

TÀI LIỆU

QUY TRÌNH CÀI ĐẶT

Quy trình triển khai, cấu hình hệ thống ESB

|  |  |
| --- | --- |
| Ngày hoàn thành | 01/02/2013 |
| Người lập | Nguyễn Văn Tích  Phạm Thị Hoa  Vũ Trung Kiên |
| Người xem xét | Ngô Xuân Phong  Quản trị dự án |

**Hà nội, tháng 02/2013**

Mục lục

[1 Cấu hình RSA Agent trên ESB để làm việc với RSA 3](#_Toc347926872)

[1.1 Thực hiện import token data 3](#_Toc347926873)

[1.2 Tạo RSA authentication agent 4](#_Toc347926874)

[1.3 Cấu hình authentication agent 6](#_Toc347926875)

[1.4 Lấy file sdconf.rec 9](#_Toc347926876)

[1.5 Lấy thông tin về Command user và password của RSA 10](#_Toc347926877)

[1.6 Lấy file certificate của RSA server 10](#_Toc347926878)

[1.7 File authuser.properties 13](#_Toc347926879)

[1.8 Tạo Security domain Customer 15](#_Toc347926880)

[1.9 Tạo và gán quyền cho user apiadmin 15](#_Toc347926881)

[2 Deploy ứng dụng Monitor lên Websphere Aplication Server. 19](#_Toc347926882)

[2.1 Tạo DB user 19](#_Toc347926883)

[2.2 Tạo Application Server Cluster 19](#_Toc347926884)

[2.3 Cấu hình JDBC Provider và Data sources 21](#_Toc347926885)

[2.4 Deploy ứng dụng 24](#_Toc347926886)

[2.5 Kiểm tra ứng dụng mornitor 31](#_Toc347926887)

[3 Deploy ứng dụng TAXGW lên WAS 31](#_Toc347926888)

[3.1 Deploy 31](#_Toc347926889)

[3.2 Kiểm tra ứng dụng GIPBankSevice kết nối cổng thuế 39](#_Toc347926890)

[3.3 Kiểm tra ứng dụng service kết nối hải quan lấy thông tin 40](#_Toc347926891)

[3.4 Kiểm tra sevice kết nối hải quan để đối chiếu 41](#_Toc347926892)

# Deploy ứng dụng Monitor lên Websphere Aplication Server.

Yêu cầu: Máy chủ ứng dụng đã được cài đặt theo quy trình để cập trong tài liệu “Quy trình cài đặt”.

## Tạo DB user và import CSDL

* Tạo và gán quyền cho user trong CSDL:

create user esb\_msb identified by oracle1;

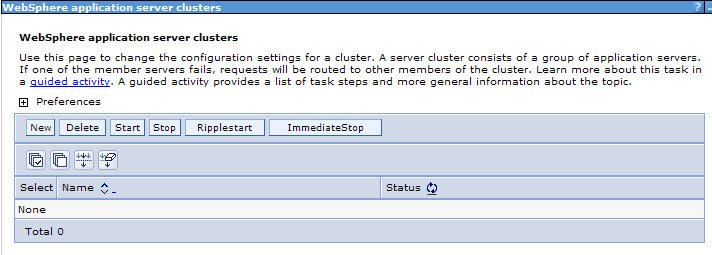
grant create session, resource to esb\_msb;

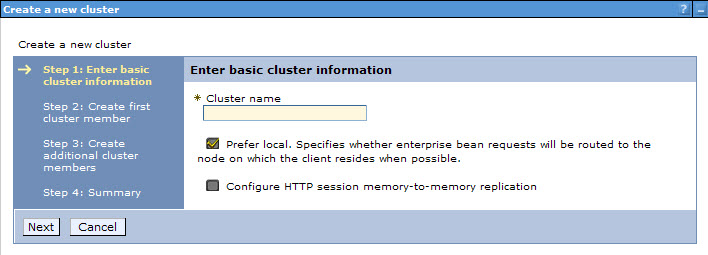
grant execute on dbms\_crypto to esb\_msb;

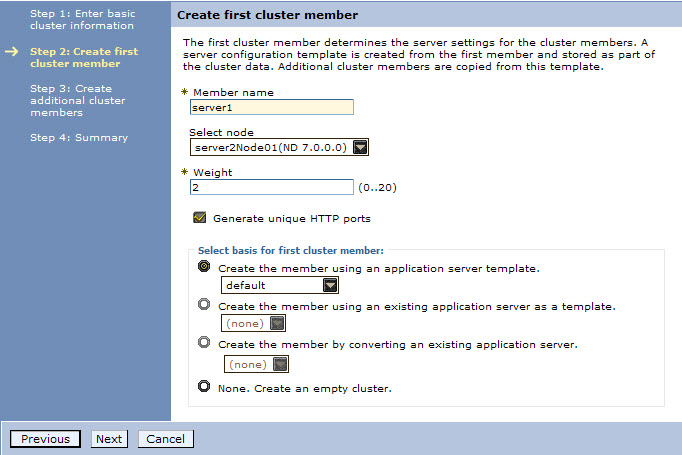
* Thực hiện import file esb\_msb\_uat.dmp

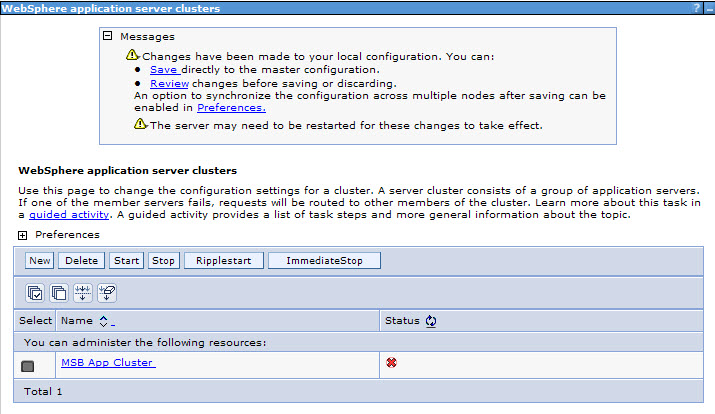
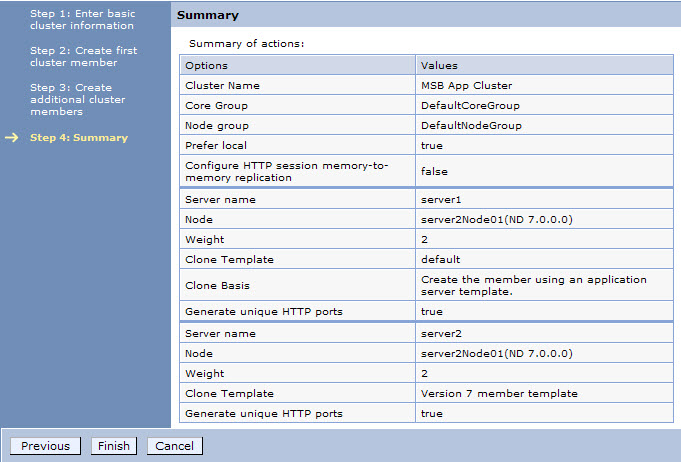
## Tạo Application Server Cluster

Vào IBM console bằng địa chỉ http://10.1.3.23:9060/imb/console



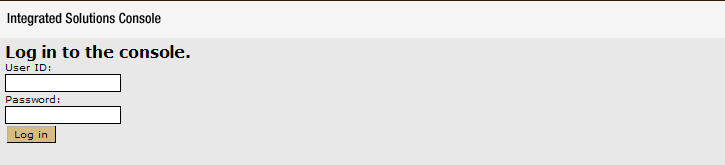






## Cấu hình JDBC Provider và Data sources

*Để thực hiện các bước cấu hình dưới đây yêu cầu phải đăng nhập vào hệ thống Websphere Admin Console theo địa chỉ: https://<host>:<port>/ibm/console/logon.jsp với user/password theo tài liệu* “*Quy trình cài đặt hệ thống*”.host:10.1.3.23,port :9060

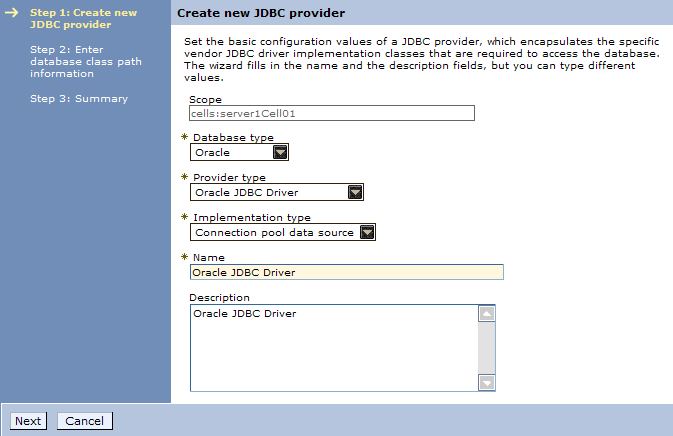
**

Step1: Chọn tab **Resources** 🡪 **JDBC Provider**

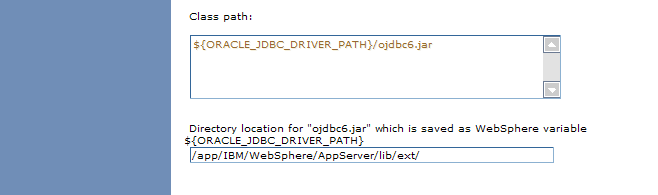
Step2: Chọn Scope: Cell=server1Cell01 và nhấn **New**

Step3: Chọn các options:

* Database type: Oracle
* Provider type: Oracle JDBC Driver
* Implementation type: Connection pool data source
* Chọn **Next** để tiếp tục.



Step4: Chọn đường dẫn cấu hình biến class path **ORACLE\_JDBC\_DRIVER\_PATH**, copy gói ojdbc6.jar từ thư mục **libs/resource** vào đường dẫn vừa chọn. Đường dẫn mặc định là */app/IBM/WebSphere/AppServer/lib/ext/*

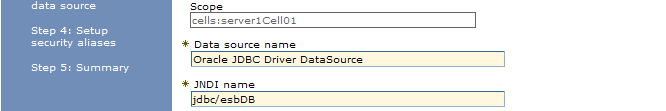


Step1: Chọn tab **Resources** 🡪 **Data sources**

Step2: Chọn Scope: Cell=server1Cell01 và nhấn **New**

Step3: Nhập thông tin cơ bản:

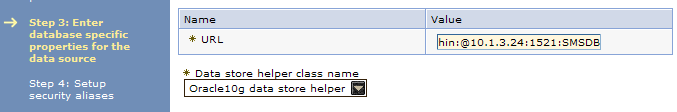
* Data source name: tùy chọn
* JNDI name: jdbc/ibsDB



Step4: Chọn JDBC Provider

* Chọn Select an existing JDBC provider
* Chọn Oracle JDBC Driver

Step5: Nhập URL cho datasource.



Step6: Bỏ qua phần thiết lập security alias, nhấn **Next** và **Finish** để kết thúc.

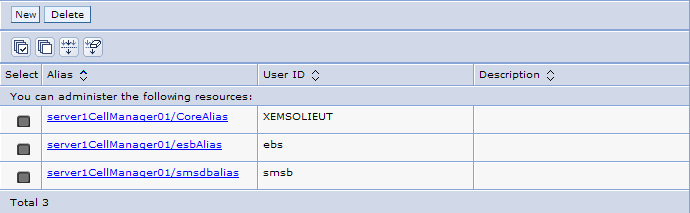
**Cấu hình Securities Authentication Aliases**

Step1: Chọn tab **Resources** 🡪 **Data sources**. Nhấn vào 1 trong các datasource đã được tạo ra từ mục 2.2.

Step2: Trong phần **Related Items**, nhấn JASS – J2C authentication data.

Step3: Nhấn **New** để tạo alias. Nhập thông tin Alias:

* Alias: Tên tùy chọn
* UserId/Password: là các userId/password tương ứng với các thông tin kết nối với từng datasource.



Step4: Quay trở lại datasource, trong mục **Security settings**, chọn alias tương ứng cho mục Component-managed authentication alias và Container-managed authentication alias.

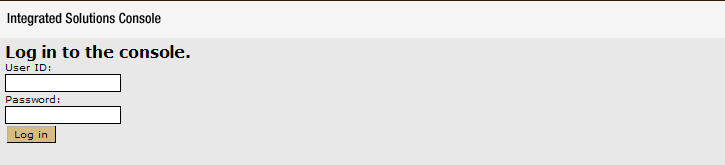
Step5: Cấu hình tương tự cho các datasource còn lại. Nhấn **Test Connection** để kiểm tra kết nối thành công hay không.



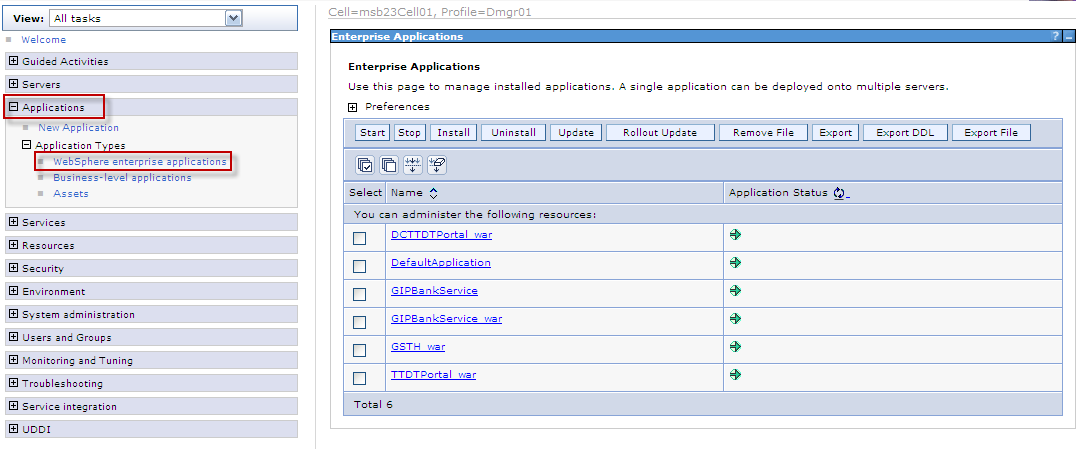
## Deploy ứng dụng

*Để thực hiện các bước cấu hình dưới đây yêu cầu phải đăng nhập vào hệ thống Websphere Admin Console theo địa chỉ: https://<host>:<port>/ibm/console/logon.jsp với user/password theo tài liệu* “*Quy trình cài đặt hệ thống*”. host:10.1.3.23,port :9060

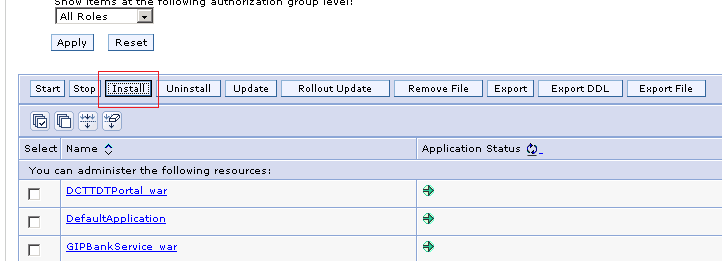
Login vào hệ thống IBM Admin Console.

**

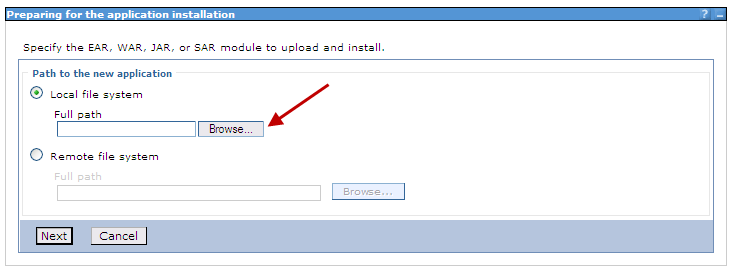
Chọn tab **Application** 🡪 **New Application** 🡪 **New Enterprise Application**.



