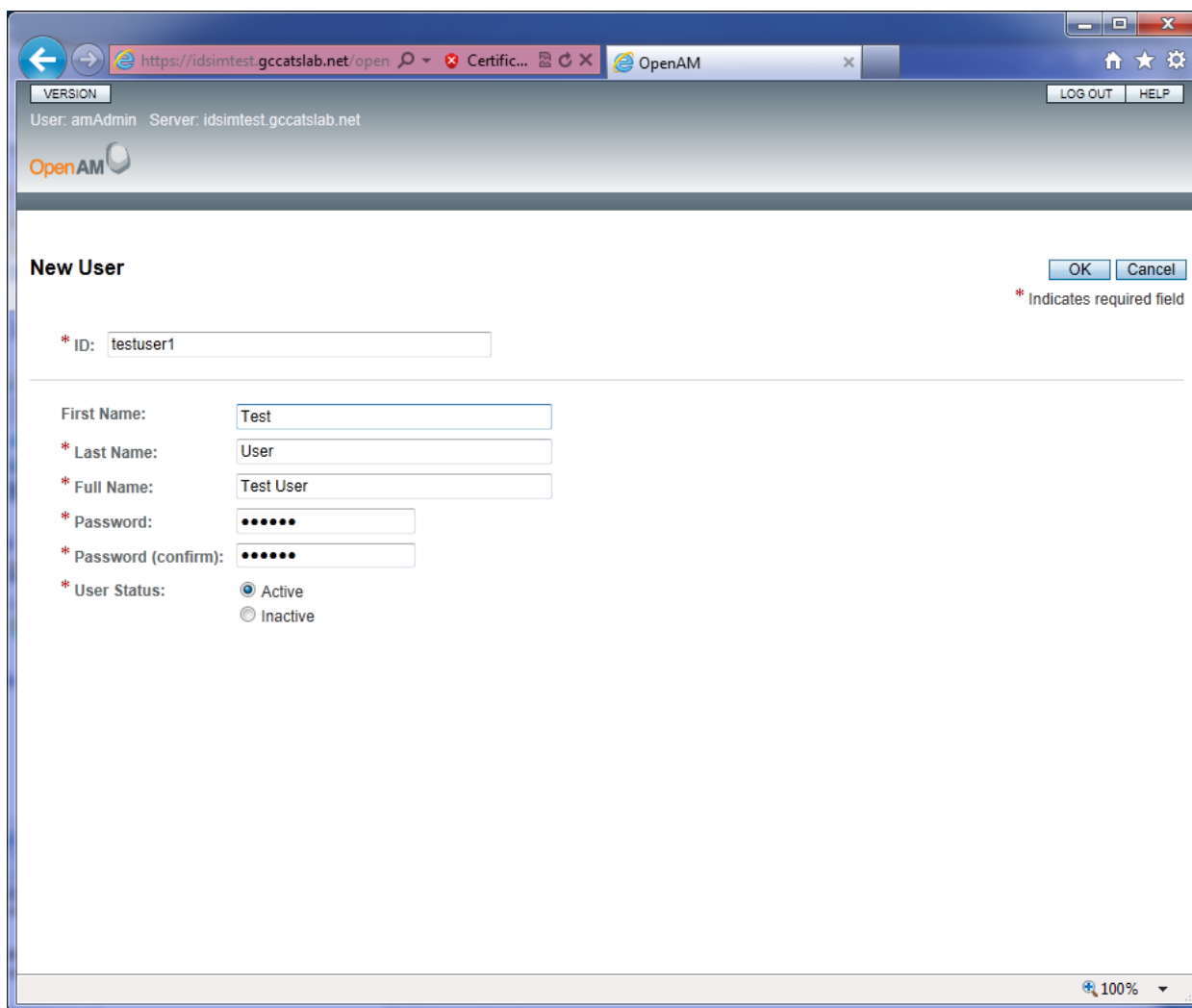
4. Select the “Top Level Realm” link.



