

MOBILISER 5 INSTALLATION GUIDE

KEYSTORES

Project: Project Name

Document Status:

Release Date:

Document Version: 1.3

Date: 11 April 2013

Table of ContentS

[1 About this Document 3](#_Toc353453121)

[1.1 Purpose 3](#_Toc353453122)

[1.2 Revision History 3](#_Toc353453123)

[1.3 Reference Documents 3](#_Toc353453124)

[2 Introduction 4](#_Toc353453125)

[3 Mobiliser Release 5 Java SSL Setup 5](#_Toc353453126)

[3.1 Connectivity Overview 5](#_Toc353453127)

[3.2 Money Mobiliser 7](#_Toc353453128)

[3.3 Brand Mobiliser 8](#_Toc353453129)

[3.4 Mobiliser Internal Portals 10](#_Toc353453130)

[3.5 Mobiliser External Portals 12](#_Toc353453131)

[4 Apache HTTPD SSL Setup 14](#_Toc353453132)

[4.1 Connectivity Overview 14](#_Toc353453133)

[4.2 Money Mobiliser 15](#_Toc353453134)

[4.3 Brand Mobiliser 15](#_Toc353453135)

[4.4 Mobiliser Internal Portals 15](#_Toc353453136)

[4.5 Mobiliser External Portals 16](#_Toc353453137)

[4.6 Apache HTTPD SSL certificate creation 16](#_Toc353453138)

[4.7 Apache HTTPD SSL configuration 17](#_Toc353453139)

[5 Passwords 19](#_Toc353453140)

# About this Document

## Purpose

This document contains the part of keystores of the Mobiliser Release 5 Installation Guide.

## Revision History

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Version No. | Date | Author | Changes | Reviewed by | Signed off by |
| 1.0 | 2012-09-20 | Beppler | Document created |  |  |
| 1.1 | 2013-02-20 | Zey | Design changes |  |  |
| 1.2 | 2013-03-25 | Zey | Minor changes, Document released |  |  |
| 1.3 | 2013-04-11 | Beppler | Minor formatting changes |  |  |

## Reference Documents

|  |  |  |  |
| --- | --- | --- | --- |
| Document Name | Document Version No. | Document location | Purpose |
| Mobiliser 5 Installation Guide | 1.2 | Mobile B2C Document Library |  |
| Mobiliser 5 Installation Guide - Site Preparation Plan | 1.3 | Mobile B2C Document Library |  |
| Mobiliser 5 Installation Guide - Load Balancer | 1.3 | Mobile B2C Document Library |  |

# Introduction

After following the **Mobiliser Release 5 Installation Guide**, the system is up and running without encrypted communication between the components. Following this guide will create self-signed certificates for each internal system and import the certificates into the responsible keystore. During certificate creation, there are some passwords to be created.

**Do not use the same password twice!**

From a security perspective, it’s sufficient to use self-signed certificates for internal communication. The certificate which is accessible via a public network like the internet should be signed by a trusted third party or a companywide installed certification authority (CA). The webserver certificate setup is not part of this document.

# Mobiliser Release 5 Java SSL Setup

## Connectivity Overview

Internal communication between Mobiliser Release 5 components is done via HTTP or HTTPS.

Figure 1: Internal Communication shows simplified the internal communication between each Mobiliser component.



Figure 1: Internal Communication

The green arrows show the internal communication direction. This guide will enable HTTPS for each communication. The Java Keystore is global for any Java instance running within the Mobiliser environment. This means that Mobiliser Portals and Money Mobiliser on the Application servers share the same Java Keystore.

Each orange lock of Figure 2: Java Keystore Import represents a new created keystore. The cyan arrows show where the extracted **public** keys are stored. No private key will be exported. They will remain within the keystore.

The public certificates of Mobiliser Portals aren’t extracted in this chapter as the Mobiliser Portals aren’t destination endpoints of the internal communication.



Figure 2: Java Keystore Import

## Money Mobiliser

This section will provide the steps to create the self-signed certificate used in Money Mobiliser and will import the public certificate part in all necessary Java keystores.