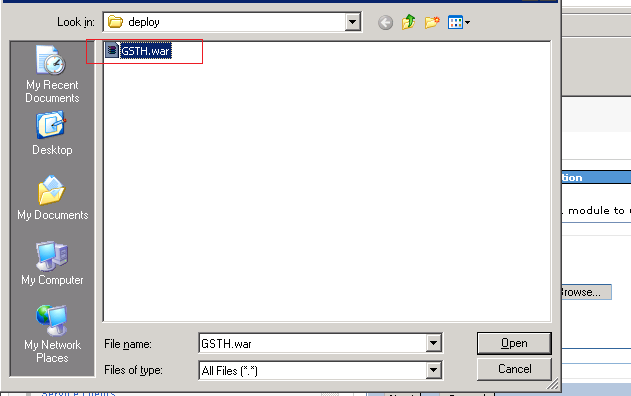
Click chọn Install .



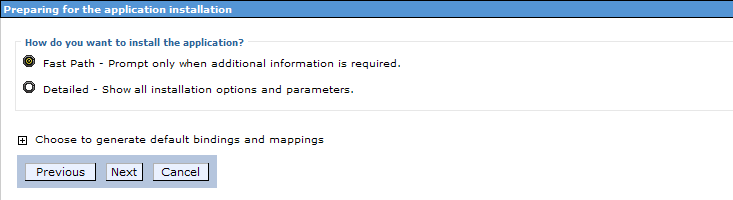
Trỏ đến thư mục chưa ứng dụng cần deploy rồi nhấn **Next** (Chọn local file system để trỏ đến ứng dụng trên máy hoặc remote file system để trỏ đến máy server cài đặt WAS).



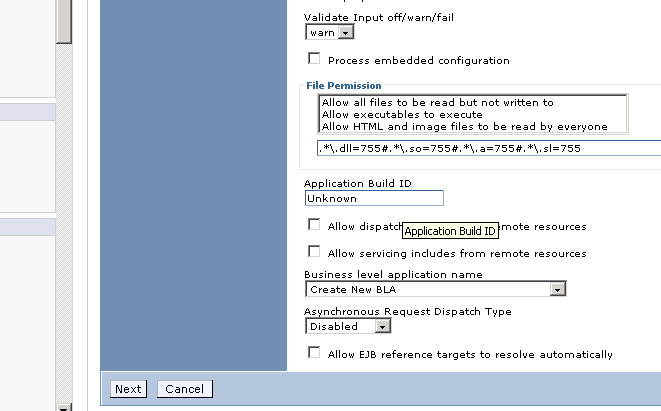
Chọn file.war



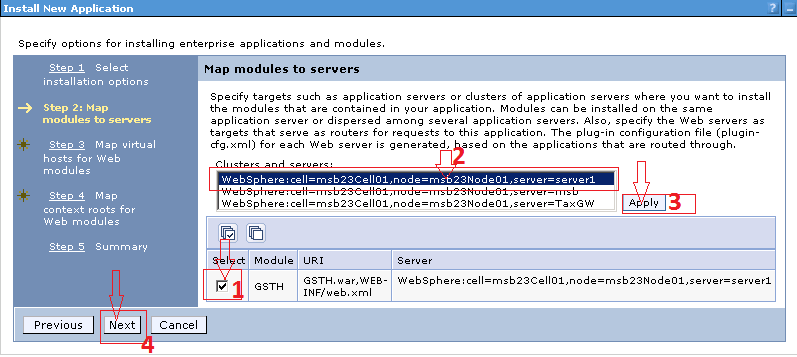
Chọn **Fast Path** và nhấn **Next**.



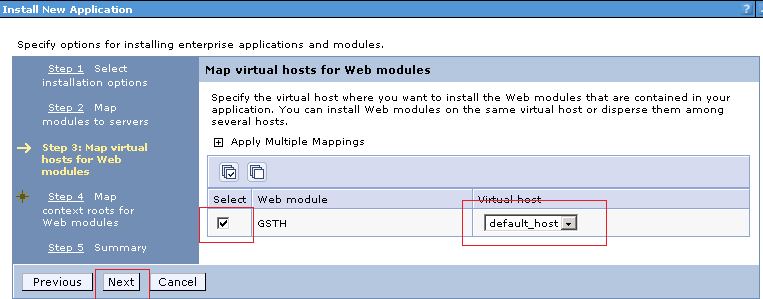
Click next.



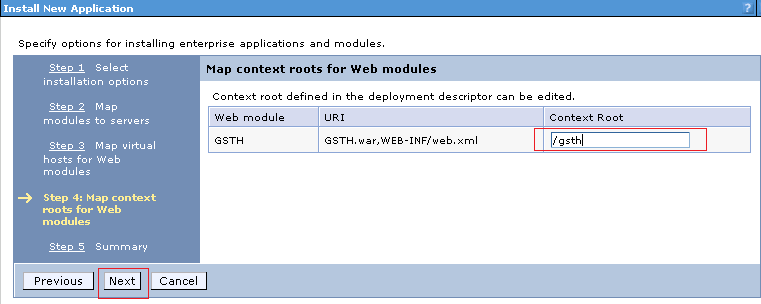
->Làm theo các bước giống trong hình



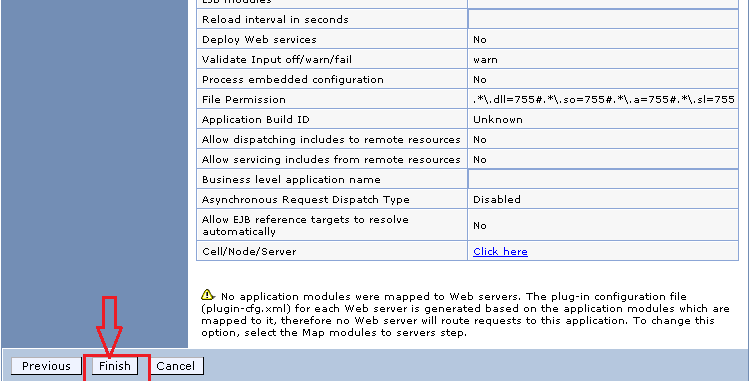
->Làm theo các bước giống trong hình



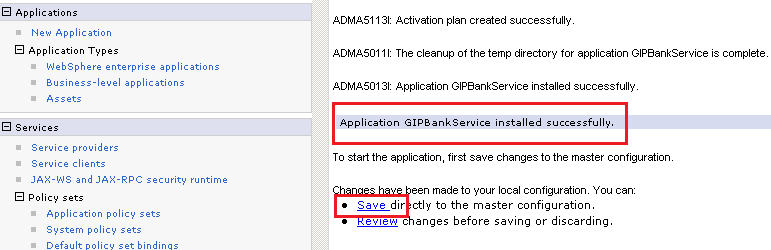
Nhập vào Context Root là “/gsth” sau đó click next.



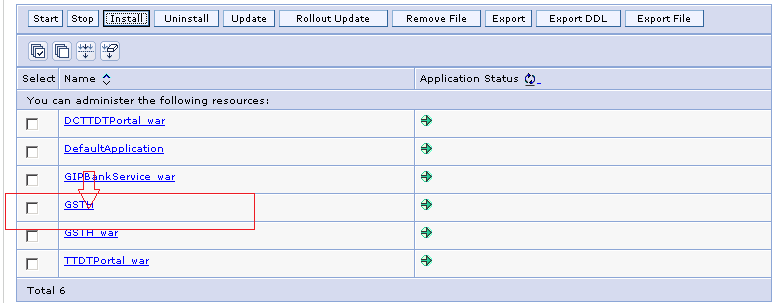
->Click finish



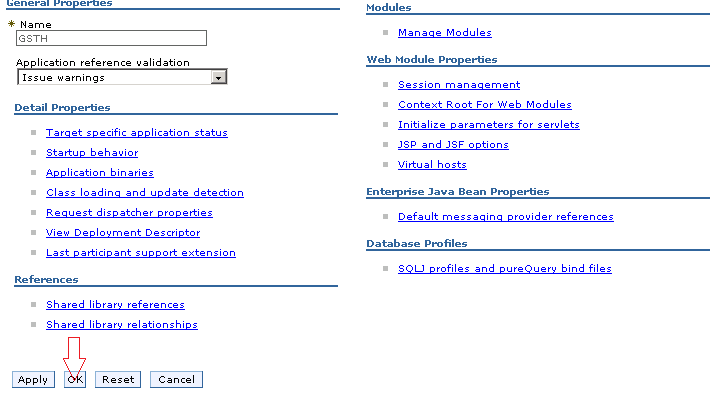
Chờ quá trình install -> sau đó sẽ thấy kết quả như hình dưới-> click save.



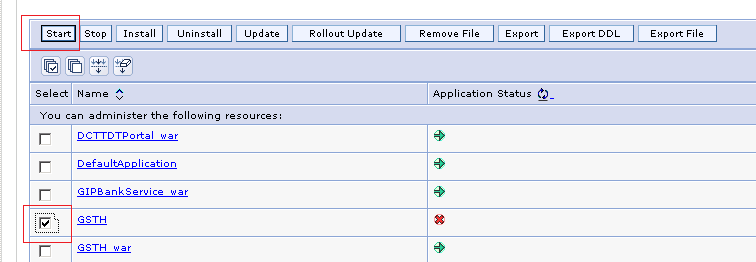
Click vao aplication mới deploy lên server để xem thông tin.



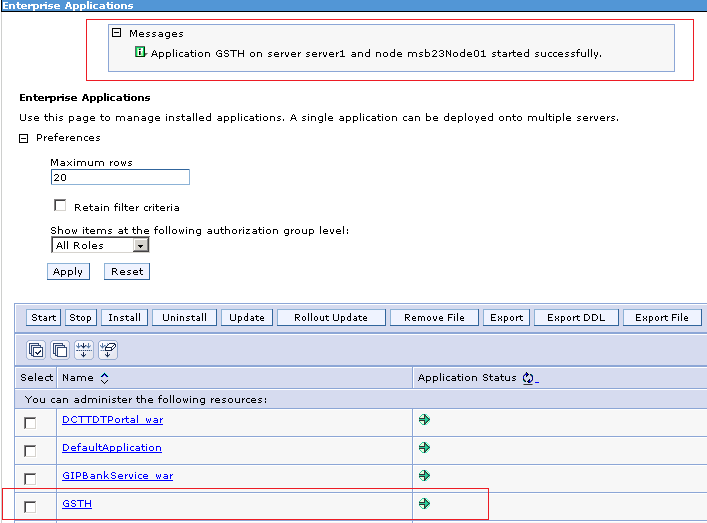
xem các thông tin về ứng dụng.sau đó click-> ok ->và chọn save ở màn hình tiếp theo



Star ứng dụng -> check chọn ứng dụng mới được deploy lên(ở đây là GSTH) sau đó click -> start



Nếu deploy thành công sẽ có thông báo như hình dưới.



## Kiểm tra ứng dụng mornitor

Kiểm tra xem hệ thống đã đươc deploy thàng công chưa bằng cách gỡ vào địa chỉ trình duyệt địa chỉ sau http://10.1.3.23:9080/gsth/.sẽ thấy màn hình đăng nhập ứng dụng.



# Deploy ứng dụng ESB lên Message Broker

Yêu cầu:

* Đã cài đặt MB
* Đã tạo user và import dữ liệu

## Deploy ứng dụng

-Copy file nén vào thư mục **/opt/ibm/mqsi/7.0/bin** (có thể thay đổi theo thực tế máy chủ)

-Vào thư mục này và chạy lệnh deploy

|  |
| --- |
| **. mqsiprofile** |

|  |
| --- |
| mqsideploy <MSBBRK\_PRO> -e <MSB\_EXEGRP\_PRO> -a <MsbgatewayArchivePro.bar> |

Ghi chú:

+ MSBBRK\_PRO là tên của broker

+ MSB\_EXEGRP\_PRO là tên của execution group

+MsbgatewayArchivePro.bar là file chứa ứng dụng

## Kiểm tra ứng dụng

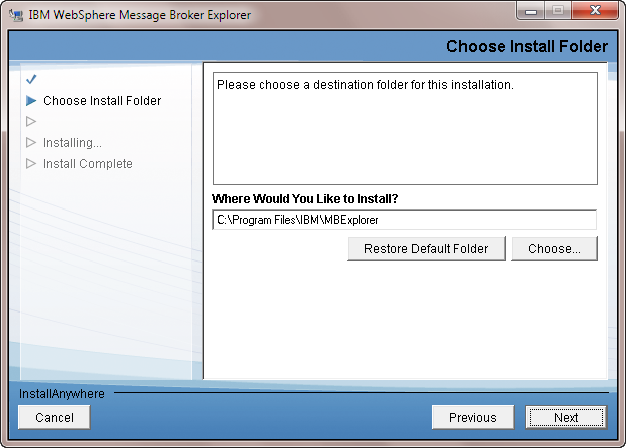
Để kiểm tra xem ứng dụng có còn hoạt động không ta dùng công cụ MB7 Explorer tại máy client Windows.

### Hướng dẫn cài đặt MB7 Explorer trên client Windows

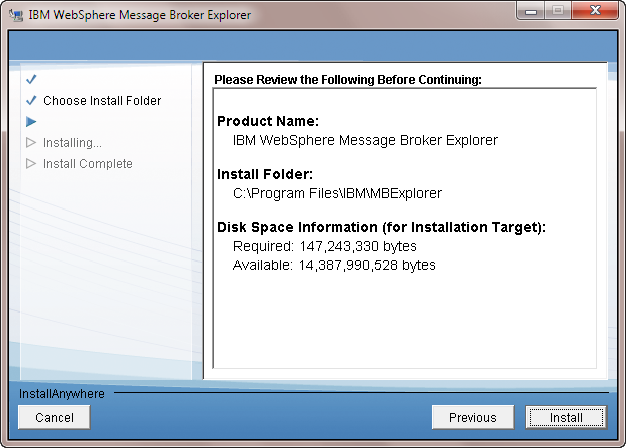
Step1: Chạy file cài



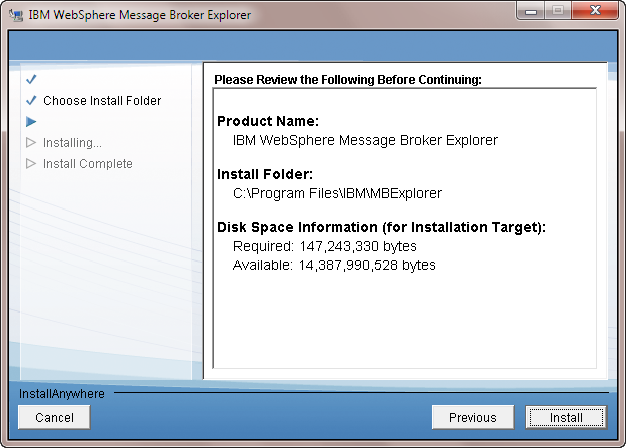
Step2: Chọn thư mục



Step3:Tiếp tục cài đặt

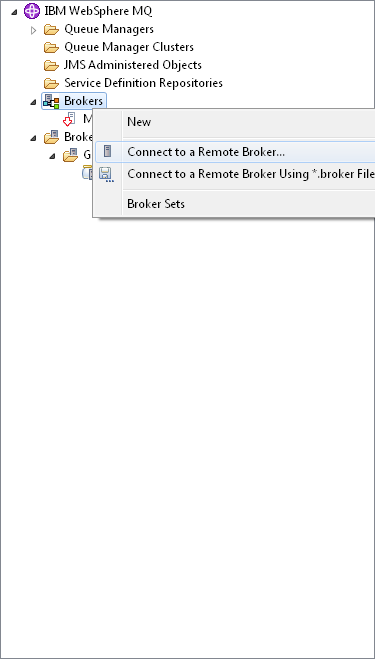


Step4 Kết thúc cài đặt

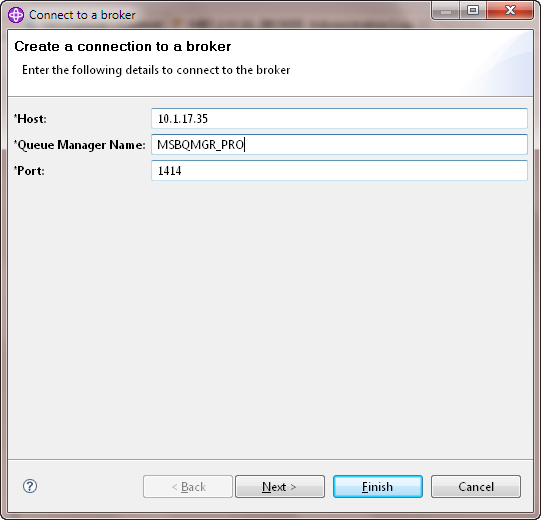


Step5: Cấu hình trỏ đến Broker trên máy server

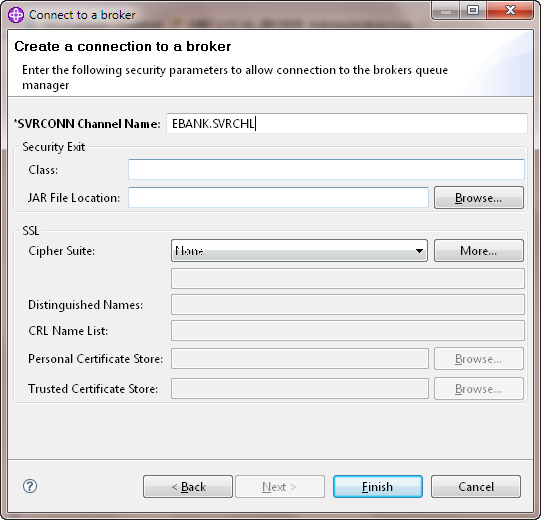
-Vào MQ 7 Explorer



Cấu hình tham số

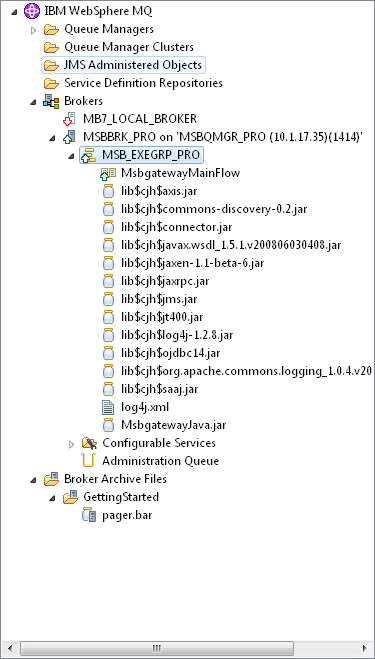


Cấu hình channel



### Kiểm tra ứng dụng

Vào MQ 7 Explorer, nếu kết quả hiển thị tương tự như hình dưới đây thì hệ thông đang hoạt động tốt (với mũi tên hướng lên màu xanh) .



