

# HP Operations Orchestration Software

Software Version: 7.50

## *Guide to Enabling Single Sign-on*

Document Release Date: March 2009

Software Release Date: March 2009



## Legal Notices

### Warranty

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

### Restricted Rights Legend

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

### Copyright Notices

© Copyright 2009 Hewlett-Packard Development Company, L.P.

### Trademark Notices

All marks mentioned in this document are the property of their respective owners.

# Finding or updating documentation on the Web

Documentation enhancements are a continual project at Hewlett-Packard Software. You can obtain or update the HP OO documentation set and tutorials at any time from the HP Software Product Manuals web site. You will need an HP Passport to log in to the web site.

## To obtain HP OO documentation and tutorials

1. Go to the HP Software Product Manuals web site (<http://support.openview.hp.com/selfsolve/manuals>).
2. Log in with your HP Passport user name and password.  
OR

If you do not have an HP Passport, click **New users – please register** to create an HP Passport, then return to this page and log in.

If you need help getting an HP Passport, see your HP OO contact.

3. In the **Product** list box, scroll down to and select **Operations Orchestration**.
4. In the **Product Version** list, click the version of the manuals that you're interested in.
5. In the **Operating System** list, click the relevant operating system.
6. Click the **Search** button.
7. In the **Results** list, click the link for the file that you want.

## Where to Find Help, Tutorials, and More

The HP Operations Orchestration software (HP OO) documentation set is made up of the following:

- Help for Central

Central Help provides information to the following:

- Finding and running flows
- For HP OO administrators, configuring the functioning of HP OO
- Generating and viewing the information available from the outcomes of flow runs

The Central Help system is also available as a PDF document in the HP OO home directory, in the \Central\docs subdirectory.

- Help for Studio

Studio Help instructs flow authors at varying levels of programming ability.

The Studio Help system is also available as a PDF document in the HP OO home directory, in the \Studio\docs subdirectory.

- Animated tutorials for Central and Studio

HP OO tutorials can each be completed in less than half an hour and provide basic instruction on the following:

- In Central, finding, running, and viewing information from flows
- In Studio, modifying flows

The tutorials are available in the Central and Studio subdirectories of the HP OO home directory.

- Self-documentation for operations and flows in the Accelerator Packs and ITIL folders

Self-documentation is available in the descriptions of the operations and steps that are included in the flows.

# Support

For support information, including patches, troubleshooting aids, support contract management, product manuals and more, visit the following site:

- <http://support.openview.hp.com>

# Table of Contents

Warranty .....	ii
Restricted Rights Legend .....	ii
Trademark Notices .....	ii
Finding or updating documentation on the Web.....	iii
Where to Find Help, Tutorials, and More .....	iii
Support .....	iv
This Guide.....	1
Using Single Sign-on.....	1
Using this document – procedures for enabling SSO.....	1
Enabling SSO with network load balancing.....	2
Providing group membership for the logged-in user.....	2
Enabling SSO for Central .....	2
Enabling SSO for the web browser.....	2
Enabling SSO for Central – Windows AD.....	3
Enabling SSO for Central – MIT KDC.....	6
Enabling SSO for the Java Flow Invoke tool .....	7
Enabling SSO for the Java Flow Invoke tool – Windows AD.....	7
Enabling SSO for the Java Flow Invoke tool – MIT KDC.....	11
Index .....	15

# This Guide

This Guide is intended for customers, Hewlett-Packard Software Systems Engineers (SEs), and Customer Engineers (CEs) who have installed or are deploying Operations Orchestration 7.20. The material here assumes that the reader is familiar with Kerberos fundamentals – that is, with terms such as principal, ticket, realm, KDC and keytab.

## Using Single Sign-on

You can obtain security and performance benefits by configuring Central so that the credentials of the person who is already logged on the machine are provided as login credentials in several situations:

- For Central, when Central is run on one of the following systems:
  - The Web browser is Internet Explorer or Firefox, on a machine running the Windows operating system.
  - The Web browser is Firefox, on a machine running Linux.
- For flows that are started from the Java version of the flow invocation tool (JRSFlowInvoke.jar).
- In either of the above uses, when a network load balancing cluster has been installed for Central. This feature is called *single sign-on (SSO)*.

**Note:** SSO support in Central works with any compliant Kerberos 5 implementation. The procedures for enabling single sign-on for Central vary depending on whether Central uses a Linux key distribution center (KDC) or a Windows KDC (Active Directory, which supports the Kerberos 5 specification).

## Using this document – procedures for enabling SSO

The following list is your guide to the procedures in this document for enabling SSO on Central and/or for use with the Java Flow Invoke tool. (Note that enabling SSO for Central completes some of the steps needed to enable SSO for the Java Flow Invoke tool.)