5. Select the “Subjects” Tab.



6. At the top of the user list select the “New...” button.



The screenshot shows a web browser window with the URL <https://idsimtest.gccatslab.net/open>. The browser's address bar shows a warning icon and the text "Certific...". The OpenAM logo is visible in the top left corner of the page. The page title is "New User". The user is logged in as "amAdmin" and the server is "idsimtest.gccatslab.net". The form contains the following fields:

- * ID: testuser1
- First Name: Test
- * Last Name: User
- * Full Name: Test User
- * Password: [masked]
- * Password (confirm): [masked]
- * User Status: ☒ Active, ☐ Inactive

Buttons for "OK" and "Cancel" are located in the top right corner. A legend indicates that "*" indicates a required field. The bottom right corner shows a zoom level of 100%.

7. Enter the data for the new user account and select “OK”.

2.6 Enabling Signature Algorithm (SHA-256)

The IDP Simulator is capable of verifying both SHA-1 and SHA-256 signatures from RPs. The instruction below is to specify the use of the SHA-256 algorithm for when the IDP simulator sign it's own SAML messages.

1. From the IDP Simulator home page, launch the OpenAM admin console.

Firefox

OpenAM (Login)

Government of Canada
Gouvernement du Canada

Canada.gc.ca | Services | Departments | Français

IDP Simulator

Canada

Login

Username:
amadmin

Password:
••••••••••

Login Clear

Version: 0.0

Terms and conditions | Transparency

HEALTH
healthycanadians.gc.ca

TRAVEL
travel.gc.ca

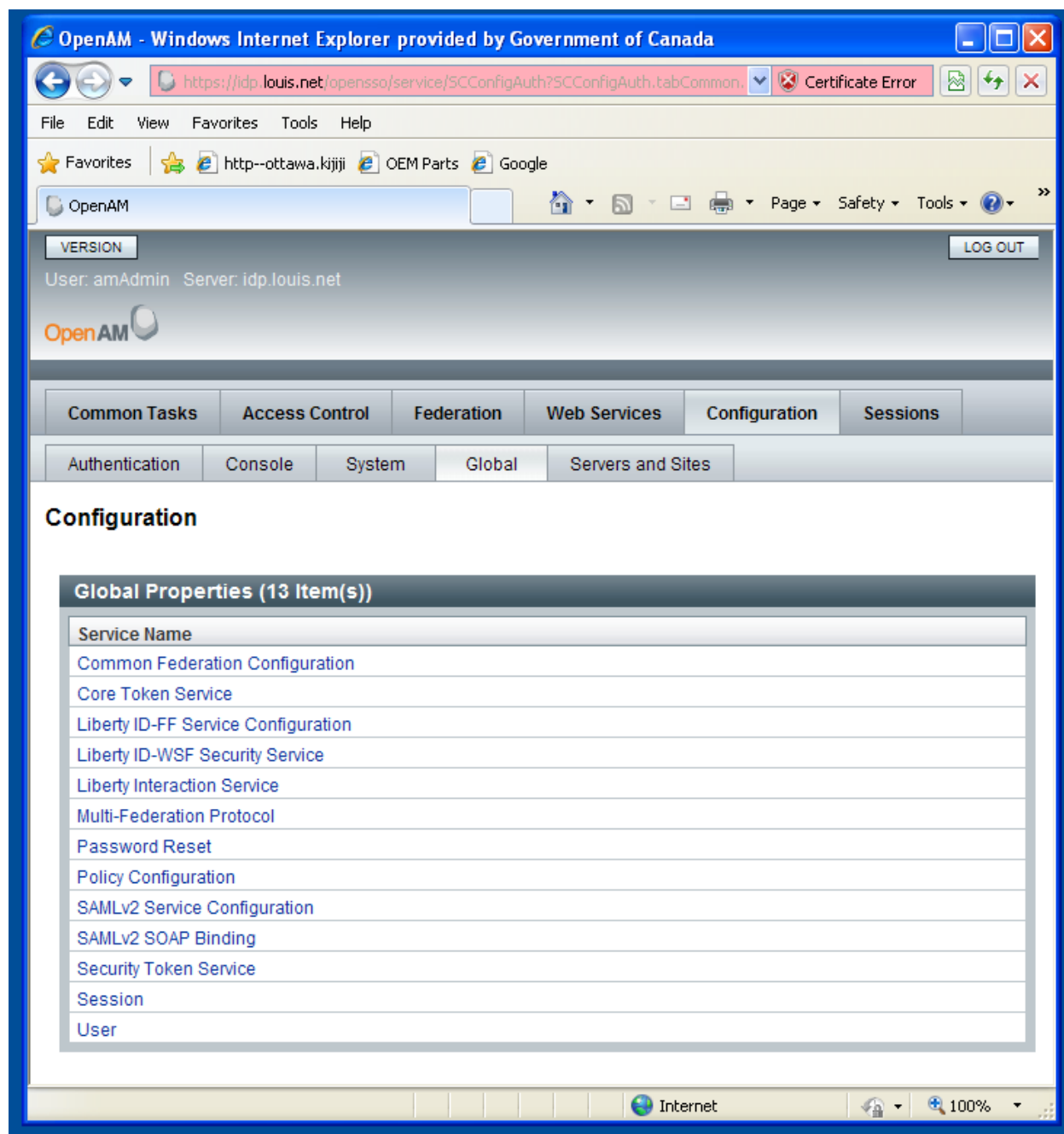
SERVICE CANADA