# Cấu hình RSA Agent trên ESB để làm việc với RSA

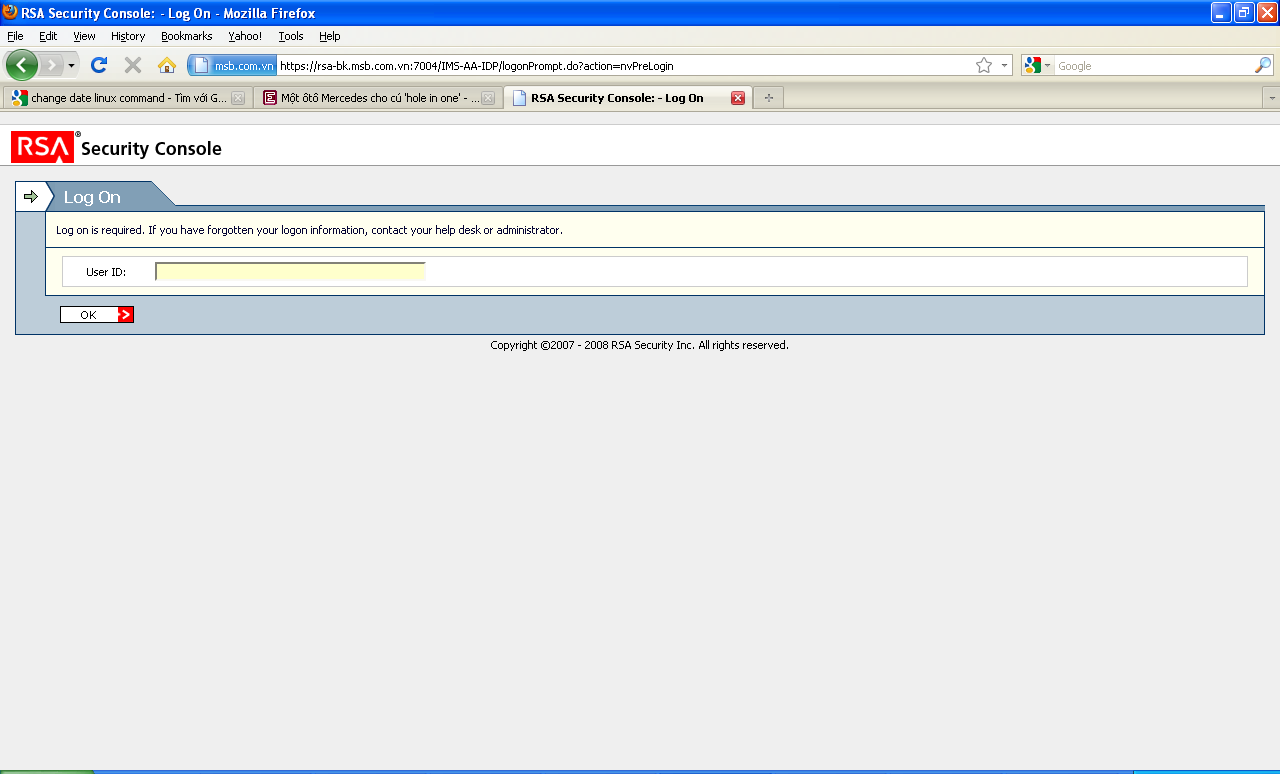
Yêu cầu:

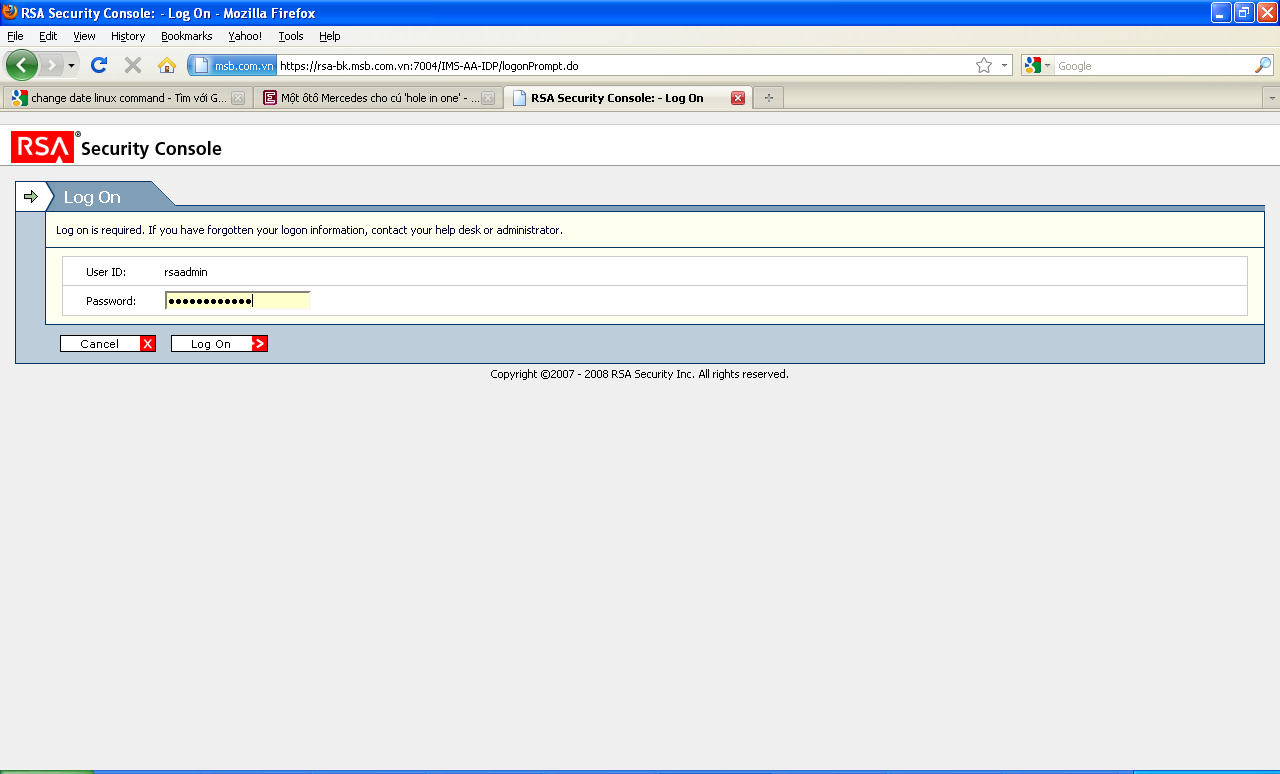
* Đã cài đặt RSA server (tên RSA server có thể khác so với tài liệu này)
* Đã deploy RSA Agent lên Message Broker

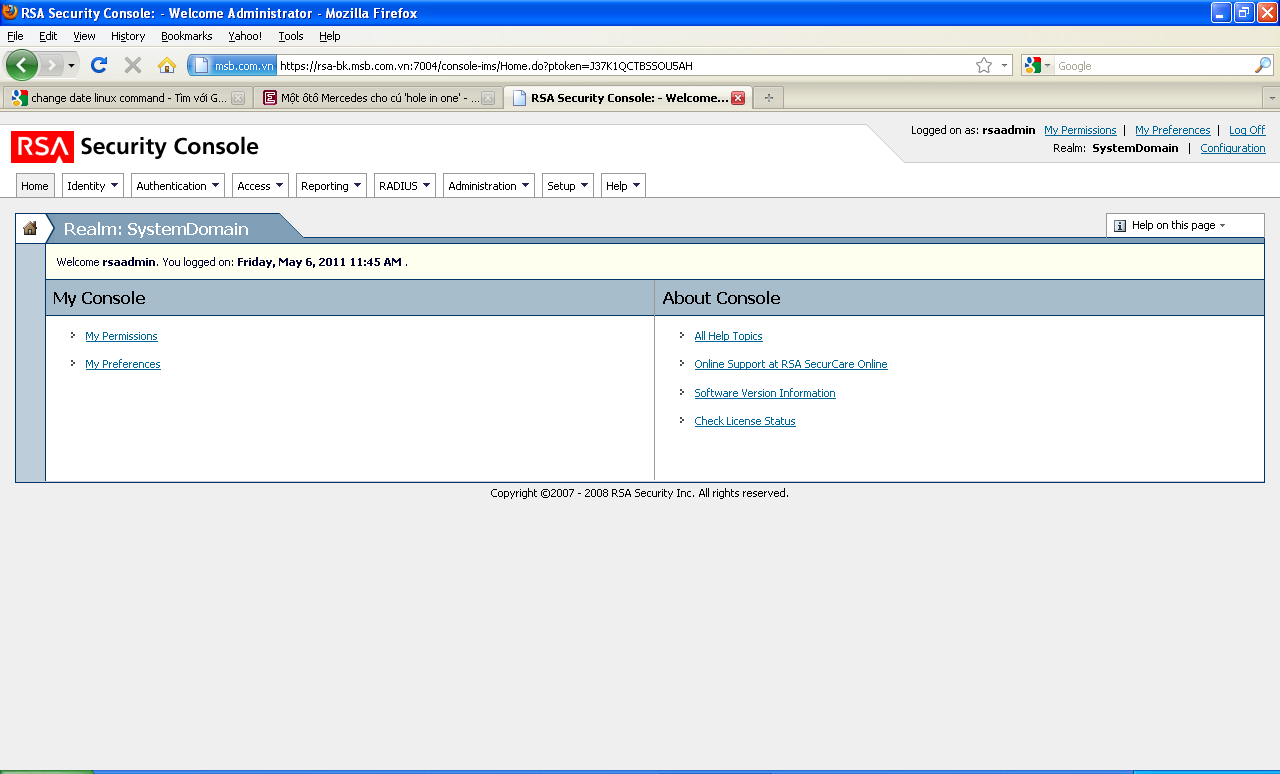
## Thực hiện import token data

Chỉ thực hiện khi chưa import.

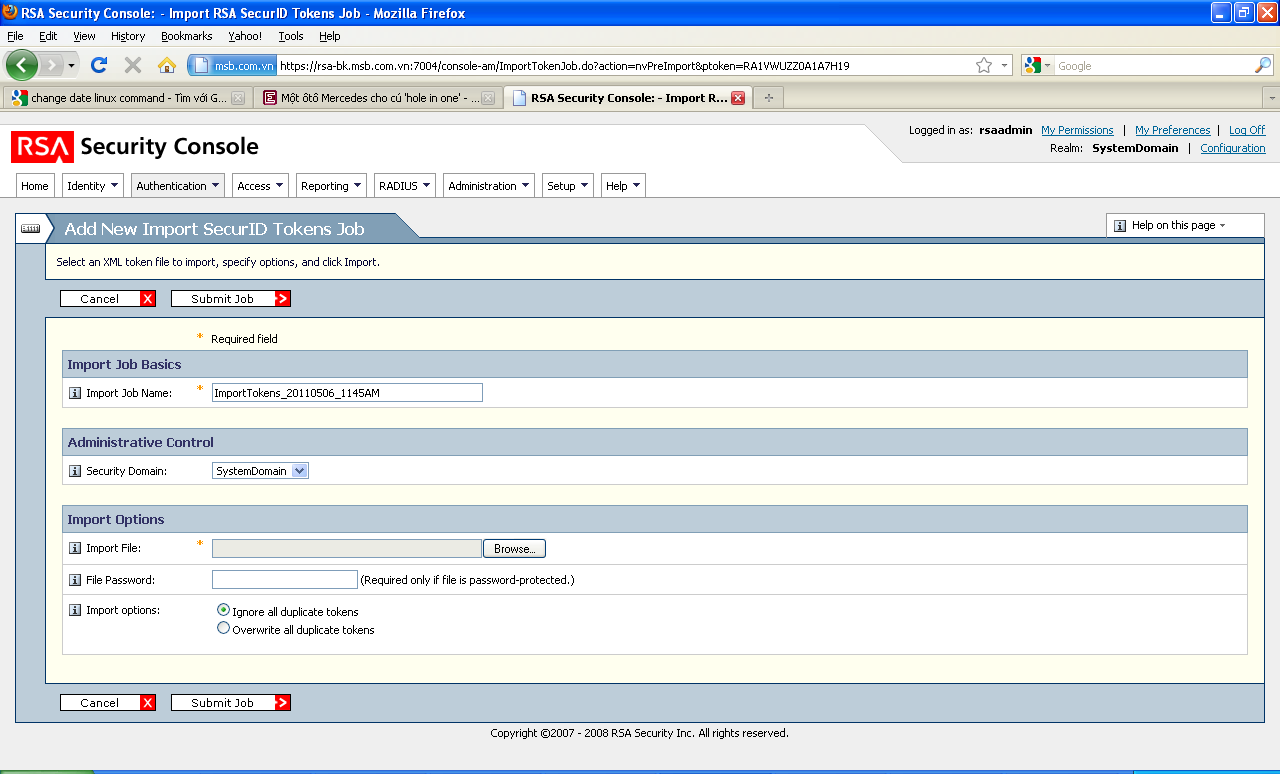
Vào https://rsa-pro.msb.com.vn:7004/console-ims/