8. Provide HP OO group membership for the logged-in user and enable SSO for the web browser, as described in [Providing group membership for the logged-in user](#).
9. To enable and configure SSO for Central:
  - a. Enable SSO for the web browser, as described in [Enabling SSO for the web browser](#).
  - b. Complete one of the following sections, depending on whether you are authenticating with Windows Active Directory (AD) or MIT KDC:
    - [Enabling SSO for Central – Windows AD](#)
    - [Enabling SSO for Central – MIT KDC](#)
10. To enable and configure SSO for use with the Java Flow Invoke tool, complete one of the following sections, depending on whether you are authenticating with AD or MIT KDC:
  - [Enabling SSO for the Java Flow Invoke tool – Windows AD](#)
  - [Enabling SSO for the Java Flow Invoke tool – MIT KDC](#)

The alternative procedures for enabling SSO on with a Linux KDC or a Windows KDC are documented in each section, on enabling SSO for Central or for use of the Java Flow Invoke tool.

## Enabling SSO with network load balancing

The procedures for enabling SSO when a network load balancer (NLB) fronts Central are the same as without an NLB, except for the following:

- Generate the service principal and keytab files for the machine on which the NLB is installed and not for the individual Central nodes behind the load balancer.

For example, suppose that:

- The NLB machine is `nlb.mydomain.com`
- There are two Central nodes behind the load balancer: `central1.mydomain.com` and `central2.mydomain.com`

In this case, the service principal would be `HTTP/nlb.mydomain.com@MYDOMAIN.COM` (if Windows AD is used, the AD user account would be `HTTP/nlb.mydomain.com`), and the keytab file would be `nlb.keytab`.

- Copy the keytab to `central1.mydomain.com` and `central2.mydomain.com`.
- Modify the respective entries in `jaasLogin.conf` on those machines to point to `keytab=nlb.keytab` and `principal=HTTP/nlb.mydomain.com@MYDOMAIN.COM`
- If you are using SSO with the Java Flow Invoke tool, the SSO flow invocation script that you call must point to `nlb.<domain>.com`, as in the following:

```
sso_invoke nlb.mydomain.com:<port_number>/Library/MyFlows/myFlow
```

where `<port_number>` is the port on which the network load balancer is listening.

These differences are folded into the following procedures.

## Providing group membership for the logged-in user

Group membership for SSO is confirmed by Kerberos. As a result, use of AD has both an LDAP aspect and a Kerberos aspect. Enabling SSO for AD logins therefore requires configuration of elements such as a keytab and the `krb5.conf` file, even if the Kerberos provider is not enabled on the Central **Administration** tab.

However, HP OO does not obtain a user's groups from his or her AD/Kerberos ticket. Therefore, for each user whose login credentials are used in SSO, the administrator must do one of the following:

- Create a default group with at least one member for the Kerberos provider.

In most cases, this is not recommended.

- Explicitly define an external account and assign its members to an internal HP OO group.

For example, for SSO to work for the MYDOMAIN user `jdoh`, the HP OO administrator should define the external account `MYDOMAIN\jdoh` and assign this account to at least one internal group.

## Enabling SSO for Central

To enable SSO for Central, you enable SSO for the web browser, then for Central.

### Enabling SSO for the web browser

Whether you use Internet Explorer or Firefox, Windows or Linux, it is necessary to enable SSO for your web browser.

## To enable SSO for Internet Explorer 6.x or 7.x

- On MSDN, follow the directions on <http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnsecure/html/http-ss0-1.asp>.

## To enable SSO for Firefox 2.x

1. Open the browser, and type the following in the address bar and press ENTER:  
**about:config**
2. Scroll down to locate the property **network.negotiate-auth.delegation-uris** and set it to the following:  
**.mydomain.ad**  
This sets a URL pattern for the sites that are allowed to use SSO.
3. Set the same pattern for the property **network.negotiate-auth.trusted-uris**.
4. On a Linux system, you may also need to set the property **network.negotiate-auth.gsslib** to **false**.
5. Locate and open the WEB-INF/applicationContext.xml file.
6. In the file, in the authenticationEntryPoint bean, locate and replace  
`/static/Login.htm`  
with  
`/static/SSOLogin.htm"`
7. Restart Central.
8. Login as a domain user for the domain the Central is in (MYDOMAIN in these examples) and open a Web browser that has had SSO enabled.  
**Note:** This must be a different machine from the Central server. SSO will not work on that machine.
9. To test SSO, try to navigate to any HP OO URL (such as OO/app), using the fully qualified machine name (coast.mydomain.ad) to exactly match the machine-name part of the service account `HTTP/coast.mydomain.ad@MYDOMAIN.AD`.  
For example, <https://coast.mydomain.ad:8443/PAS/app>.