1. Login to **van-aps-1** as user “sybase”.
2. Stop Money Mobiliser using user “sap-money”.

sudo -u sap-money /opt/sybase/money/bin/mobiliser.sh stop

1. Remove the old keystore which is delivered by default installation using user “sap-money”.

sudo -u sap-money rm /opt/sybase/money/conf/keys/server/keystore

1. Create a new /opt/sybase/money/conf/keys/server/keystore using user “sap-money”.

sudo -u sap-money /opt/sybase/java/current/bin/keytool -genkey -v -keystore /opt/sybase/money/conf/keys/server/keystore -alias money -keyalg RSA -keysize 2048 -validity 8000

This will lead to a similar output of the following, fill in appropriately:

Enter keystore password: *password1*  
Re-enter new password: *password1*What is your first and last name?  
 [Unknown]:  *van-aps-1*  
What is the name of your organizational unit?  
 [Unknown]: *Sybase 365*What is the name of your organization?  
 [Unknown]: *SAP*  
What is the name of your City or Locality?  
 [Unknown]: *Raunheim*What is the name of your State or Province?  
 [Unknown]: *Hessen*What is the two-letter country code for this unit?  
 [Unknown]: *DE*Is CN=van-aps-1, OU=Sybase 365, O=SAP, L=Raunheim, ST=Hessen, C=DE correct?  
 [no]: *yes*

Generating 2,048 bit RSA key pair and self-signed certificate (SHA1withRSA) with a validity of 9,999 days  
 for: CN=van-aps-1, OU=Sybase 365, O=SAP, L=Raunheim, ST=Hessen, C=DE  
Enter key password for <money>  
 (RETURN if same as keystore password): *password2*  
Re-enter new password: *password2*  
[Storing /opt/sybase/money/conf/keys/server/keystore]

1. Export this certificate to /tmp/money.cert using user “sap-money”.

sudo -u sap-money /opt/sybase/java/current/bin/keytool -exportcert -v -keystore /opt/sybase/money/conf/keys/server/keystore -alias money -file /tmp/money.cert

1. Import this certificate into Java keystore using user “sap-mob”.

sudo -u sap-mob /opt/sybase/java/current/bin/keytool -importcert -v -keystore /opt/sybase/java/current/jre/lib/security/cacerts -alias money -file /tmp/money.cert

This will lead to a similar output of the following, fill in appropriately:

Enter keystore password: changeit (this is the default Java keystore password)   
Owner: CN=, OU=Sybase 365, O=SAP, L=Raunheim, ST=Hessen, C=DE  
Issuer: CN=, OU=Sybase 365, O=SAP, L=Raunheim, ST=Hessen, C=DE  
Serial number: 5058f3d1  
Valid from: Wed Sep 19 00:21:05 CEST 2012 until: Fri Feb 03 23:21:05 CET 2040  
Certificate fingerprints:  
 MD5: B9:1F:A7:1C:85:32:41:60:66:93:BB:F2:01:5D:1E:E7  
 SHA1: AA:96:0F:F5:3C:81:AB:4D:DA:10:B3:96:4E:31:2E:C7:55:D0:D1:89  
 Signature algorithm name: SHA1withRSA  
 Version: 3  
Trust this certificate? [no]: yes  
Certificate was added to keystore  
[Storing /opt/sybase/java/current/jre/lib/security/cacerts]

1. Use “sap-money” to edit /opt/sybase/money/conf/cfgbackup/org.ops4j.pax.web.properties and adjust the values accordingy:

org.osgi.service.http.secure.enabled=true  
org.ops4j.pax.web.ssl.keystore=${mobiliser.home}/conf/keys/server/keystore  
org.ops4j.pax.web.ssl.password=*password1*  
org.ops4j.pax.web.ssl.keypassword=*password2*  
org.osgi.service.http.port.secure=8443

1. Copy the file /tmp/money.cert to **van-msg-1** and **van-web-1** using user “sybase”.

scp /tmp/money.cert sybase@:/tmp  
scp /tmp/money.cert sybase@:/tmp

1. **Repeat step 6** on **van-msg-1** and **van-web-1** to import the certificate accordingly.

## Brand Mobiliser

This section will provide the steps to create the self-signed certificate used in Brand Mobiliser and will import the public certificate part in all necessary Java keystores.