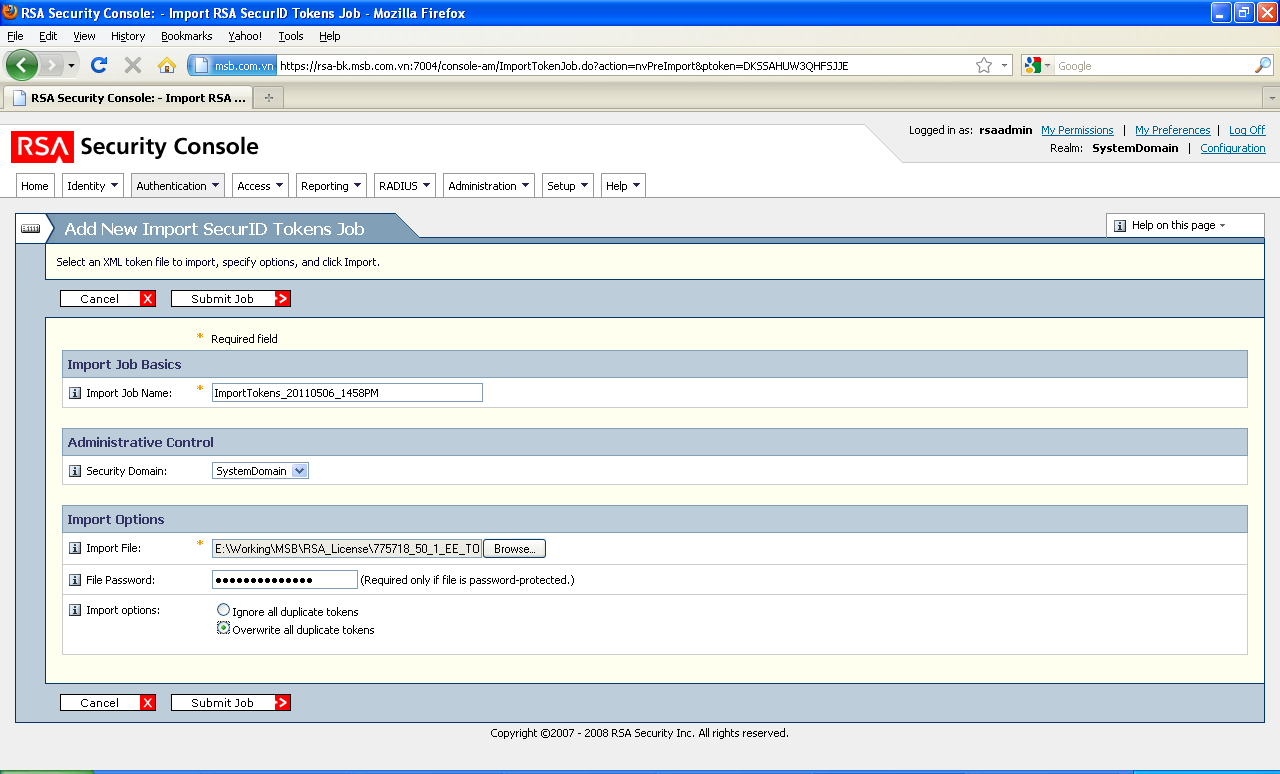




Vào menu Authentication 🡪 SecurId Tokens 🡪 Import Token Jobs 🡪 Add new



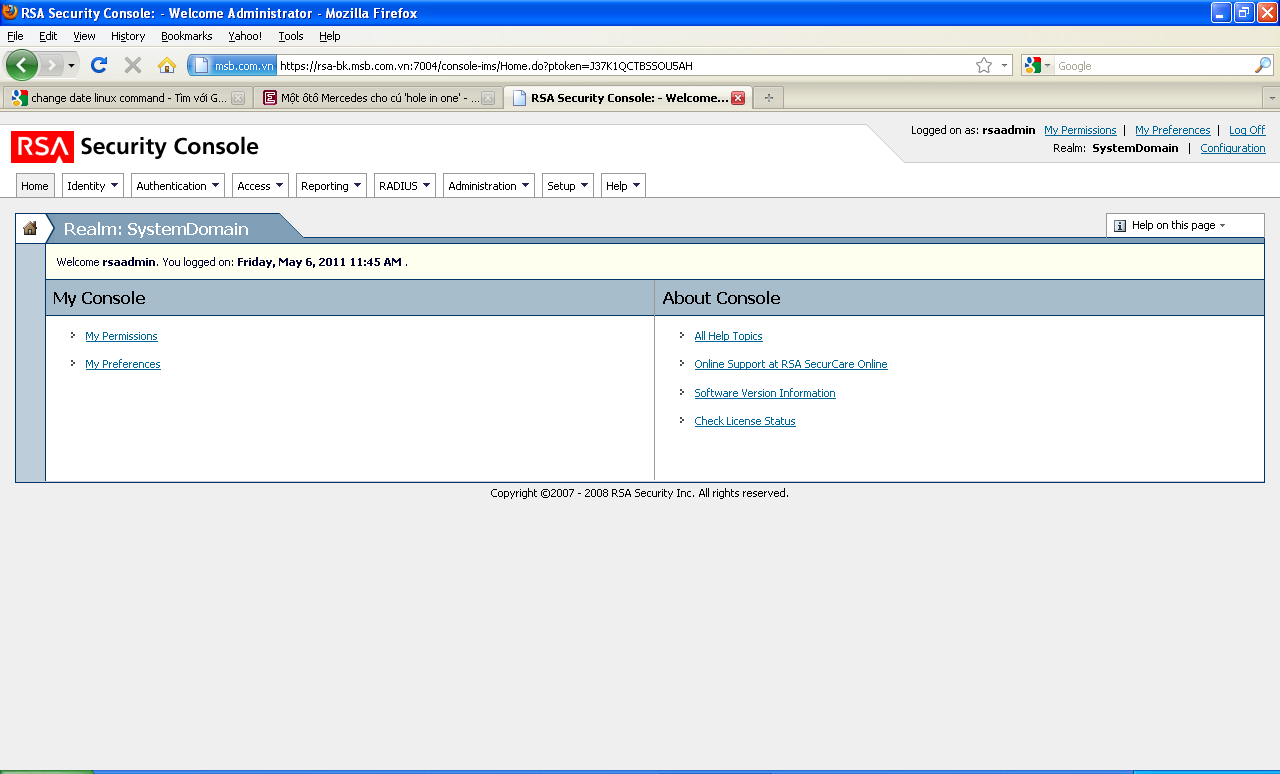
Nhập mật khẩu có được từ thẻ cào mà RSA gửi (tương ứng với mỗi hộp thiết bị có 1 thẻ cào chứa mật khẩu để import)



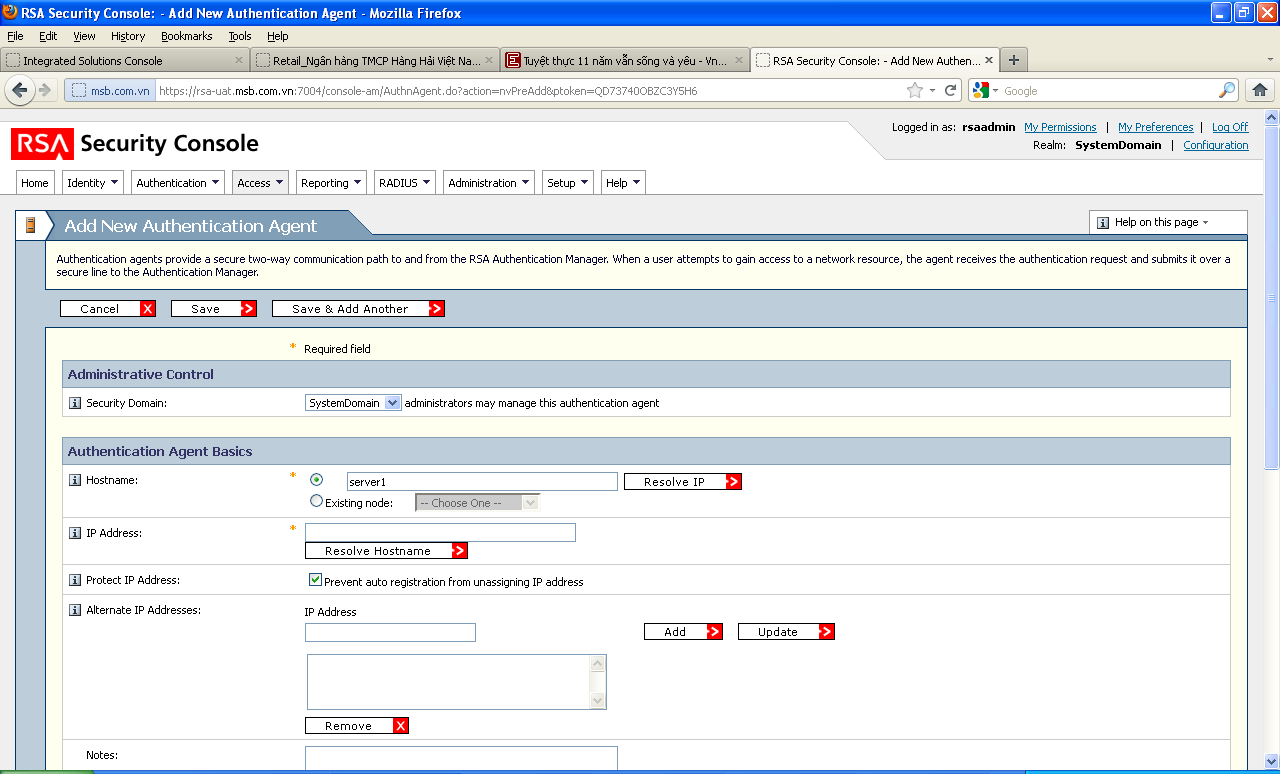
## Tạo RSA authentication agent

**Lưu ý:** trước khi làm viêc này thì agent (máy chủ cài ứng dụng có dùng RSA**, cụ thể trong trường hợp này thì là máy chủ cài ESB**) và RSA server phải ping được đến nhau theo tên (có thể đặt trong host file).

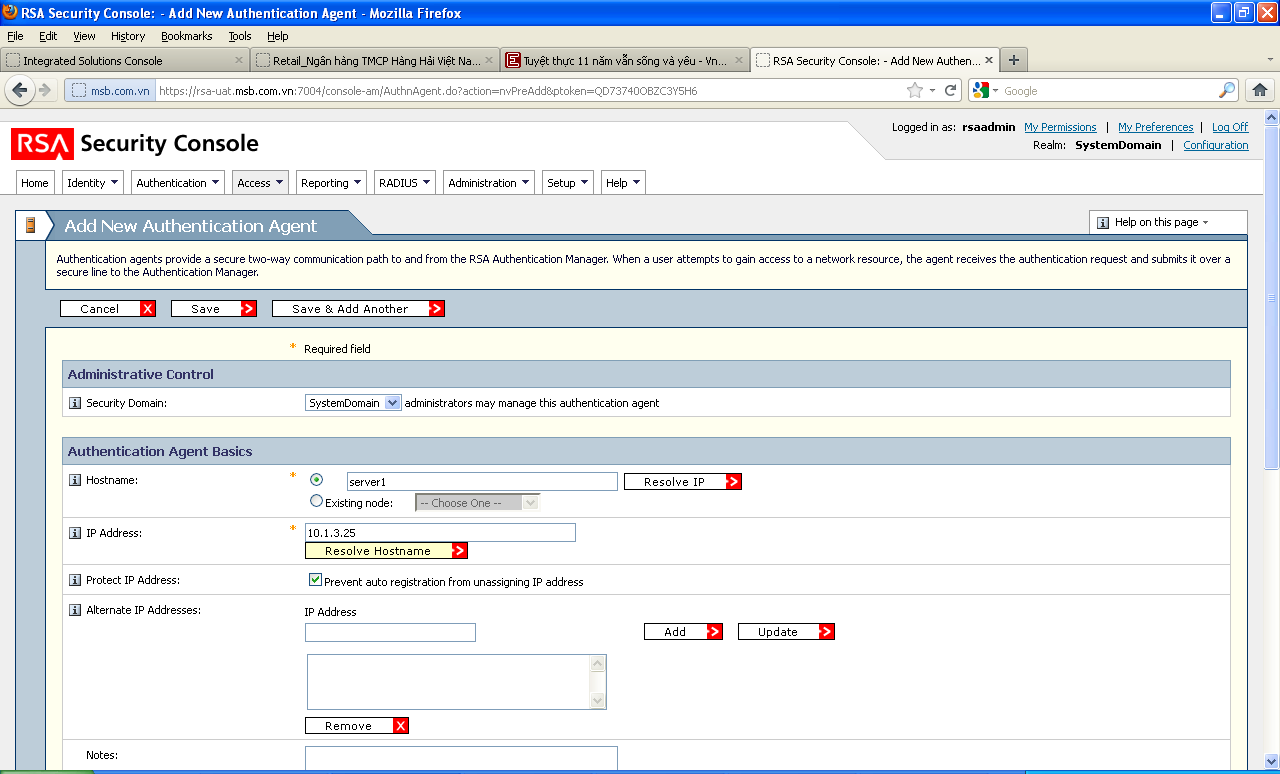
Vào Security Console tại <https://rsa-pro.msb.com.vn:7004/console-ims/>



Vào Menu Access 🡪 Authentication Agents 🡪 Add New. Tại phần Authentication Agent Basics nhập tên của máy chủ ứng dụng vào trường Hostname:

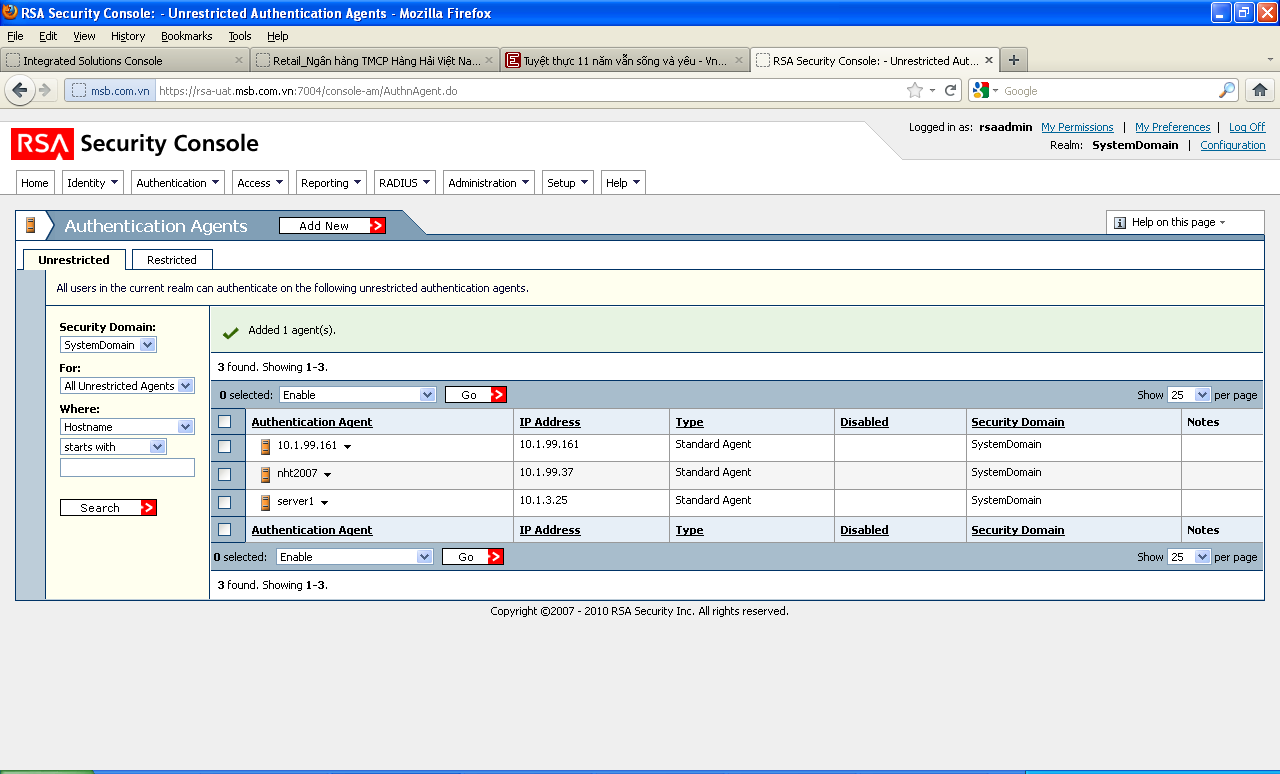


Sau đó click và Resolve IP, trường IP address sẽ được fill IP của máy chủ ứng dụng vào.