servicecanada.gc.ca

JOBS
jobbank.gc.ca

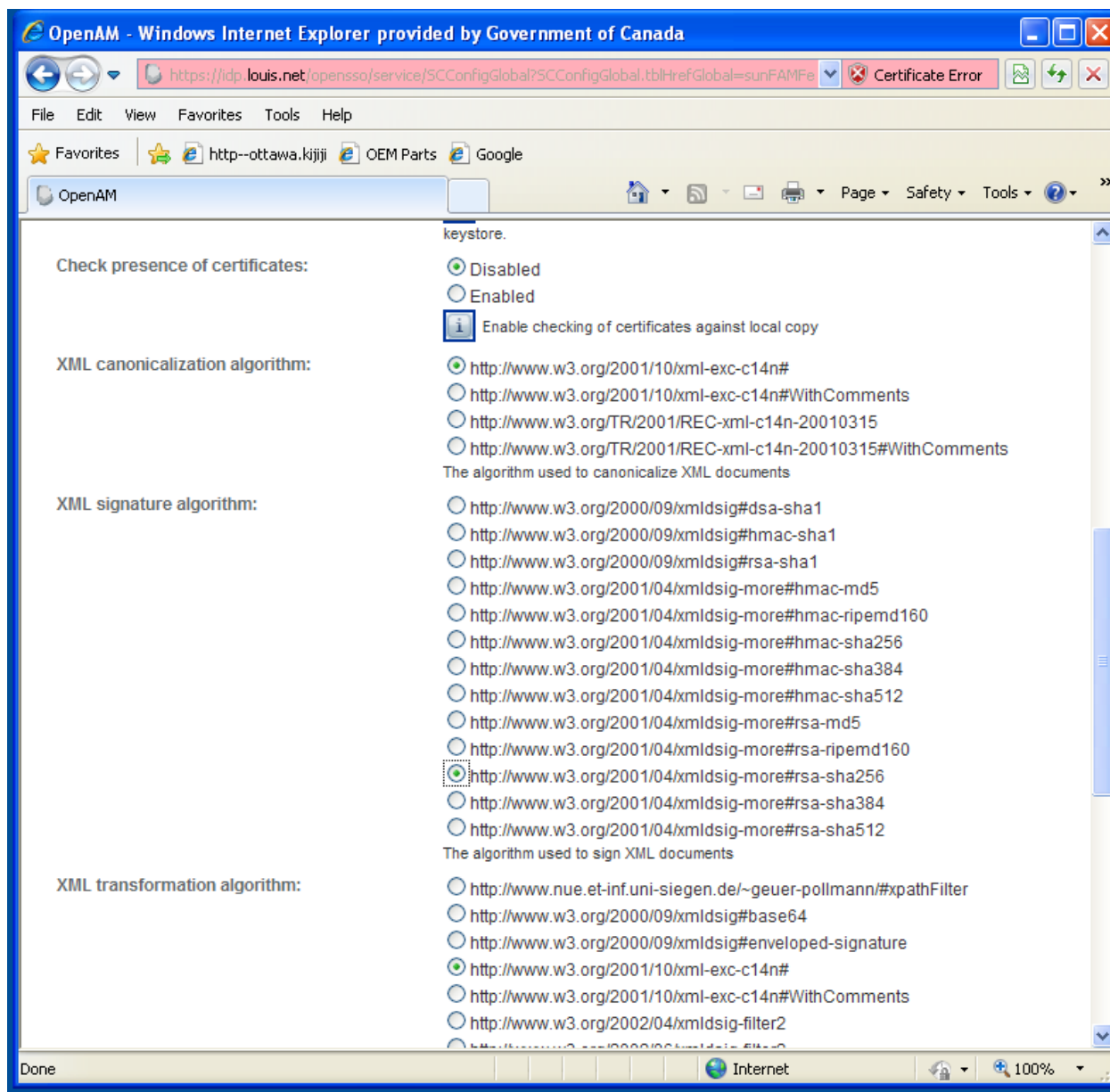
ECONOMY
actionplan.gc.ca

Canada.gc.ca

2. Log in as “amadmin” (the password is “SAMLTest1”).



3. Select “Configuration”, then the “Global” tab.
4. Select ‘Common Federation Configuration’.



5. Scroll down and select "http://www.w3.org/2001/04/xmldsig-more#rsa-sha256".
6. Scroll back up, select 'Save'. OpenAM is now configured to work with your application.
7. You should log out of the admin console before attempting a test (or OpenAM will satisfy your application's authentication request by performing a single-sign on for the "amadmin" user). For best results, close and re-open your browser before testing.

3. Load and Performance Testing Tips

The IDP Simulator can be used to support load and performance testing of your Relying Party application and enrolment system. Testing by Shared Services Canada has shown that when allocated 2GB of memory and 4 CPUs, the IDP Simulator can sustain over 5,000 login/logout transactions per minute.

Here are a few useful tips for using the IDP Simulator in your performance testing environment:

- The very first time OpenAM sends an assertion to an RP for a given credential; it creates the NameID (PAI) for that RP and stores it in the directory. There is a significant (5x) performance hit when it does this, so it's a good idea to get your load testing tool to log in to each test credential once (via a SAML request from your RP) before starting actual testing of the RP application.