1. Login to **van-aps-1** as user “sybase”.
2. Stop Stop Brand Mobiliser using user “sap-brand”.

sudo -u sap-brand /opt/sybase/brand/run.sh stop

1. Create a new directory **/opt/sybase/brand/conf/keys/server** using user “sap-brand”:

sudo -u sap-brand mkdir -p /opt/sybase/brand/conf/keys/server

1. Create a new keystore **/opt/sybase/brand/conf/keys/server/keystore** using user “sap-brand”.

sudo -u sap-brand /opt/sybase/java/current/bin/keytool -genkey -v -keystore /opt/sybase/brand/conf/keys/server/keystore -alias brand -keyalg RSA -keysize 2048 -validity 8000

This will lead to a similar output of the following, fill in appropriately:

Enter keystore password: password3  
Re-enter new password: password3  
What is your first and last name?  
 [Unknown]: van-msg-1  
What is the name of your organizational unit?  
 [Unknown]: Sybase 365  
What is the name of your organization?  
 [Unknown]: SAP  
What is the name of your City or Locality?  
 [Unknown]: Raunheim  
What is the name of your State or Province?  
 [Unknown]: Hessen  
What is the two-letter country code for this unit?  
 [Unknown]: DE  
Is CN=van-msg-1, OU=Sybase 365, O=SAP, L=Raunheim, ST=Hessen, C=DE correct?  
 [no]: yes

Generating 2,048 bit RSA key pair and self-signed certificate (SHA1withRSA) with a validity of 9,999 days  
 for: CN=van-msg-1, OU=Sybase 365, O=SAP, L=Raunheim, ST=Hessen, C=DE

Enter key password for <money>  
 (RETURN if same as keystore password): password4  
Re-enter new password: password4  
[Storing /opt/sybase/brand/conf/keys/server/keystore]

1. Export this certificate to /tmp/brand.cert using user “sap-brand”.

sudo -u sap-brand /opt/sybase/java/current/bin/keytool -exportcert -v -keystore /opt/sybase/brand/conf/keys/server/keystore -alias brand -file /tmp/brand.cert

1. Import this certificate into Java keystore using user “sap-mob”.

sudo -u sap-mob /opt/sybase/java/current/bin/keytool -importcert -v -keystore /opt/sybase/java/current/jre/lib/security/cacerts -alias brand -file /tmp/brand.cert

This will lead to a similar output of the following, fill in appropriately:

Enter keystore password: changeit (this is the default Java keystore password)   
Owner: CN=, OU=Sybase 365, O=SAP, L=Raunheim, ST=Hessen, C=DE  
Issuer: CN=, OU=Sybase 365, O=SAP, L=Raunheim, ST=Hessen, C=DE  
Serial number: 5058f3d1  
Valid from: Wed Sep 19 00:21:05 CEST 2012 until: Fri Feb 03 23:21:05 CET 2040  
Certificate fingerprints:  
 MD5: B9:1F:A7:1C:85:32:41:60:66:93:BB:F2:01:5D:1E:E7  
 SHA1: AA:96:0F:F5:3C:81:AB:4D:DA:10:B3:96:4E:31:2E:C7:55:D0:D1:89  
 Signature algorithm name: SHA1withRSA  
 Version: 3  
Trust this certificate? [no]: yes  
Certificate was added to keystore  
[Storing /opt/sybase/java/current/jre/lib/security/cacerts]

1. Use “sap-brand” to edit /opt/sybase/brand/conf/cfgbackup/org.ops4j.pax.web.properties and adjust the values accordingly:

org.osgi.service.http.secure.enabled=true  
org.ops4j.pax.web.ssl.keystore=/opt/sybase/brand/conf/keys/server/keystore  
org.ops4j.pax.web.ssl.password=*password3*  
org.ops4j.pax.web.ssl.keypassword=*password4*  
org.osgi.service.http.port.secure=8444

1. Edit /opt/sybase/brand/conf/cfgbackup/service.mobiliser.plugin.properties and adjust the values accordingy using user “sap-brand”:

jaxbBaseUrl=https://van-aps-1:8443/mobiliser/services

1. Copy the file /tmp/brand.cert to **van-aps-1** using user “sybase”.  
   scp /tmp/brand.cert sybase@van-aps-1:/tmp
2. **Repeat step 6** on **van-aps-1** to import the certificate accordingly.