If SSO works for the user, the user will be able to open Central without being prompted for credentials. If the SSO login fails for some reason (such as misconfiguration, or lack of access for the user due to a disabled account, or lack of group membership), the standard login (username/password) dialog appears.

## Enabling SSO for Central – Windows AD

To track an example through the following procedure, we'll assume the following:

- Central (either Windows or Linux) is located at coast.mydomain.com
- The Windows AD domain controller is at mydomain.com
- The realm is MYDOMAIN.COM (note that for Windows AD, the realm name is usually the domain name, upper-cased).
- The account for which SSO is attempted is "jdoe".
- The HP OO home directory is represented as "OO\_HOME" in discussion and in commands.

## To enable single sign-on for Central, using Windows AD

1. Add an AD account for the host (the Central server that the Java flow invocation tool will point at when running the flows). The account must have the following format:  
`HTTP/<server_name.domain_name>`



It is advisable to configure this AD account with the settings "Password never expires" and "Use DES encryption types for this account".

If you do not set DES encryption types for the account, AD uses the RC4-HMAC encryption type. Using our example, the account that you add would be:

HTTP/coast.mydomain.com

2. On the domain controller machine, open a command-line window and generate a keytab file, using the following command:

```
ktpass -out <server_name>.keytab -princ  
<service_name>/<server_name.domain_name>@<REALM_NAME> -mapuser  
<service_name>/<server_name.domain_name> -pass *** -crypto DES-CBC-MD5 -ptype  
KRB5_NT_PRINCIPAL
```

where:

\*\*\* is the password that you specified when you created the above AD account.

In our example, this command would look like this:

```
ktpass -out coast.keytab -princ HTTP/coast.mydomain.com@MYDOMAIN.COM -mapuser  
HTTP/coast.mydomain.com -pass *** -crypto DES-CBC-MD5 -ptype KRB5_NT_PRINCIPAL
```

**Note for using a load balancer:** In this step, generate the service principal and keytab file for the NLB machine instead of for the Central nodes in the cluster. Using our example, the command would be:

```
ktpass -out nlb.keytab -princ HTTP/nlb.mydomain.com@MYDOMAIN.COM -mapuser  
HTTP/nlb.mydomain.com -pass *** -crypto DES-CBC-MD5 -ptype KRB5_NT_PRINCIPAL
```

3. Copy the keytab file (coast.keytab in our example) to the Central server, into OO\_HOME/Central/conf directory.

**Note for using a load balancer:** In this step, in our NLB example, the keytab file would be nlb.keytab, and you would copy this keytab file to OO\_HOME/Central/conf on each of the Central nodes, central1.mydomain.com and central2.mydomain.com.

4. Open OO\_HOME/Central/conf/jaasLogin.conf in a text editor.

**Note for using a load balancer:** In this step, in our NLB example, you open jaasLogin.conf on each of the Central nodes, central1.mydomain.com and central2.mydomain.com.

5. In jaasLogin.conf, add the following "com.sun.security.jgss.accept" section after the DharmaKrb5JAAS section, replacing OO\_HOME in the highlighted section with the correct path:

```
DharmaKrb5JAAS {  
    com.sun.security.auth.module.Krb5LoginModule required  
        refreshKrb5Config=true;  
};
```

```
com.sun.security.jgss.accept {  
    com.sun.security.auth.module.Krb5LoginModule  
        required  
        storeKey=true  
        doNotPrompt=true  
        useKeyTab=true  
        kdc=mydomain.com  
        keyTab="OO_HOME/Central/conf/coast.keytab"  
        realm="MYDOMAIN.COM"  
        principal="HTTP/coast.mydomain.com@MYDOMAIN.COM"  
        debug=true;
```

```
};
```

**Note for using a load balancer:** In this step, in our NLB example, in each copy of jaasLogin.conf:

- The keytab to point to is nlb.keytab.
  - The principal is [HTTP/nlb.mydomain.com@MYDOMAIN.COM](#)
6. In Central/conf, create a krb5.conf file that includes definition of the default realm and KDC (or make sure that the existing krb5.conf includes that information).

In our example, a minimal krb5.conf file would look like this:

```
[libdefaults]
    default_realm = MYDOMAIN.COM
    ticket_lifetime = 24000

[realms]
    MYDOMAIN.COM = {
        kdc = mydomain.com
        admin_server = mydomain.com
        default_domain = .mydomain.com
    }
```

```
[domain_realm]
    .mydomain.com = MYDOMAIN.COM
    mydomain.com = MYDOMAIN.COM
```

```
[pam]
    debug = true
```

7. Log in to Central and, on the **Administration** tab, click the **System Configuration** subtab.
8. Scroll down to **Kerberos Authentication Settings** and configure the location for the Kerberos 5 configuration file (krb5.conf) to point to "/Central/conf/krb5.conf".