- Since the objective is to load test your application and not the IDP simulator, your testing tool should be configured to refrain from fetching unneeded page resources (images, css stylesheets, javascript files) that are referenced by the IDP Simulator login page.

4. Other Testing Tools

There are a number of simple tools available that can be of great help when testing the SAML interface between an RP and a CSP.

4.1.1 Browser HTTP Tracing

Most modern web browsers have built-in or third-party tools that can be used to observe the HTTP messages being sent to and from the browser. These can be of great help when examining the exchange of SAML messages that use the HTTP redirect and HTTP post bindings. For Example:

1. Microsoft Internet Explorer 9 provides an HTTP capture tool that can be accessed by pressing F12 and then clicking on the "Network" tab.
2. There are several add-ons available for Mozilla Firefox at <https://addons.mozilla.org/>. Two of the more useful are "HTTPFox", and "SAML Tracer".
3. The HTTP capture tool in Google Chrome can be accessed by launching the developer tools (Ctrl-Shift-I) and then selecting the "Network" icon.

4.1.2 URL and Base-64 Decoding Tools

SAML messages sent using the HTTP redirect and post bindings are Base 64 encoded and then URL encoded. Several public web services are available that can decode these strings allowing you to examine the SAML messages in their XML form. These can be easily found by searching for "URL Decoder" and "Base 64 Decoder" in your favorite search engine. Note that the "SAML Tracer" add-on for Firefox automatically performs URL and Base 64 decoding of SAML messages.