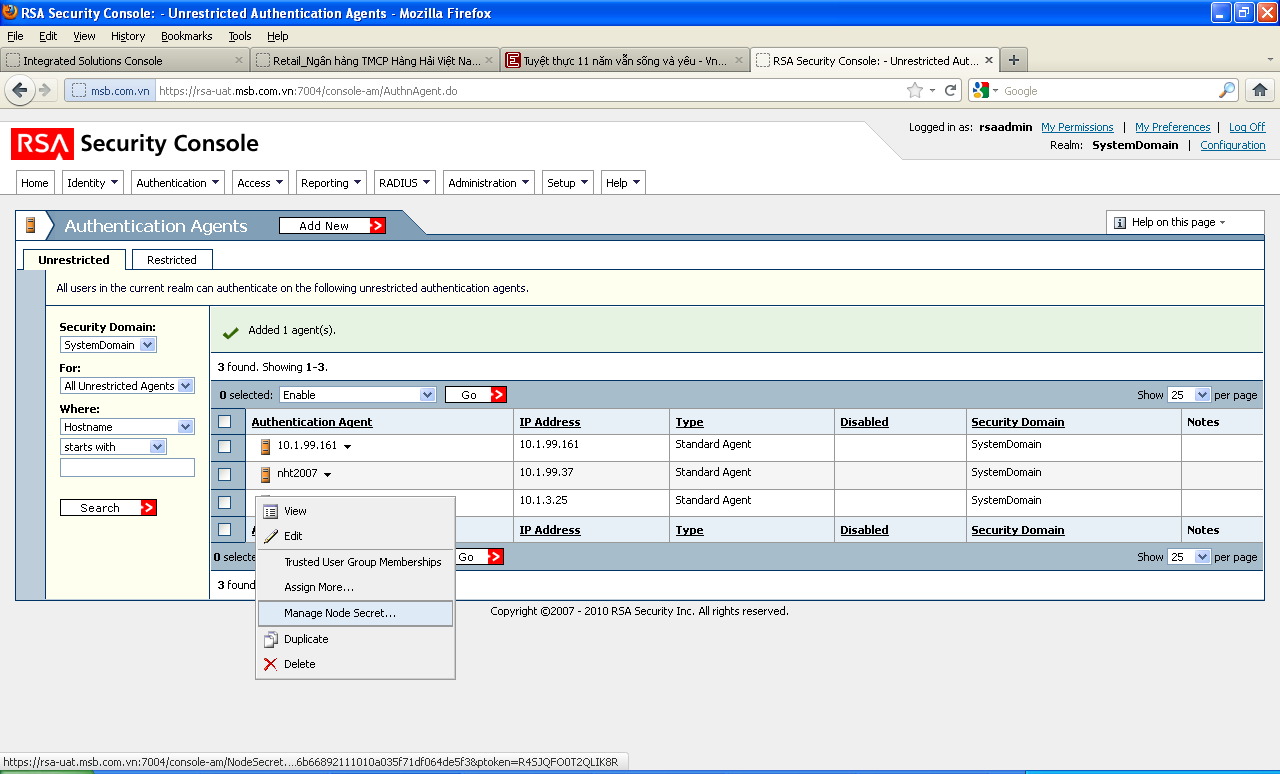
Các trường khác để mặc định.

Chọn Save. Sẽ về màn hình liệt kê các Agent đã tồn tại.

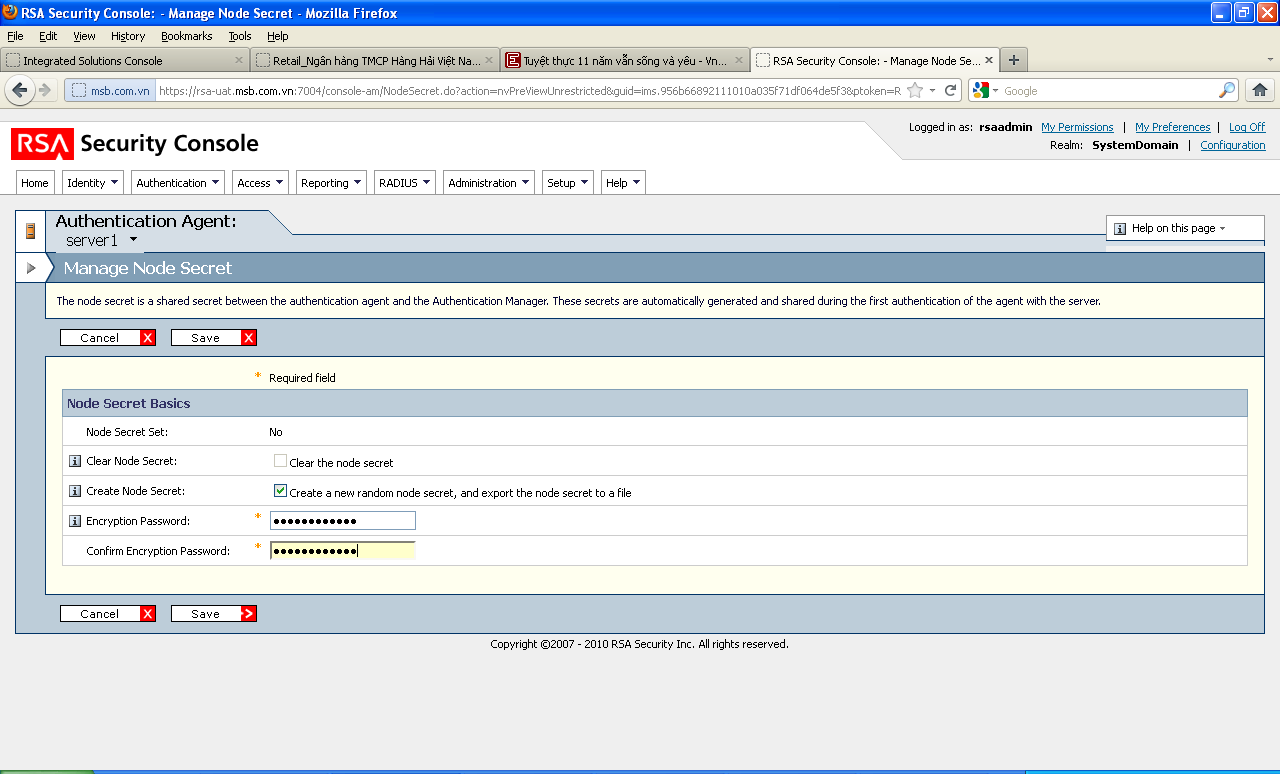


## Cấu hình authentication agent

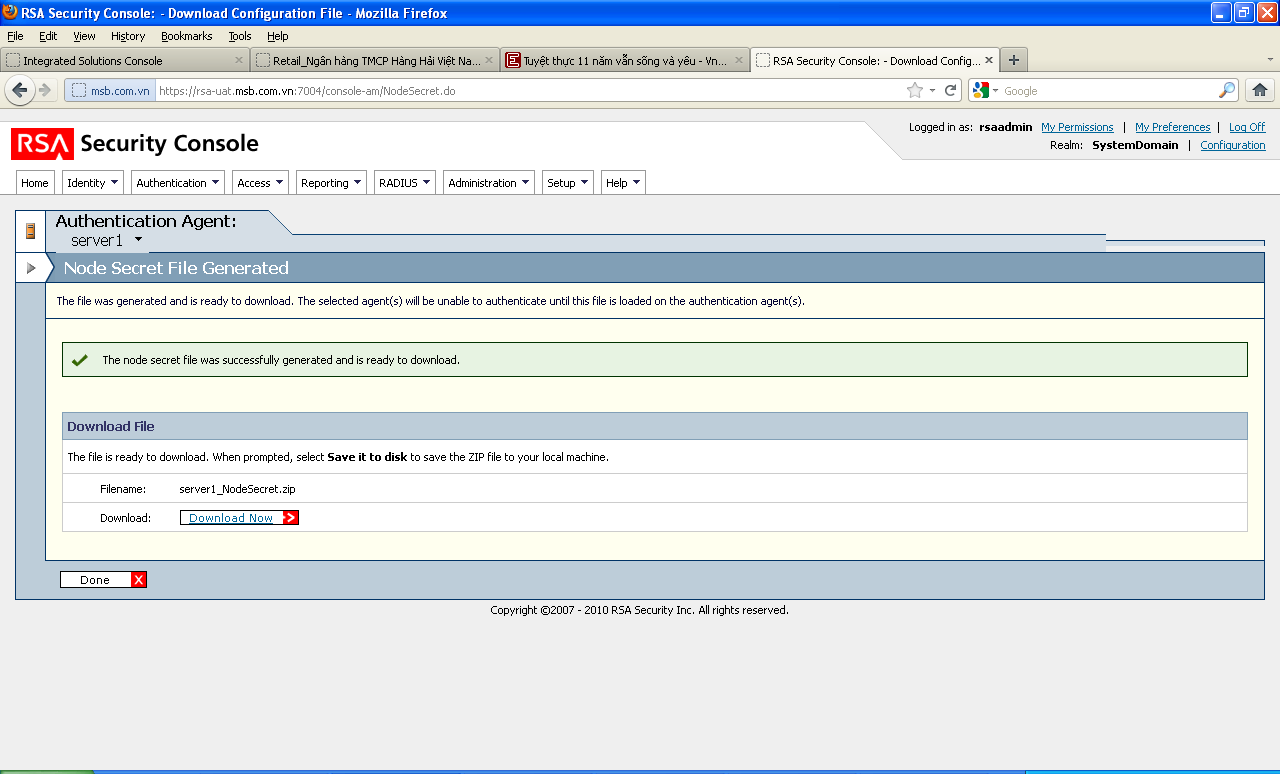
Chọn Agent vừa thêm sau đó chọn Manage Node Secret.



Ta đến màn hình, tiếp theo, nhập mật khẩu của Node Secret (VD maritime\_123).



Click Save:



Chọn Download Now để download file node secret được sinh ra.

Click Done.

Extrack file zip vừa có, ta có file nodesecret.rec. Copy file này lên thư mục /u01/RSASecurity/RSAAuthenticationManager/utils/bin/ace\_nsload/linux-2.4-x86 của máy chủ RSA.

Vào máy chủ RSA chạy các lệnh sau:

**export USR\_ACE=/u01/app/RSASecurity/RSAAuthenticationManager/utils/bin/ace\_nsload/linux-2.4-x86**

**export VAR\_ACE=/u01/app/RSASecurity/RSAAuthenticationManager/utils/bin/ace\_nsload/linux-2.4-x86**

**cd /u01/app/RSASecurity/RSAAuthenticationManager/utils/bin/ace\_nsload/linux-2.4-x86**

**./agent\_nsload -f nodesecret46.rec -p maritime\_123**

(maritime\_123 là mật khẩu của node secret ta nhập lúc trước)

Ta sẽ có các thông báo như sau:

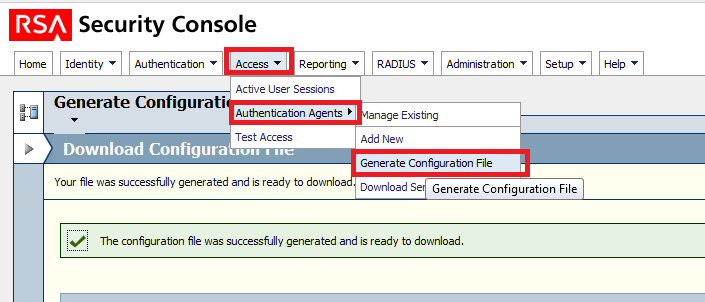
Loading Node Secret....

The Node Secret is successfully loaded

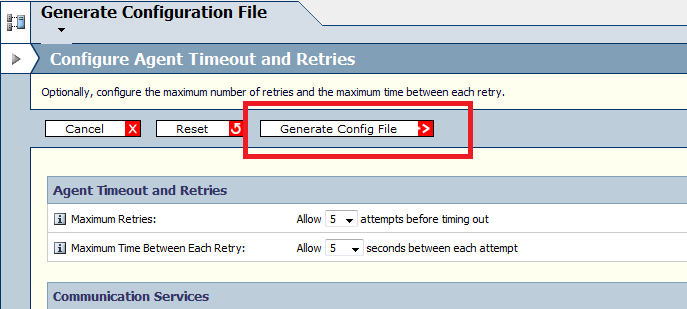
Các lệnh trên sinh ra file secureid. Copy file này lên thư mục /home/rsa trên máy chủ ứng dụng.

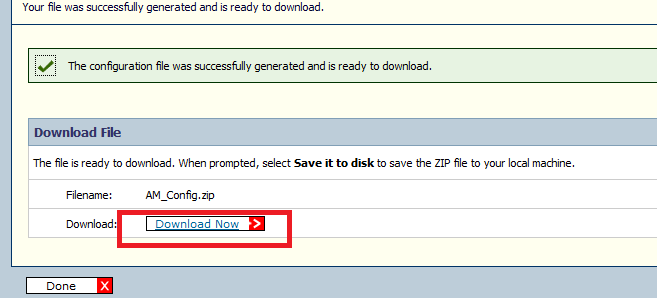
## Lấy file sdconf.rec

Vào Security console ->Access ->Authentication agent ->Genirate configrunation File



Click Genirate config File -> Download .Sau đó giải nén và copy file sdconf.rec về máy ứng dụng





## Lấy thông tin về Command user và password của RSA

Vào máy chủ RSA bằng user rsa (user cài đặt RSA), chạy các lệnh sau:

cd /u01/app/RSASecurity/RSAAuthenticationManager/utils

./rsautil manage-secrets --action listkeys

Enter Master password: \*\*\*\*\*\*\*\*\*\*\*\*

Secrets stored in ./etc/systemfields.properties.

com.rsa.cmdclient.user .............: **CmdClient\_xlcpi3ng**

com.rsa.cmdclient.user.password ....: **PSt9AbmoZB**

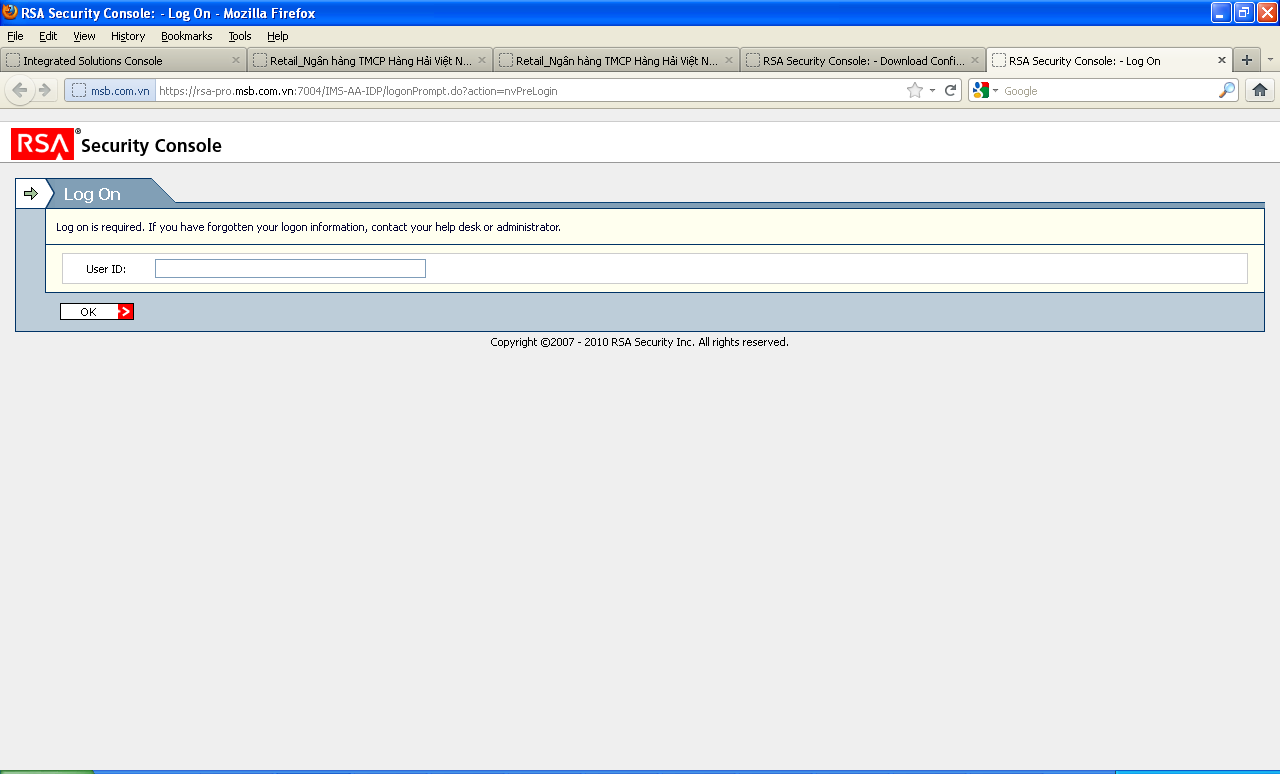
com.rsa.ssl.root.key.password ......: KkBuFgnqsP

com.rsa.ssl.root.store.password ....: cWT171w1HnMaster password là mật khẩu của RSA khai lúc cài.