**Notes:**

- Do not set a realm or a KDC on that page, because Central will now obtain them from the krb5.conf file.
  - You do not need to enable Kerberos authentication unless that is used for logging in.
9. If Central is a Windows version hosted on a Windows 2000/2003 system, add the following registry key:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\Kerberos\Parameters
Value Name: allowtgtsessionkey
Value Type: REG_DWORD
Value: 0x01
```

It is necessary to enable delegation for the AD service account (HTTP/coast.battleground.ad in the example) so that flows using the logged-in user's credentials to authenticate with the logged-in Kerberos ticket.

10. To enable delegation for the AD service account:
- a. Open the properties for AD service (HTTP/coast.battleground.ad) account.
  - b. On the **Delegation** tab, select **Trust this user for delegation to any service (Kerberos only)**.

## Enabling SSO for Central – MIT KDC

**Note:** The following procedure assumes that the system uses a Linux version of MIT KDC.

To track an example through the following procedure, we'll assume the following:

- Central (either Windows or Linux) is located at fitzroy.mydomain.com
- KDC is at kdc.mydomain.com
- The realm is MYDOMAIN.COM.
- The account for which SSO is attempted is "jdoe".
- The HP OO home directory is represented as "OO\_HOME" in discussion and in commands.

### To enable single sign-on using MIT KDC

1. On the KDC machine, add a service principal for *HTTP/fitzroy.mydomain.com@MYDOMAIN.COM* using the kadmin's `addprinc` command (for information on using kadmin, see the man pages for kadmin):

```
kadmin: addprinc -randkey HTTP/fitzroy.mydomain.com@MYDOMAIN.COM
```

2. Export the principal you just created to fitzroy.keytab:

```
kadmin: ktadd -k fitzroy.keytab HTTP/fitzroy.mydomain.com
```

**Note for using a load balancer:** In this step, generate the service principal and keytab file for the NLB machine instead of for the Central nodes in the cluster. Using our example, the command would be:

```
ktpass -out nlb.keytab -princ HTTP/nlb.mydomain.com@MYDOMAIN.COM -mapuser  
HTTP/nlb.mydomain.com -pass *** -crypto DES-CBC-MD5 -ptype KRB5_NT_PRINCIPAL
```

3. Copy the keytab file to the Central machine at OO\_HOME/Central/conf

**Note for using a load balancer:** In this step, in our NLB example, the keytab file would be nlb.keytab, and you would copy this keytab file to OO\_HOME/Central/conf on each of the Central nodes, central1.mydomain.com and central2.mydomain.com.

4. In Central/conf, create a krb5.conf file that includes definition of the default realm and KDC (or make sure that the existing krb5.conf includes that information).

In our example, a minimal krb5.conf file would look like this:

```
[libdefaults]  
    default_realm = MYDOMAIN.COM  
    ticket_lifetime = 24000  
    default_tkt_enctypes = des3-cbc-sha1
```

```
[realms]  
    MYDOMAIN.COM = {  
        kdc = kdc.mydomain.com  
        admin_server = kdc.mydomain.com  
        default_domain = mydomain.com  
    }
```

```
[domain_realm]  
    .mydomain.com = MYDOMAIN.COM  
    mydomain.com = MYDOMAIN.COM
```

```
[pam]
```

```
debug = true
```

5. Open /Central/conf/jaasLogin.conf in a text editor.

**Note for using a load balancer:** In this step, in our NLB example, you open jaasLogin.conf on each of the Central nodes, central1.mydomain.com and central2.mydomain.com.

6. Add the following "com.sun.security.jgss.accept" section after the DharmaKrb5JAAS section, replacing OO\_HOME with the correct path:

```
DharmaKrb5JAAS {
    com.sun.security.auth.module.Krb5LoginModule required
        refreshKrb5Config=true;
};

com.sun.security.jgss.accept {
    com.sun.security.auth.module.Krb5LoginModule
        required
        storeKey=true
        doNotPrompt=true
        useKeyTab=true
        kdc=kdc.mydomain.com
        keyTab="OO_HOME/Central/conf/fitzroy.keytab"
        realm="MYDOMAIN.COM"
        principal="HTTP/fitzroy.mydomain.com@MYDOMAIN.COM"
        debug=true;
};
```

**Note for using a load balancer:** In this step, in our NLB example, in each copy of jaasLogin.conf, the keytab to point to is nlb.keytab and the principal is [HTTP/nlb.mydomain.com@MYDOMAIN.COM](http://nlb.mydomain.com@MYDOMAIN.COM).

7. Log in to Central and on the **Administration** tab, click the **System Configuration** subtab.
8. If the SSO java invocation is from a Linux machine that is not configured to obtain Kerberos tickets automatically, obtain a forwardable ticket from the Windows domain controller (you might have to change /etc/krb5.conf to point it to the Windows domain controller), using a command like the following:

```
kinit -f jdoe@MYDOMAIN.COM
```

9. If Central is a Windows version hosted on a Windows 2000/2003 system, add the following registry key:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\Kerberos\Parameters
Value Name: allowtgtsessionkey
Value Type: REG_DWORD
Value: 0x01
```

## Enabling SSO for the Java Flow Invoke tool

### Enabling SSO for the Java Flow Invoke tool – Windows AD

To track an example through the following procedure, we'll assume the following:

- Central (either Windows or Linux) is located at coast.mydomain.com
- The Windows AD domain controller is at mydomain.com

- The realm is MYDOMAIN.COM (note that for Windows AD, the realm name is usually the domain name, upper-cased).
- The account for which SSO is attempted is "jdoe".
- The HP OO home directory is represented as "OO\_HOME" in discussion and in commands.

## To enable single sign-on using Windows AD

1. Add an AD account for the host (the Central server that the Java flow invocation tool will point at when running the flows). The account must have the following format:

```
HTTP/<server_name.domain_name>
```

It is advisable to configure this AD account with the settings "Password never expires" and "Use DES encryption types for this account".

If you do not set DES encryption types for the account, AD uses the RC4-HMAC encryption type.

Using our example, the account that you add would be:

```
HTTP/coast.mydomain.com
```

2. On the domain controller machine, open a command-line window and generate a keytab file, using the following command:

```
ktpass -out <server_name>.keytab -princ
<service_name>/<server_name.domain_name>@<REALM_NAME> -mapuser
<service_name>/<server_name.domain_name> -pass *** -crypto DES-CBC-MD5 -ptype
KRB5_NT_PRINCIPAL
```

where:

\*\*\* is the password that you specified when you created the above AD account.

In our example, this command would look like this:

```
ktpass -out coast.keytab -princ HTTP/coast.mydomain.com@MYDOMAIN.COM -mapuser
HTTP/coast.mydomain.com -pass *** -crypto DES-CBC-MD5 -ptype KRB5_NT_PRINCIPAL
```

**Note for using a load balancer:** In this step, generate the service principal and keytab file for the NLB machine instead of for the Central nodes in the cluster. Using our example, the command would be:

```
ktpass -out nlb.keytab -princ HTTP/nlb.mydomain.com@MYDOMAIN.COM -mapuser
HTTP/nlb.mydomain.com -pass *** -crypto DES-CBC-MD5 -ptype KRB5_NT_PRINCIPAL
```

3. Copy the keytab file (coast.keytab in our example) to the Central server, into OO\_HOME/Central/conf directory.

**Note for using a load balancer:** In this step, in our NLB example, the keytab file would be nlb.keytab, and you would copy this keytab file to OO\_HOME/Central/conf on each of the Central nodes, central1.mydomain.com and central2.mydomain.com.

4. In Central/conf, create a krb5.conf file that includes definition of the default realm and KDC (or make sure that the existing krb5.conf includes that information).

In our example, a minimal krb5.conf file would look like this:

```
[libdefaults]
    default_realm = MYDOMAIN.COM
    ticket_lifetime = 24000
```

```
[realms]
    MYDOMAIN.COM = {
        kdc = mydomain.com
        admin_server = mydomain.com
```

```
    default_domain = .mydomain.com
}
```

```
[domain_realm]
    .mydomain.com = MYDOMAIN.COM
    mydomain.com = MYDOMAIN.COM
```

```
[pam]
    debug = true
```

5. Open OO\_HOME/Central/conf/jaasLogin.conf in a text editor.

**Note for using a load balancer:** In this step, in our NLB example, you open jaasLogin.conf on each of the Central nodes, central1.mydomain.com and central2.mydomain.com.

6. Add the following "com.sun.security.jgss.accept" section after the DharmaKrb5JAAS section, replacing OO\_HOME in the highlighted section with the correct path:

```
DharmaKrb5JAAS {
    com.sun.security.auth.module.Krb5LoginModule required
        refreshKrb5Config=true;
};
```

```
com.sun.security.jgss.accept {
    com.sun.security.auth.module.Krb5LoginModule
        required
        storeKey=true
        doNotPrompt=true
        useKeyTab=true
        kdc=mydomain.com
        keyTab="OO_HOME/Central/conf/coast.keytab"
        realm="MYDOMAIN.COM"
        principal="HTTP/coast.mydomain.com@MYDOMAIN.COM"
        debug=true;
};
```

**Note for using a load balancer:** In this step, in our NLB example, in each copy of jaasLogin.conf, the keytab to point to is nlb.keytab and the principal is [HTTP/nlb.mydomain.com@MYDOMAIN.COM](http://nlb.mydomain.com@MYDOMAIN.COM).