## Mobiliser Internal Portals

1. Login to **van-aps-1** as user “sybase”.
2. Stop Money Portals using user “sap-portal”.

sudo -u sap-portal /opt/sybase/portal/bin/catalina.sh stop

1. Create new directory /opt/sybase/portal/conf/keys/serverfor keystore using user “sap-portal”:

sudo -u sap-portal mkdir -p /opt/sybase/portal/conf/keys/server

1. Create a new keystore /opt/sybase/portal/conf/keys/server/keystoreusing user “sap-portal”.

sudo -u sap-portal /opt/sybase/java/current/bin/keytool -genkey -v -keystore /opt/sybase/portal/conf/keys/server/keystore -alias intportal -keyalg RSA -keysize 2048 -validity 8000

This will lead to a similar output of the following, fill in appropriately:

Enter keystore password: *password5*  
Re-enter new password: *password5*  
What is your first and last name?  
 [Unknown]: van-aps-1  
What is the name of your organizational unit?  
 [Unknown]: Sybase 365  
What is the name of your organization?  
 [Unknown]: SAP  
What is the name of your City or Locality?  
 [Unknown]: Raunheim  
What is the name of your State or Province?  
 [Unknown]: Hessen  
What is the two-letter country code for this unit?  
 [Unknown]: DE  
Is CN=van-aps-1, OU=Sybase 365, O=SAP, L=Raunheim, ST=Hessen, C=DE correct?  
 [no]: yes

Generating 2,048 bit RSA key pair and self-signed certificate (SHA1withRSA) with a validity of 9,999 days  
 for: CN=van-aps-1, OU=Sybase 365, O=SAP, L=Raunheim, ST=Hessen, C=DE  
Enter key password for <money>  
 (RETURN if same as keystore password): *password6*  
Re-enter new password: *password6*  
[Storing /opt/sybase/portal/conf/keys/server/keystore]

1. Export this certificate to /tmp/intportal.cert using user “sap-portal”.

sudo -u sap-portal /opt/sybase/java/current/bin/keytool -exportcert -v -keystore /opt/sybase/portal/conf/keys/server/keystore -alias intportal -file /tmp/intportal.cert

1. Use “sap-portal” to edit /opt/sybase/portal/conf/server.xml and adjust the values accordingly to the following table:

|  |
| --- |
| OLD |
| […]  <Connector port="8082" protocol="HTTP/1.1"  connectionTimeout="20000"  redirectPort="8443" /> […]  <!--  <Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true"  maxThreads="150" scheme="https" secure="true"  clientAuth="false" sslProtocol="TLS" />  --> […] <Connector port="8009" protocol="AJP/1.3" redirectPort="8443" /> […] |

|  |
| --- |
| NEW |
| […]  <Connector port="8082" protocol="HTTP/1.1"  connectionTimeout="20000"  redirectPort="8445" /> […]  ~~<!--~~  <Connector port="8445" protocol="HTTP/1.1" SSLEnabled="true"  maxThreads="150" scheme="https" secure="true"  keystoreFile="${catalina.home}/conf/keys/server/keystore"  keystorePass="*password5*" keyAlias="intportal"  keyPass="*password6*"  clientAuth="false" sslProtocol="TLS" />    ~~-->~~ […] <Connector port="8009" protocol="AJP/1.3" redirectPort="8445" /> […] |

1. Enable secure preferences by editing /opt/sybase/portal/conf/context.xml using user “sap-portal”:

prefss://mobiliser:secret@van-aps-1:8443/mobiliser/rest/prefs?pollInterval=60000&amp;clientType=json&amp;applicationIdentifier=presentationlayer

1. Copy the file /tmp/intportal.cert to **van-web-1** using user “sybase”.

scp /tmp/intportal.cert sybase@:/tmp

## Mobiliser External Portals

1. Login to **van-web-1** as user “sybase”.
2. Stop Money Portals using user “sap-portal”.

sudo -u sap-portal /opt/sybase/portal/bin/catalina.sh stop

1. Create new directory /opt/sybase/portal/conf/keys/serverfor keystore using user “sap-portal”:

sudo -u sap-portal mkdir -p /opt/sybase/portal/conf/keys/server

1. Create a new keystore /opt/sybase/portal/conf/keys/server/keystoreusing user “sap-portal”.

sudo -u sap-portal /opt/sybase/java/current/bin/keytool -genkey -v -keystore /opt/sybase/portal/conf/keys/server/keystore -alias extportal -keyalg RSA -keysize 2048 -validity 8000

This will lead to a similar output of the following, fill in appropriately:

Enter keystore password: *password7*  
Re-enter new password: *password7*  
What is your first and last name?  
 [Unknown]: van-web-1  
What is the name of your organizational unit?  
 [Unknown]: Sybase 365  
What is the name of your organization?  
 [Unknown]: SAP  
What is the name of your City or Locality?  
 [Unknown]: Raunheim  
What is the name of your State or Province?  
 [Unknown]: Hessen  
What is the two-letter country code for this unit?  
 [Unknown]: DE  
Is CN=, OU=Sybase 365, O=SAP, L=Raunheim, ST=Hessen, C=DE correct?  
 [no]: yes