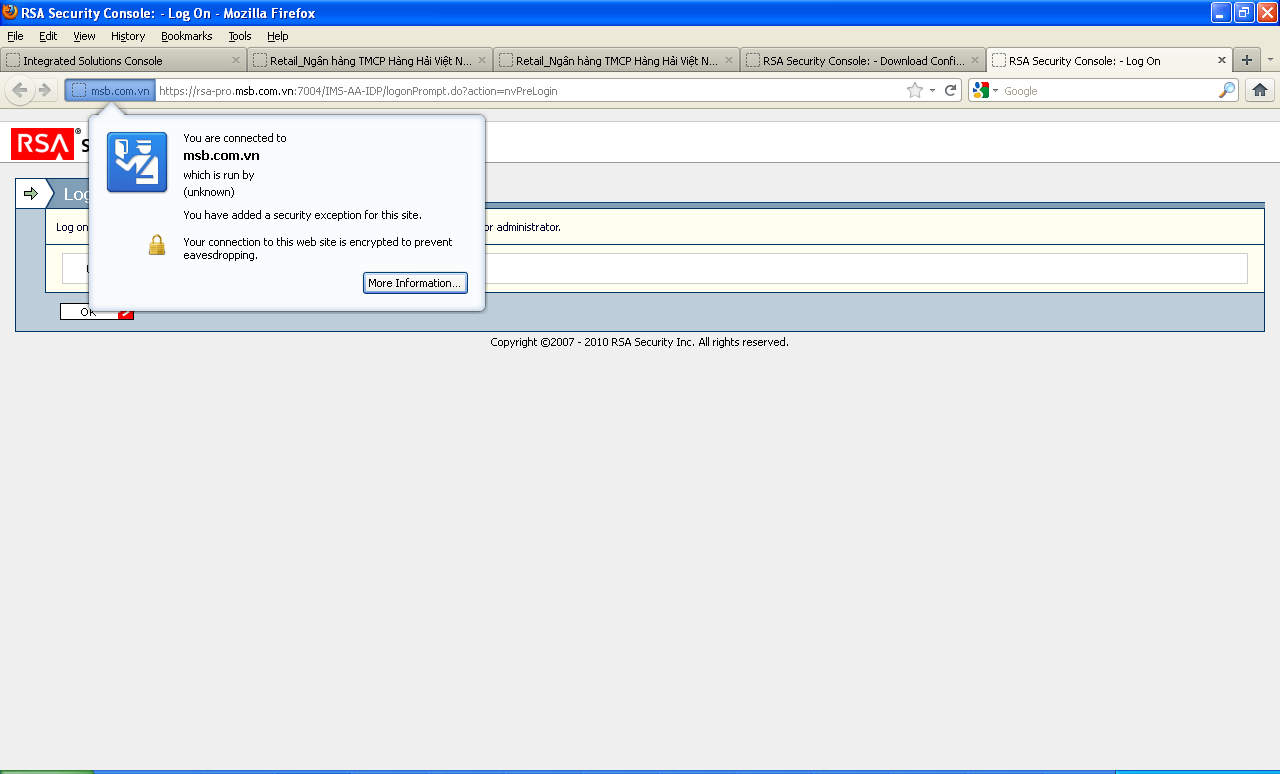
Ghi lại 2 thông tin về user và password trên.(cập nhật thông tin này vào file rsa.ptoperties)

## Lấy file certificate của RSA server

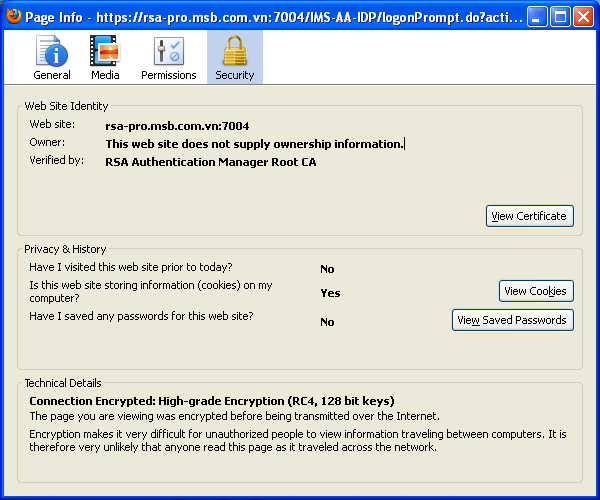
Dùng browser, lấy file certificate về như sau:



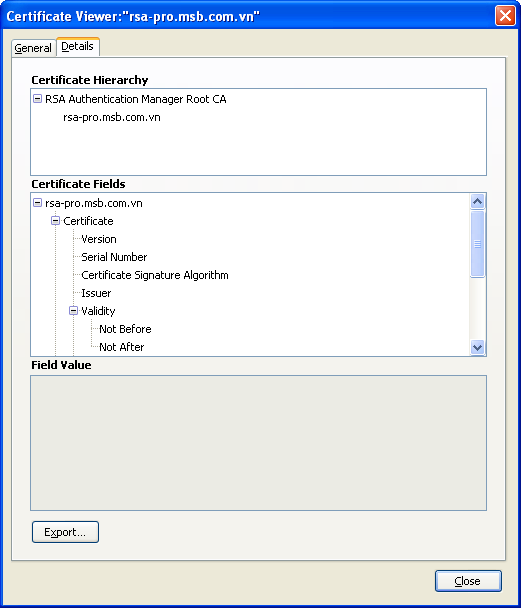
Clict msb.com.vn trên address bar.



Click More.



Click View Certificate, chọn tab Details



Click Export để export thành file DER có tên là rsa-pro.der.

Chạy lệnh:

"C:\Program Files\Java\jre6\bin\keytool" -importcert -file D:\rsa-esb.der -alias am73cert -keystore rsa-esb.jks -storepass Admin01

Sẽ sinh ra file rsa-pro.jks, copy file này lên /home/rsa của máy chủ eBank.

## File authuser.properties

File này đặt trong thư mục /home/rsa, nội dung như sau (lưu ý thông tin về chỗ đặt file secured đã tạo trong bước 1.3 Cấu hình authentication agent)

# RSA Authentication API Properties

# Override Host IP Address

RSA\_AGENT\_HOST=10.1.17.69

# Interval in seconds between which configuration is refreshed.

RSA\_CONFIG\_READ\_INTERVAL=600

# [This section is for Data Repository configuration.]

# Type of the Server configuration.

SDCONF\_TYPE=FILE

# Path of the Server configuration.

#SDCONF\_LOC=sdconf.rec

**SDCONF\_LOC=/home/rsa/sdconf.rec**

# Type of the Server statuses.

SDSTATUS\_TYPE=FILE

# Path of the Server statuses.

#SDSTATUS\_LOC=JAStatus.1

SDSTATUS\_LOC=JAStatus.1

# Type of the Server options.

SDOPTS\_TYPE=FILE

# Path of the Server options.

#SDOPTS\_LOC=sdopts.rec

SDOPTS\_LOC=sdopts.rec

# Type of the Node Secret.

SDNDSCRT\_TYPE=FILE

# Path of the Node Secret.

**SDNDSCRT\_LOC=/home/rsa/securid**

# [This section is for event logger.]

# Logs event messages to the console.

RSA\_LOG\_TO\_CONSOLE=NO

# Logs event messages to a file.

RSA\_LOG\_TO\_FILE=YES

# Name of the log file.

RSA\_LOG\_FILE=rsa\_api.log

# Minimum severity level allowed to log.

RSA\_LOG\_LEVEL=INFO

# [This section is for debugger.]

# Enables debug tracing.

RSA\_ENABLE\_DEBUG=NO

# Sends tracing to the console.

RSA\_DEBUG\_TO\_CONSOLE=YES

# Sends tracing to a file.

RSA\_DEBUG\_TO\_FILE=NO

# Name of the trace file.

RSA\_DEBUG\_FILE=rsa\_api\_debug.log

# Allows function entry tracing.

RSA\_DEBUG\_ENTRY=YES

# Allows function exit tracing.

RSA\_DEBUG\_EXIT=YES

# Allows control flow tracing.

RSA\_DEBUG\_FLOW=YES

# Allows regular tracing.

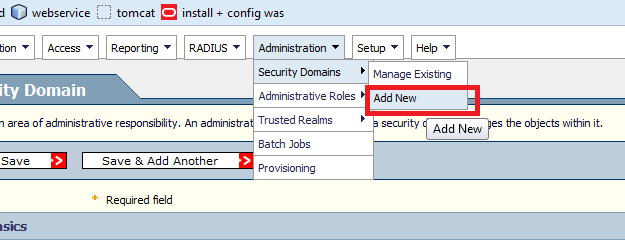
RSA\_DEBUG\_NORMAL=YES

# Traces the location.

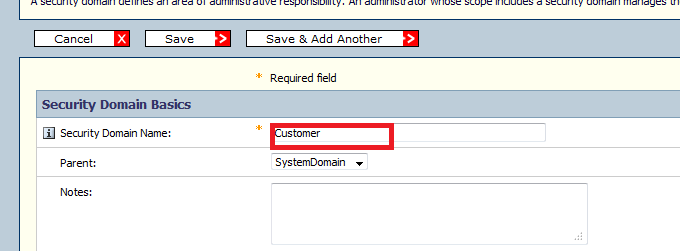
RSA\_DEBUG\_LOCATION=NO.

## Tạo Security domain Customer

Vào security console ->chọn Admintration -> Securitydomain ->Add new

 Nhập vào tên domain Customer vào ô Security Domain Name,

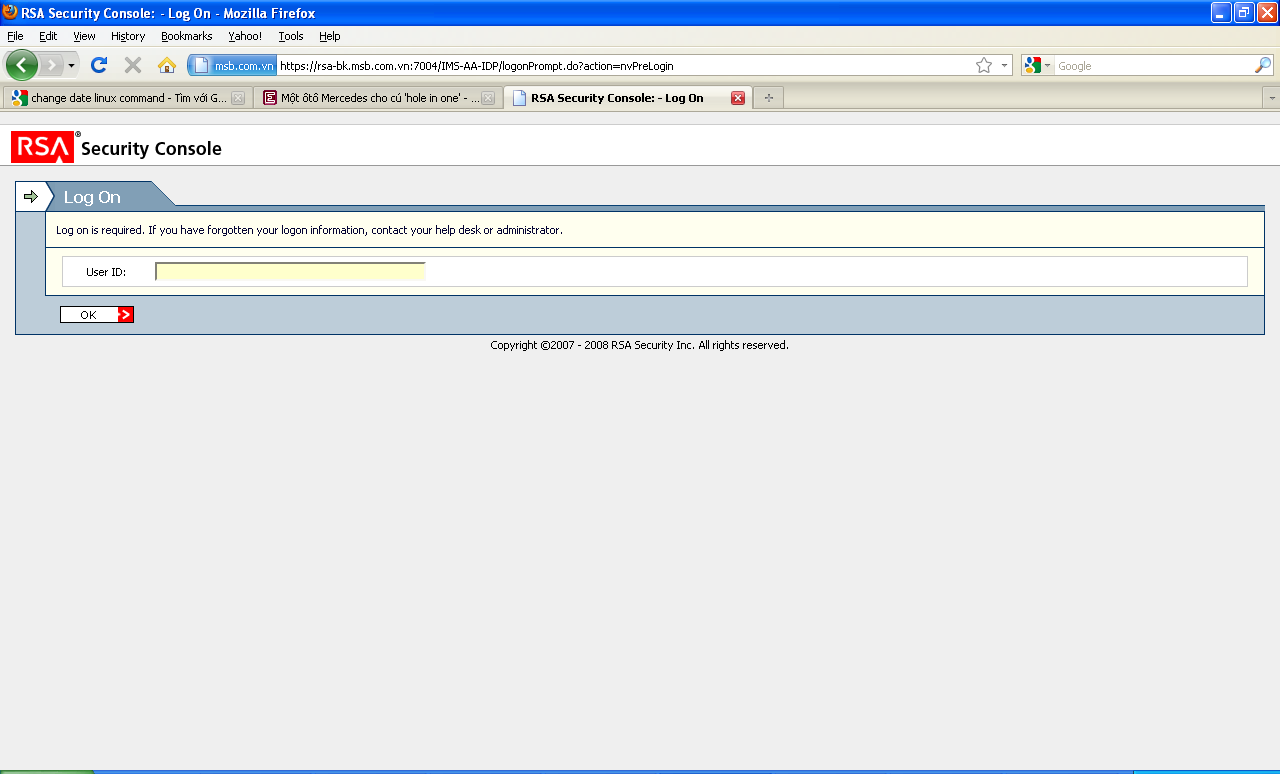
Vào security console ->chọn Admintration -> Securitydomain

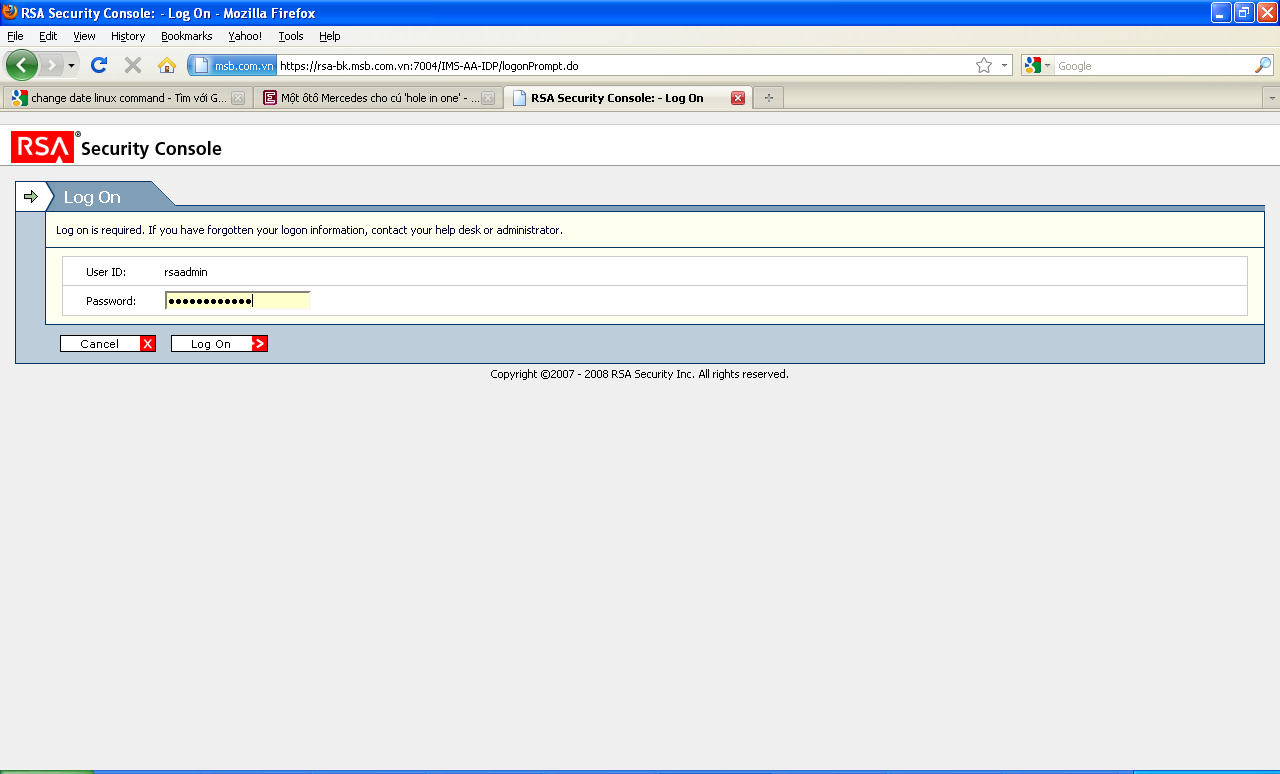


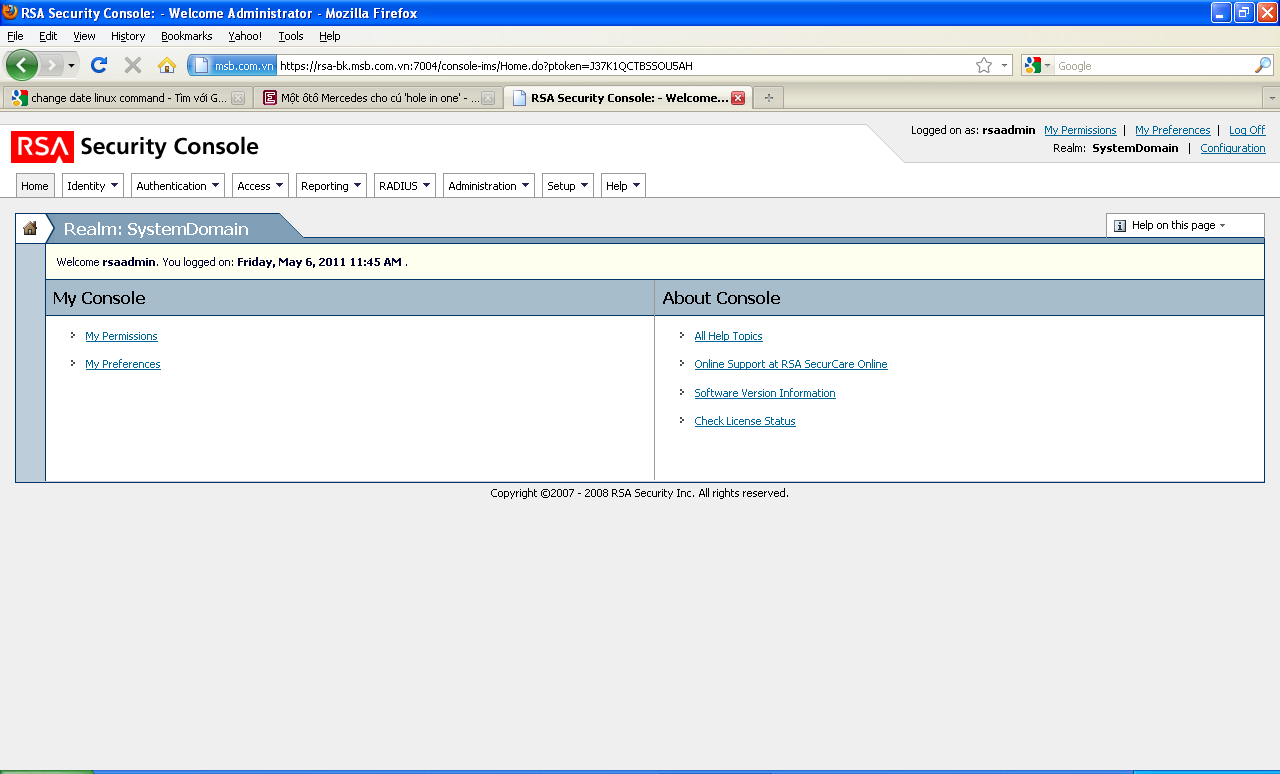
Click save.