7. Log in to Central and, on the **Administration** tab, click the **System Configuration** subtab.
8. Scroll down to **Kerberos Authentication Settings** and configure the location for the Kerberos 5 configuration file (krb5.conf) to point to "/Central/conf/krb5.conf".

**Notes:**

- Do not set a realm or a KDC on that page, because Central will now obtain them from the krb5.conf file.
  - You do not need to enable Kerberos authentication unless that is used for logging in.
9. Save your changes, and then restart Central.

By default, under OO\_HOME/Central/tools (where the java flow invocation tool JRSFlowInvoke.jar is installed) there is an sso\_invoke\_krb5.conf.sample file that looks like the following:

```
[libdefaults]
    default_realm = MYDOMAIN.COM
    ticket_lifetime = 24000
```

```
[realms]
    MYDOMAIN.COM = {
        kdc = mydomain.com
        admin_server = mydomain.com
        default_domain = .mydomain.com
    }
```

```
[domain_realm]
    .mydomain.com = MYDOMAIN.COM
    mydomain.com = MYDOMAIN.COM
```

```
[pam]
    debug = true
```

10. Copy `sso_invoke_krb5.conf.sample` to `sso_invoke_krb5.conf` and edit the latter to match your domain, realm, and KDC.

By default, under `OO_HOME/Central/tools` there is an `sso_invoke.bat` file for the Windows Central version (or `sso_invoke.sh` for the Linux Central version) that shows how to use the java flow invocation tool in single sign-on mode. You can run those shell scripts from that location. Or, if the invocation tool is to be used from a different machine than the Central server, copy the `JRSFlowInvoke.jar`, `sso_invoke.bat` (or `sso_invoke.sh`), and `sso_invoke_krb5.conf` files to that machine and adjust the paths (including the path to JRE 1.6, which is required on the target machine—you can obtain JRE 1.6 from the downloads page of the Java site, <http://java.sun.com/>).

You can invoke the shell scripts with a command such as the following:

```
sso_invoke coast.mydomain.com:8443 /Library/MyFlows/myFlow
```

**Note for using a load balancer:** In the SSO flow invocation script that you call must point to `nlb.<domain>.com`, as in the following:

```
sso_invoke nlb.mydomain.com:<port_number>/Library/MyFlows/myFlow
```

where `<port_number>` is the port on which the network load balancer is listening.

11. Log in to Central with an account that has Administrator rights.  
Next, you will need to give `HEADLESS_FLOWS` capability to the SSO users.
12. The easiest way to give `HEADLESS_FLOWS` capability to the SSO users is:
  - a. In Central, on the **Administration** tab, click the **System Configuration** sub-tab.
  - b. Scroll to the Kerberos section and set the default group to a group that has `HEADLESS_FLOWS` capability.

This way, any headless invocation using SSO will have the capabilities of that group (flows cannot be invoked using the headless tool unless the user under whose credentials the invocation happens, has `HEADLESS_FLOWS` capability).

Or, if SSO flow invocations need to be controlled on a user-by-user basis:

- On the **Administration** tab, create the Central user that matches the account under which the SSO flow invocation will happen (“jdoe” in our example) and specify that it is an external user.

For information on how to create a user and specify that it is an external user, see Help for Central.

The user must be a member of a group that has `HEADLESS_FLOWS` capability; without this capability, the user will not be able to start runs using SSO flow invocation.

In addition to having the HEADLESS\_FLOWS capability, the user under whose credentials the SSO flow invocation happens must have **read** and **execute** permissions for the flow and the operations that the flow uses. For more information on granting permissions to flows and operations see Help for Studio.

13. If the SSO java invocation is from a Linux machine that is not configured to obtain Kerberos tickets automatically, obtain a forwardable ticket from the Windows domain controller (you might have to change /etc/krb5.conf to point it to the Windows domain controller), using a command like the following:

```
kinit -f jdoe@MYDOMAIN.COM
```

14. If Central is a Windows version hosted on a Windows 2000/2003 system, add the following registry key:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\Kerberos\Parameters
```