Generating 2,048 bit RSA key pair and self-signed certificate (SHA1withRSA) with a validity of 9,999 days  
 for: CN=, OU=Sybase 365, O=SAP, L=Raunheim, ST=Hessen, C=DE  
Enter key password for <money>  
 (RETURN if same as keystore password): *password8*  
Re-enter new password: *password8*  
[Storing /opt/sybase/portal/conf/keys/server/keystore]

1. Export this certificate to /tmp/extportal.cert using user “sap-portal”.

sudo -u sap-portal /opt/sybase/java/current/bin/keytool -exportcert -v -keystore /opt/sybase/portal/conf/keys/server/keystore -alias extportal -file /tmp/extportal.cert

1. Edit /opt/sybase/portal/conf/server.xml and adjust the values accordingly to the following table using user “sap-portal”:

|  |
| --- |
| OLD |
| […]  <Connector port="8083" protocol="HTTP/1.1"  connectionTimeout="20000"  redirectPort="8443" /> […]  <!--  <Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true"  maxThreads="150" scheme="https" secure="true"  clientAuth="false" sslProtocol="TLS" />  --> […] <Connector port="8009" protocol="AJP/1.3" redirectPort="8443" /> […] |

|  |
| --- |
| NEW |
| […]  <Connector port="8083" protocol="HTTP/1.1"  connectionTimeout="20000"  redirectPort="8446" /> […]  ~~<!--~~  <Connector port="8446" protocol="HTTP/1.1" SSLEnabled="true"  maxThreads="150" scheme="https" secure="true"  keystoreFile="${catalina.home}/conf/keys/server/keystore"  keystorePass="*password7*" keyAlias="extportal"  keyPass="*password8*"  clientAuth="false" sslProtocol="TLS" />    ~~-->~~ […] <Connector port="8009" protocol="AJP/1.3" redirectPort="8446" /> […] |

1. Enable secure preferences by editing /opt/sybase/portal/conf/context.xml using user “sap-portal”:

prefss://mobiliser:secret@van-aps-1:8443/mobiliser/rest/prefs?pollInterval=60000&amp;clientType=json&amp;applicationIdentifier=presentationlayer

# Apache HTTPD SSL Setup

## Connectivity Overview

Communication between Apache HTTPD Web Server and the Mobiliser components that have to be reachable via the internet (or any other un-trusted network) is done via HTTP or HTTPS.

Figure 3: Apache HTTPD Communication shows simplified the internal communication between Apache HTTPD and each Mobiliser component.



Figure 3: Apache HTTPD Communication

The green arrows show the communication direction. This guide will enable HTTPS for each communication. The Keystore is global within the Apache HTTPD installation.

Each orange lock of Figure 4: Apache HTTPD Keystore Import represents one of the keystores created in chapter 3: Mobiliser Release 5 Java SSL Setup above. The cyan arrows show where the extracted **public** keys are stored. No private keys will be exported. They will still remain within the keystore.

The public certificates of Mobiliser Portals are used in this chapter as the Mobiliser Portals are accessed by Apache HTTPD.



Figure 4: Apache HTTPD Keystore Import

## Money Mobiliser

1. Login to **van-aps-1** as user “sybase”.
2. Export public certificates of Money Mobiliser as user “sap-money”.

sudo -u sap-money openssl x509 -inform der -in /tmp/money.cert -out /tmp/money.pem

1. Copy the public certificate of Money Mobiliser to Web server’s/tmp directory.

scp /tmp/money.cert sybase@:/tmp

## Brand Mobiliser

1. Login to **van-msg-1** as user “sybase”.
2. Export public certificates of Brand Mobiliser as user “sap-brand”.

sudo -u sap-brand openssl x509 -inform der -in /tmp/brand.cert -out /tmp/brand.pem

1. Copy the public certificate of Brand Mobiliser to Web Server’s /tmp directory.

scp /tmp/brand.cert sybase@:/tmp

## Mobiliser Internal Portals

1. Login to van-aps-1 as user “sybase”.
2. Export public certificates of Mobiliser Internal Portals as user “sap-portal”.

sudo -u sap-portal openssl x509 -inform der -in /tmp/intportal.cert -out /tmp/intportal.pem