```
Value Name: allowtgtsessionkey
```

```
Value Type: REG_DWORD
```

```
Value: 0x01
```

15. If the machine from which the java invocation tool is invoked uses Windows 2000/2003, add the same registry key (described in the preceding step) on that machine.

## Enabling SSO for the Java Flow Invoke tool – MIT KDC

The following procedure assumes that the system uses a Linux version of MIT KDC.

To track an example through the following procedure, we'll assume the following:

- Central (either Windows or Linux) is located at fitzroy.mydomain.com
- KDC is at kdc.mydomain.com
- The realm is MYDOMAIN.COM.
- The account for which SSO is attempted is "jdoe".
- The HP OO home directory is represented as "OO\_HOME" in discussion and in commands.

### To enable single sign-on using MIT KDC

1. On the KDC machine, add a service principal for [HTTP/fitzroy.mydomain.com@MYDOMAIN.COM](http://fitzroy.mydomain.com@MYDOMAIN.COM) using the kadmin's `addprinc` command (for information on using kadmin, see the man pages for kadmin):

```
kadmin: addprinc -randkey HTTP/fitzroy.mydomain.com@MYDOMAIN.COM
```

**Note for using a load balancer:** In this step, generate the service principal for the NLB machine instead of for the Central nodes in the cluster. Using our example, the command would be:

```
kadmin: addprinc -randkey HTTP/nlb.mydomain.com@MYDOMAIN.COM
```

2. Export the principal you just created to fitzroy.keytab:

```
kadmin: ktadd -k fitzroy.keytab HTTP/fitzroy.mydomain.com
```

**Note for using a load balancer:** In this step, export the service principal to the keytab file for the NLB machine instead of for the Central nodes in the cluster. Using our example, the command would be:

```
kadmin: ktadd -k nlb.keytab HTTP/nlb.mydomain.com
```

3. Copy the keytab file to the Central machine at OO\_HOME/Central/conf

**Note for using a load balancer:** In this step, in our NLB example, the keytab file would be nlb.keytab, and you would copy this keytab file to OO\_HOME/Central/conf on each of the Central nodes, central1.mydomain.com and central2.mydomain.com.



4. In Central/conf, create a krb5.conf file that includes definition of the default realm and KDC (or make sure that the existing krb5.conf includes that information).

In our example, a minimal krb5.conf file would look like this:

```
[libdefaults]
    default_realm = MYDOMAIN.COM
    ticket_lifetime = 24000
    default_tkt_enctypes = des3-cbc-sha1

[realms]
    MYDOMAIN.COM = {
        kdc = kdc.mydomain.com
        admin_server = kdc.mydomain.com
        default_domain = mydomain.com
    }

[domain_realm]
    .mydomain.com = MYDOMAIN.COM
    mydomain.com = MYDOMAIN.COM
```

```
[pam]
    debug = true
```

5. Open /Central/conf/jaasLogin.conf in a text editor.

**Note for using a load balancer:** In this step, in our NLB example, you open jaasLogin.conf on each of the Central nodes, central1.mydomain.com and central2.mydomain.com.

6. Add the following "com.sun.security.jgss.accept" section after the DharmaKrb5JAAS section, replacing OO\_HOME with the correct path:

```
DharmaKrb5JAAS {
    com.sun.security.auth.module.Krb5LoginModule required
        refreshKrb5Config=true;
};

com.sun.security.jgss.accept {
    com.sun.security.auth.module.Krb5LoginModule
        required
        storeKey=true
        doNotPrompt=true
        useKeyTab=true
        kdc=kdc.mydomain.com
        keyTab="OO_HOME/Central/conf/fitzroy.keytab"
        realm="MYDOMAIN.COM"
        principal="HTTP/fitzroy.mydomain.com@MYDOMAIN.COM"
        debug=true;
};
```

**Note for using a load balancer:** In this step, in our NLB example, in each copy of jaasLogin.conf, the keytab to point to is nlb.keytab and the principal is [HTTP/nlb.mydomain.com@MYDOMAIN.COM](http://nlb.mydomain.com@MYDOMAIN.COM).

7. Log in to Central and on the **Administration** tab, click the **System Configuration** subtab.

8. Scroll down to **Kerberos Authentication Settings** and configure the location for the Kerberos 5 configuration file (krb5.conf) to point to "/Central/conf/krb5.conf".

**Notes:**

- Do not set a realm or a KDC on that page, because Central will now obtain them from the krb5.conf file.
  - You do not need to enable Kerberos authentication unless that is used for logging in.
9. Save your changes, and then restart Central.

By default, under OO\_HOME/tools (where the java flow invocation tool JRSFlowInvoke.jar, is by default installed) there is an sso\_invoke\_krb5.conf.sample file that looks like:

```
[libdefaults]
    default_realm = MYDOMAIN.COM
    ticket_lifetime = 24000
    default_tkt_enctypes = des3-cbc-shal

[realms]
    MYDOMAIN.COM = {
        kdc = mydomain.com
        admin_server = mydomain.com
        default_domain = .mydomain.com
    }

[domain_realm]
    .mydomain.com = MYDOMAIN.COM
    mydomain.com = MYDOMAIN.COM

[pam]
    debug = true
```

10. Copy sso\_invoke\_krb5.conf.sample to sso\_invoke\_krb5.conf and edit the latter to match your domain, realm and KDC.

By default, under OO\_HOME/tools there is an sso\_invoke.bat file for the Windows Central version (or sso\_invoke.sh for the Linux Central version) that shows how to use the java flow invocation tool in single sign-on mode. You can run those shell scripts from that location. Or, if the invocation tool is to be used from a different machine than the Central server, copy the JRSFlowInvoke.jar, sso\_invoke.bat (or sso\_invoke.sh), and sso\_invoke\_krb5.conf files to that machine and adjust the paths (including the path to JRE 1.6, which is required on the target machine—you can obtain JRE 1.6 from the downloads page of the Java site, <http://java.sun.com/>).

The shell scripts can be invoked with a command such as in the following:

```
sso_invoke fitzroy.mydomain.com:8443 /Library/MyFlows/myFlow
```

**Note for using a load balancer:** In the SSO flow invocation script that you call must point to nlb.<domain>.com, as in the following:

```
sso_invoke nlb.mydomain.com:<port_number>/Library/MyFlows/myFlow
```

where <port\_number> is the port on which the network load balancer is listening.

11. Log in to Central with an account that has Administrator rights.  
Next, you will need to give HEADLESS\_FLOWS capability to the SSO users.
12. The easiest way to give HEADLESS\_FLOWS capability to the SSO users is:
  - a. In Central, on the **Administration** tab, click the **System Configuration** sub-tab.

- b. Scroll to the Kerberos section and set the default group to a group that has HEADLESS\_FLOWS capability.

This way, any headless invocation using SSO will have the capabilities of that group (flows cannot be invoked using the headless tool unless the user under whose credentials the invocation happens, has HEADLESS\_FLOWS capability).

Or, if SSO flow invocations need to be controlled on a user-by-user basis:

- On the **Administration** tab, create the Central user that matches the account under which the SSO flow invocation will happen ("jdoe" in our example) and specify that it is an external user.

For information on how to create a user and specify that it is an external user, see Help for Central.

The user must be a member of a group that has HEADLESS\_FLOWS capability; without this capability, the user will not be able to start runs using SSO flow invocation.

In addition to having the HEADLESS\_FLOWS capability, the user under whose credentials the SSO flow invocation happens must have **read** and **execute** permissions for the flow and the operations that the flow uses. For more information on granting permissions to flows and operations see Help for Studio.

13. If the SSO flow invocation is from a Linux machine that is not configured to obtain Kerberos tickets automatically, obtain a forward-able ticket from the KDC (you might have to change /etc/krb5.conf to point it to the kdc.mydomain.com in our example), using a command like the following:

```
kinit -f jdoe@MYDOMAIN.COM
```

14. If the SSO flow invocation is from a Windows machine, a forward-able ticket needs to be obtained from the Linux MIT KDC. This can be done by using kinit executable under OO\_HOME/jre1.6/bin.

15. If the SSO flow invocation is from a Windows 2000/2003 system, add the following registry key:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\Kerberos\Parameters  
Value Name: allowtgtsessionkey  
Value Type: REG_DWORD  
Value: 0x01
```

# Index

- copyright notices, ii
- enabling Single Sign-On
  - for Central, 3
  - for Central – MIT KDC, 6
  - for Central – Windows AD, 4
  - for the Java Flow Invoke tool, 8
  - for the Java Flow Invoke tool – MIT KDC, 12
  - for the Java Flow Invoke tool – Windows AD, 8
  - with network load balancing, 2
- group membership, providing for the logged-in user, 2
- Java Flow Invoke tool, enabling Single Sign-On for, 8
- legal notices, ii
  - copyright, ii
  - restricted rights, ii
  - trademark, ii
  - warranty, ii
- logged-in user, providing group membership for, 2
- network load balancing, enabling Single Sign-On with, 2
- restricted rights legend, ii
- Single Sign-On
  - enabling for Central – MIT KDC, 6
  - enabling for Central - Windows AD, 4
  - enabling for the Java Flow Invoke tool, 8
  - enabling for the Java Flow Invoke tool – MIT KDC, 12
  - enabling for the Java Flow Invoke tool – Windows AD, 8
  - enabling for the web browser, 3
  - enabling with network load balancing, 2
  - for Central, 3
  - procedures for enabling, 1
  - using, 1
- trademark notices, ii
- warranty, ii
- web browser, enabling Single Sign-On for, 3