1. Copy the public certificate of Brand Mobiliser to Web Server’s /tmp directory.

scp /tmp/intportal.cert sybase@:/tmp

## Mobiliser External Portals

1. Login to **van-web-1** as user “sybase”.
2. Export public certificates of Mobiliser Internal Portals as user “sap-portal”.

sudo -u sap-portal openssl x509 -inform der -in /tmp/extportal.cert -out /tmp/extportal.pem

## Apache HTTPD SSL certificate creation

1. Login to **van-web-1** as user “sybase”.
2. Create server key using user “sap-httpd”:

sudo -u sap-httpd openssl genrsa -out /opt/sybase/httpd/conf/certs/server.key 2048

1. Create Certification Request using user “sap-httpd”:

sudo -u sap-httpd openssl req -new -key /opt/sybase/httpd/conf/certs/server.key -out /opt/sybase/httpd/conf/certs/server.csr

You will get an output like the following:

Country Name (2 letter code) [XX]:DE  
State or Province Name (full name) []:Hessen  
Locality Name (eg, city) [Default City]:Raunheim  
Organization Name (eg, company) [Default Company Ltd]:Sybase 365  
Organizational Unit Name (eg, section) []:SAP  
Common Name (eg, your name or your server's hostname) []:**www.example.com**  
Email Address []:  
  
Please enter the following 'extra' attributes to be sent with your certificate request:  
  
A challenge password []:  
An optional company name []:

1. Sign the created CSR (instead of signing this yourself, you could pass it over to your CA) using user “sap-httpd”:

sudo -u sap-httpd openssl x509 -req -days 8000 -in /opt/sybase/httpd/conf/certs/server.csr -signkey /opt/sybase/httpd/conf/certs/server.key -out /opt/sybase/httpd/conf/certs/server.crt

## Apache HTTPD SSL configuration

1. Login to **van-web-1** as user “sybase”.
2. Bundle the exported certificates from previous chapters for usage by Apache HTTPD:

sudo -u sap-httpd cat /tmp/{money,brand,{int,ext}portal}.pem > /tmp/proxyca.crt  
sudo -u sap-httpd cp /tmp/proxyca.crt /opt/sybase/httpd/conf/certs/proxyca.crt

1. Copy the current configuration file port-1080.conf to port-1443.conf and edit it afterwards using user “sap-httpd”:

sudo -u sap-httpd cp /opt/sybase/httpd/conf/port-1080.conf /opt/sybase/httpd/conf/port-1443.conf

|  |
| --- |
| OLD |
| Listen 1080 <VirtualHost \*:1080>  ErrorLog logs/error-1080.log  CustomLog logs/access-1080.log combined |

|  |
| --- |
| NEW |
| Listen 1443 <VirtualHost \*:1443>  ErrorLog logs/error-1443.log  CustomLog logs/access-1443.log combined   Include conf/components/ssl.conf |

1. Edit /opt/sybase/httpd/conf/components/mobiliser-portals-internal.conf like the following using user “sap-httpd”:

|  |
| --- |
| OLD |
| ProxyPass /portal balancer://portalcluster/portal lbmethod=byrequests  Header add Set-Cookie "ROUTEID=.%{BALANCER\_WORKER\_ROUTE}e; path=/portal" env=BALANCER\_ROUTE\_CHANGED <Proxy balancer://portalcluster>  BalancerMember http://van-aps-1:8082 route=1  BalancerMember http://van-aps-2:8082 route=2  ProxySet stickysession=ROUTEID </Proxy> |

|  |
| --- |
| NEW |
| ProxyPass /portal balancer://portalcluster/portal lbmethod=byrequests  SSLProxyEngine on <Proxy balancer://portalcluster>  BalancerMember https://van-aps-1:8445 route=1  BalancerMember https://van-aps-2:8445 route=2  ProxySet stickysession=ROUTEID </Proxy> |

1. Do the same for any endpoint and external portal you have enabled for your environment.
2. Restart Apache HTTPD using user “sap-httpd”.

sudo -u sap-httpd /opt/sybase/httpd/bin/apachectl restart

# Passwords

|  |  |  |
| --- | --- | --- |
|  | | Password Value |
| Keystore password Money | (password1) |  |
| Key password Money | (password2) |  |
| Keystore password Brand | (password3) |  |
| Key password Brand | (password4) |  |
| Keystore password Internal Portals | (password5) |  |
| Key password Internal Portals | (password6) |  |
| Keystore password External Portals | (password7) |  |
| Key password External Portals | (password8) |  |