## Tạo và gán quyền cho user apiadmin

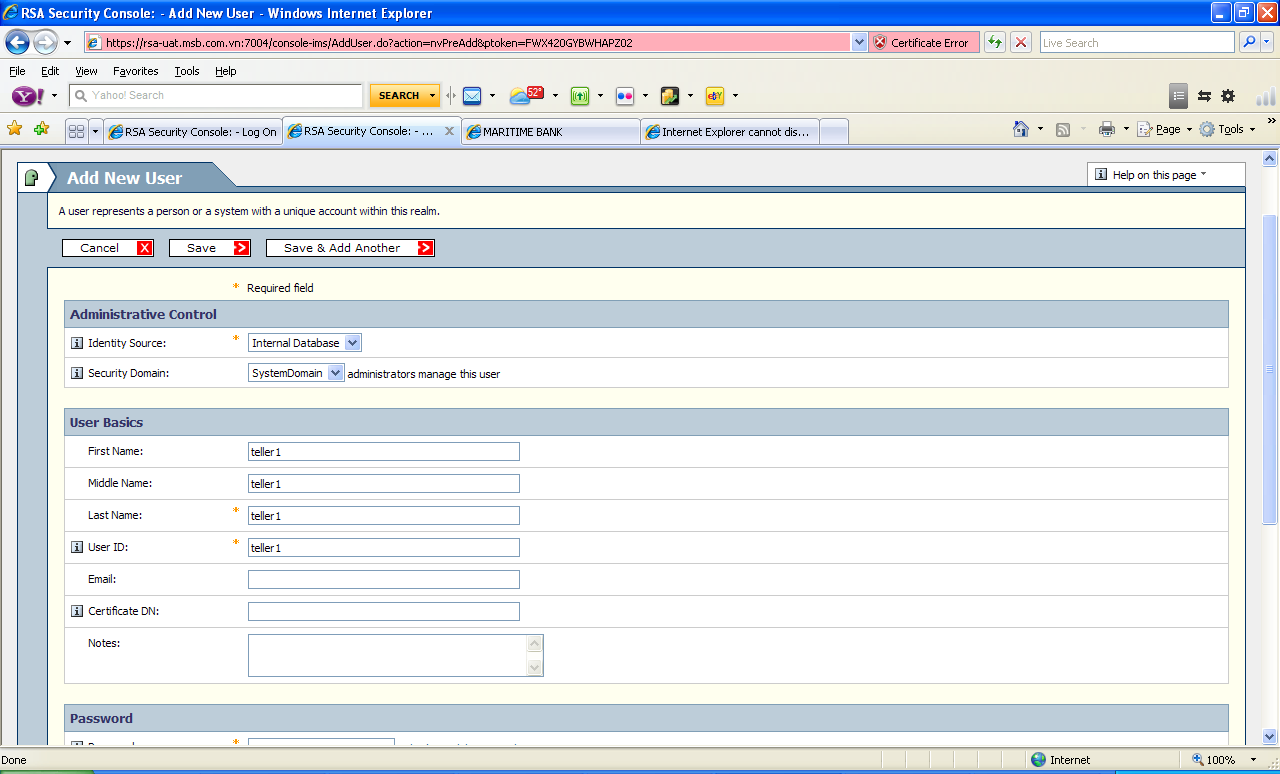
Vào https://rsa-esb.msb.com.vn:7004/console-ims/

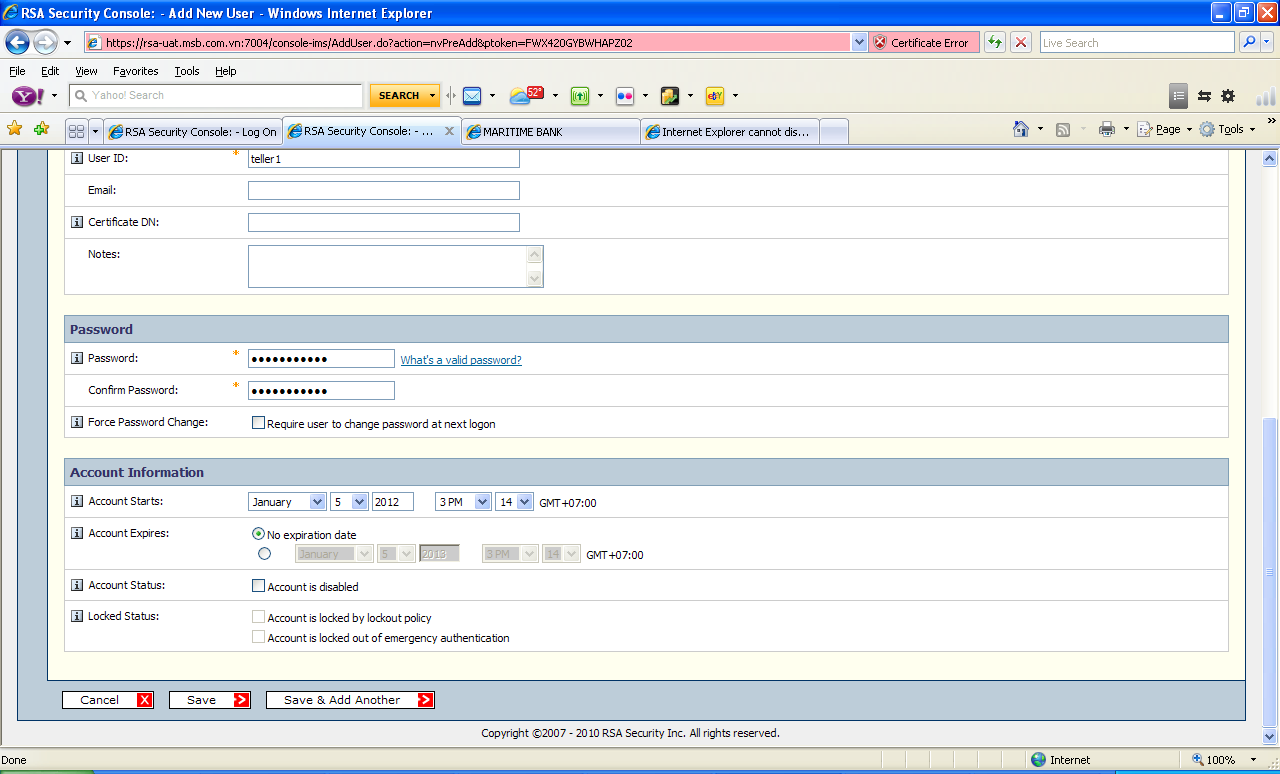




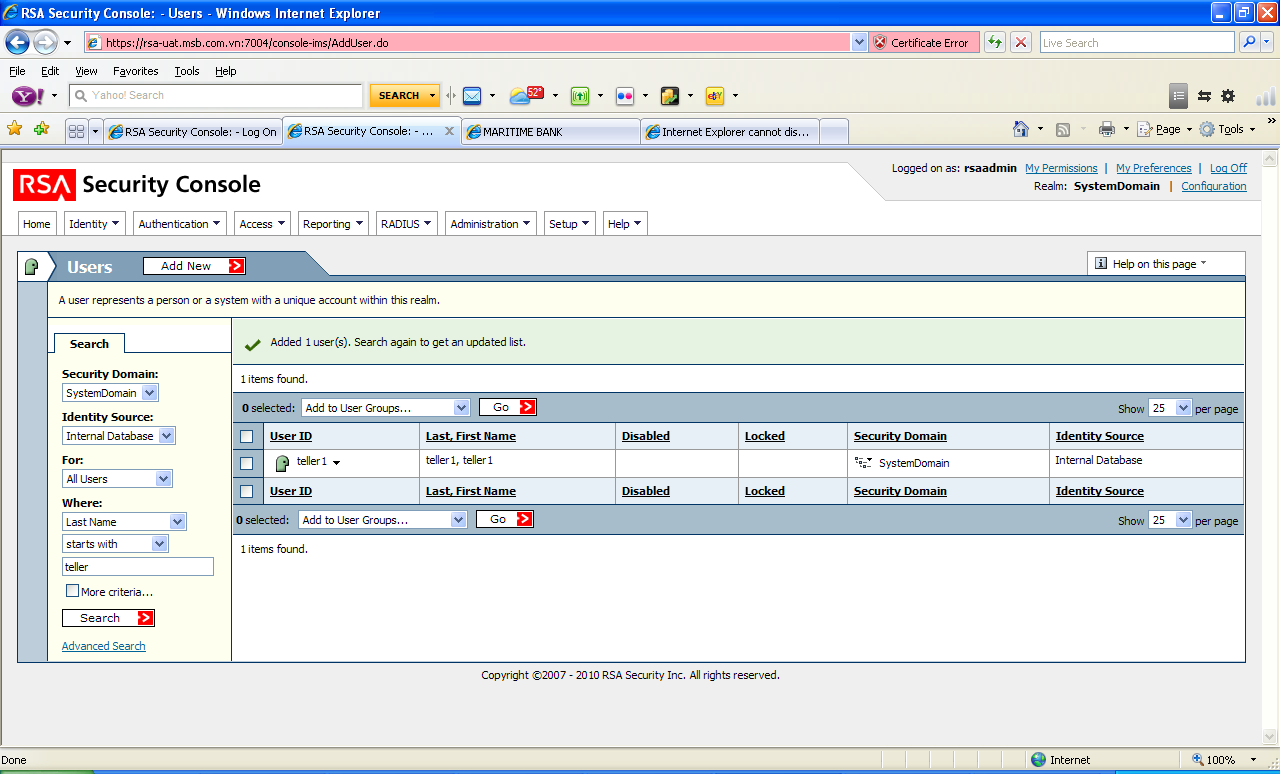


Vào menu Identity 🡪 Users 🡪 Add New

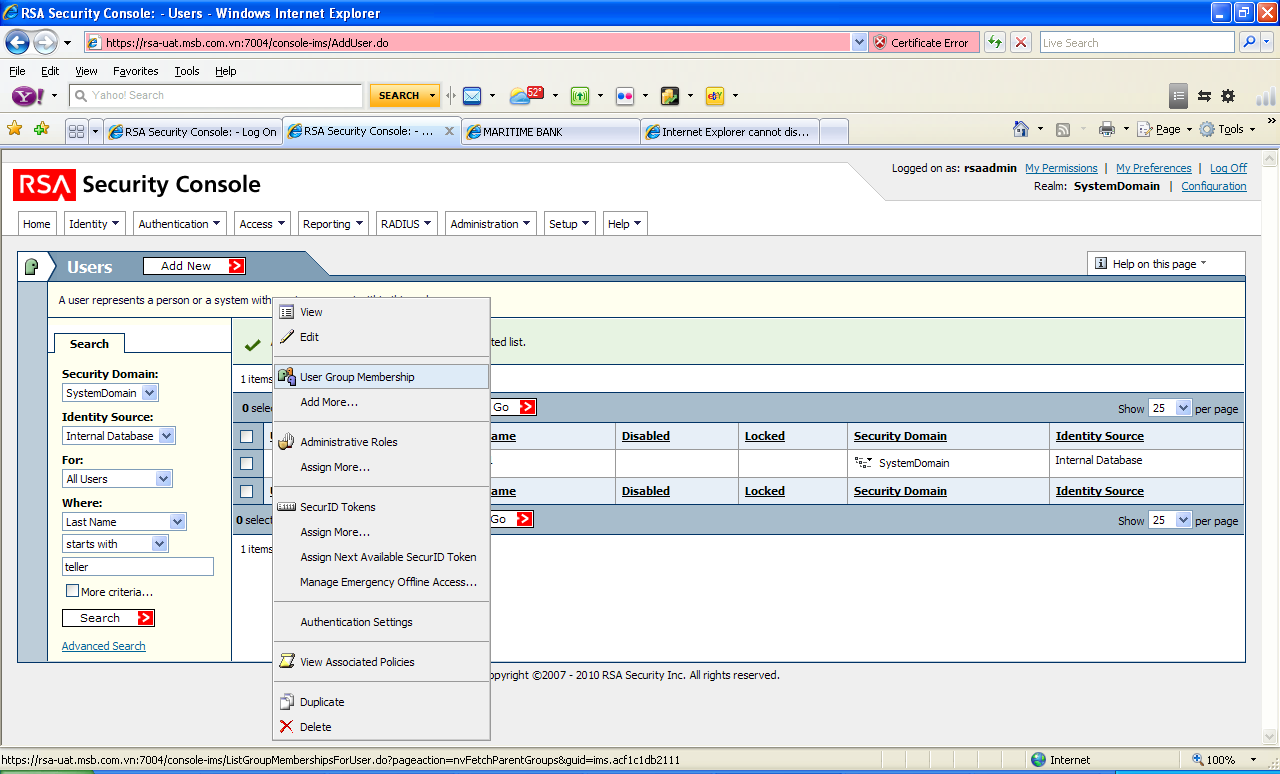


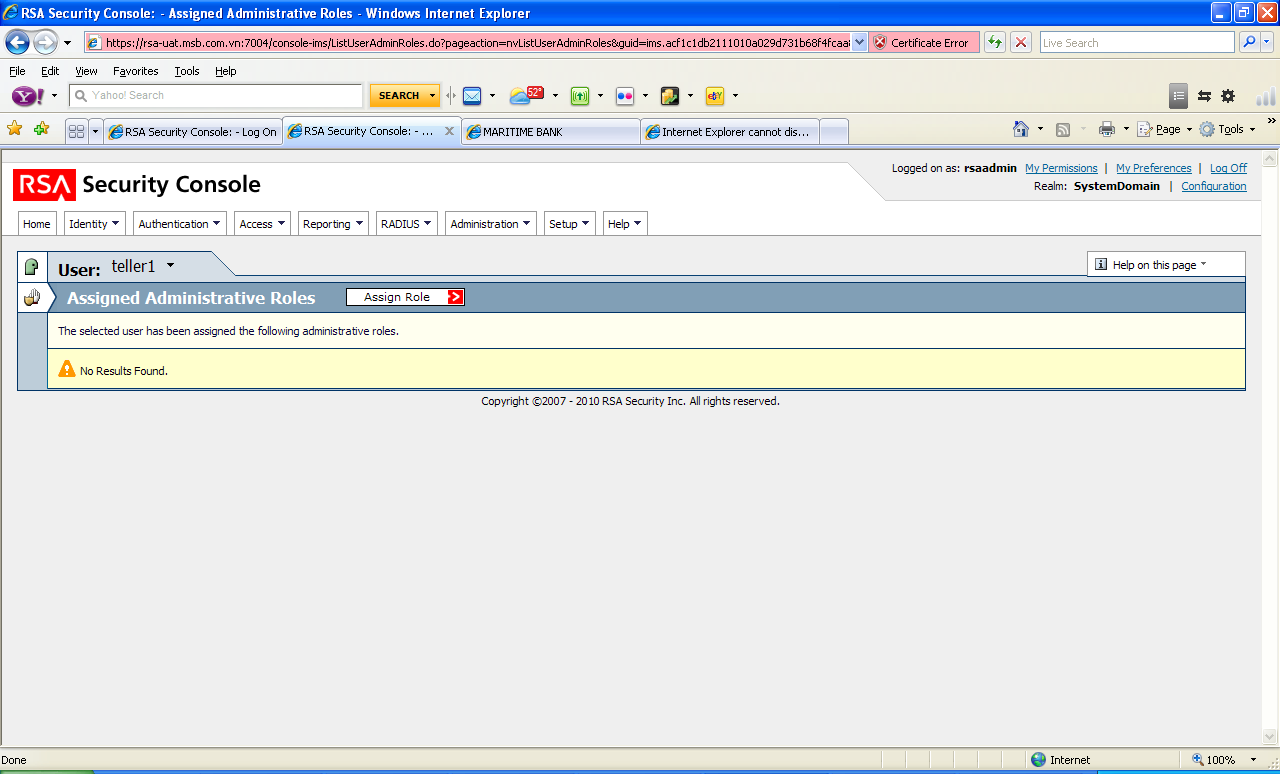


Nhập các thông tin vào, click Save, sẽ hiển thị màn hình:

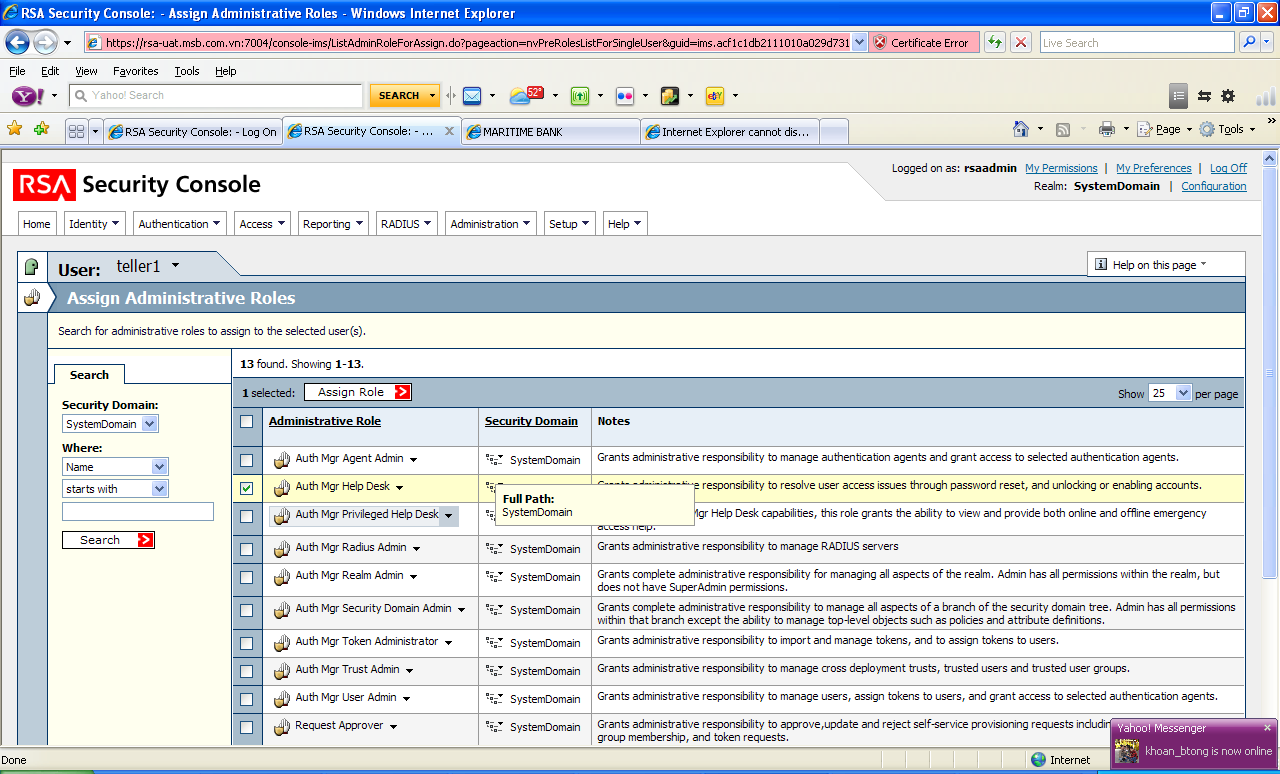


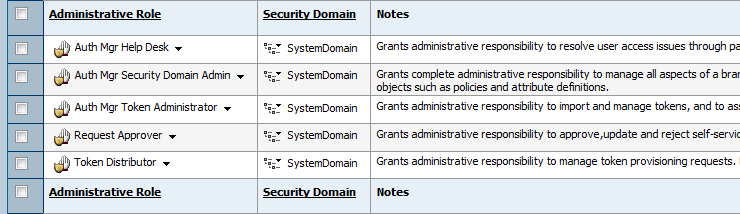
Click vào mũi tên xuống cạnh tên user, chọn Administrative Roles:





Chọn Assign Roles button:





Chọn các quyền giống hình trên .Sau đó click ->Assign role.

Note: Đây là quyền admin nên phải nhớ pasword để đăng nhập.

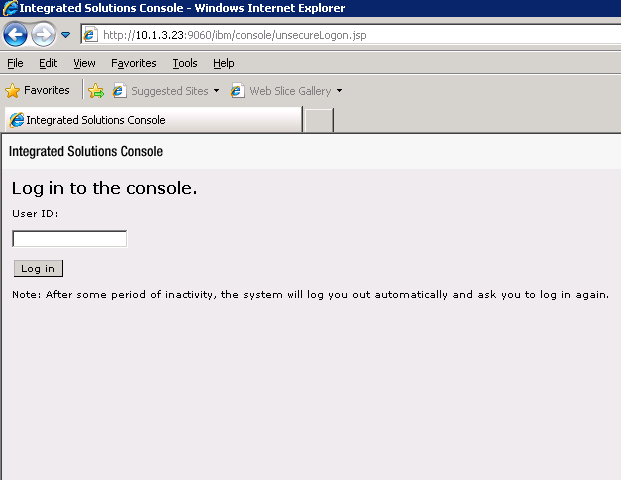
# Deploy ứng dụng TAXGW lên WAS

## Deploy

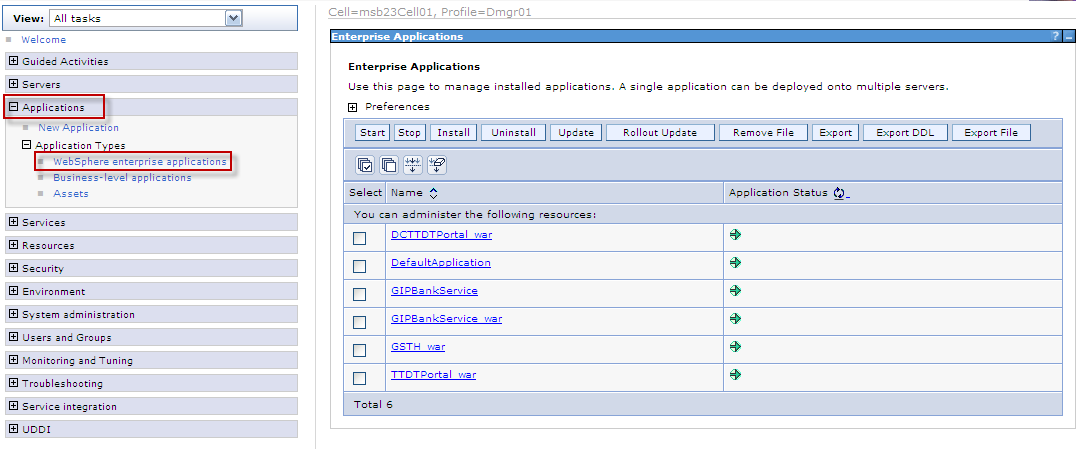
Vào <http://10.1.3.23:9060/ibm/console/login.do>

Thay 10.1.3.23:9060 = địa chỉ ip máy server và port

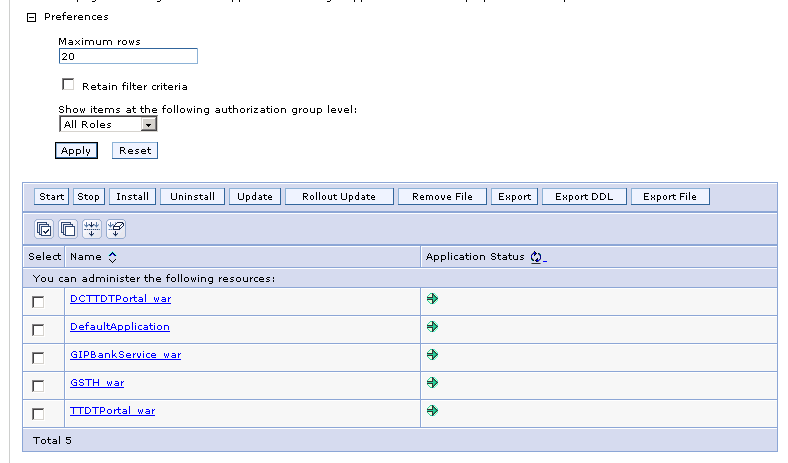
Click login



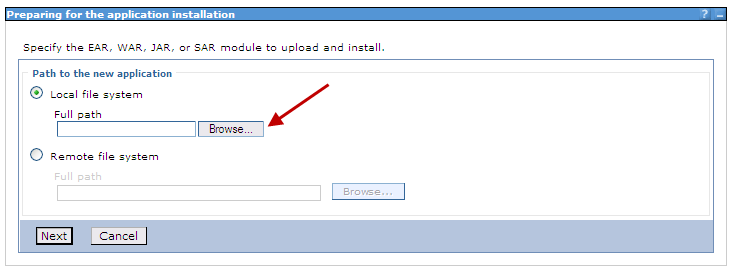
Chọn WebSphere enterprise aplication



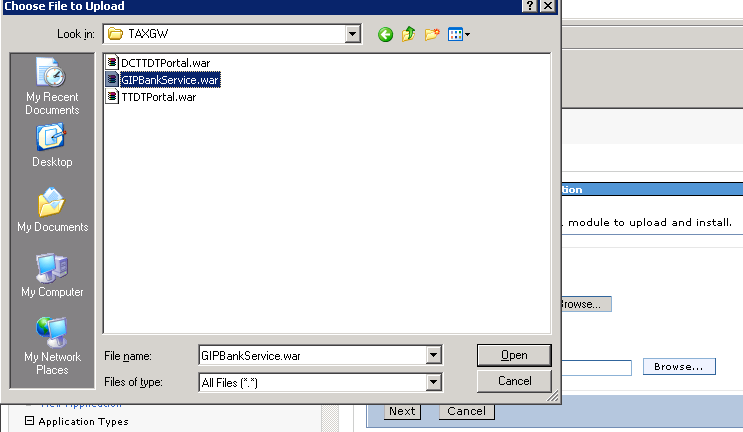
Chọn install



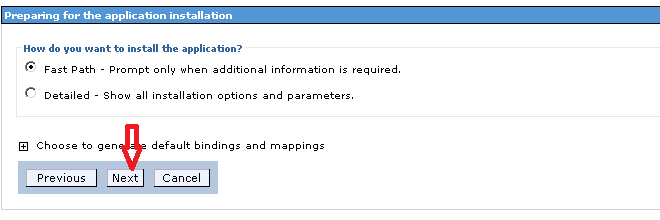
Click chọn đường dẫn đến file .war



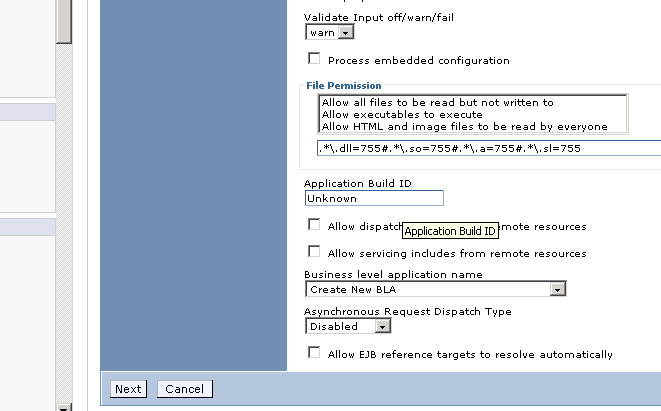
Chọn file .war -> Sau đó nhấn next



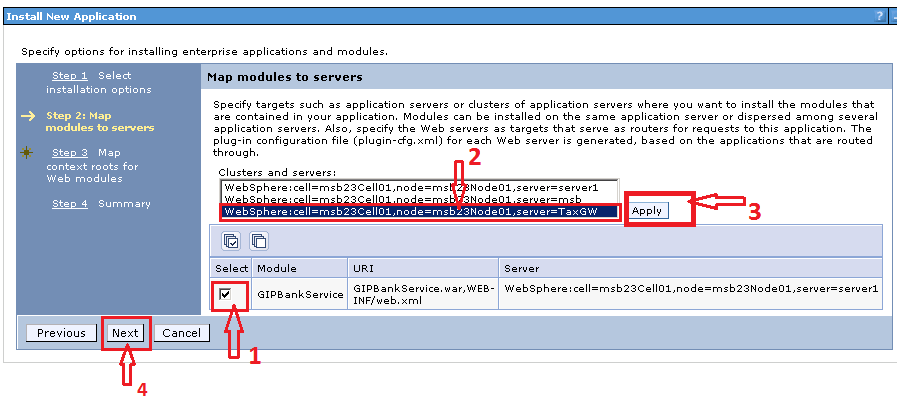
* Next



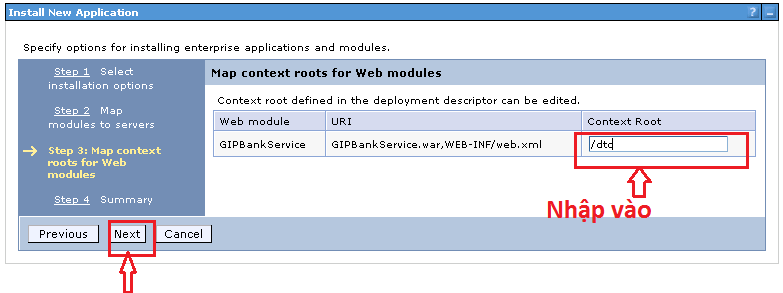
->click next



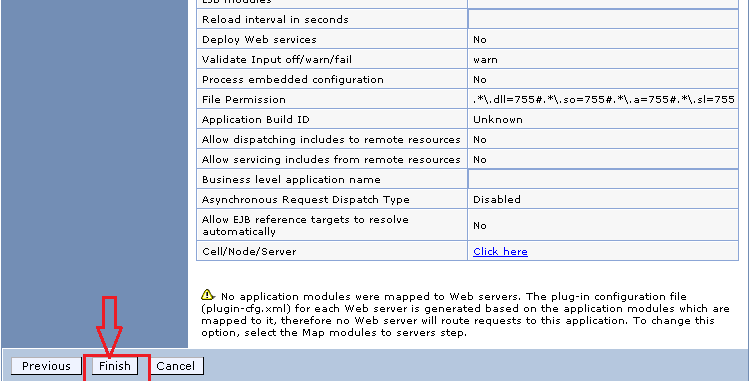
->Làm theo hình dưới



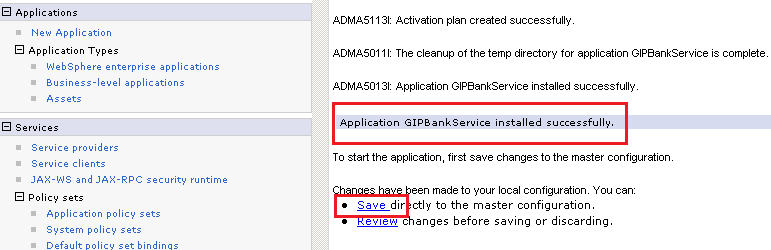
->Nhập vào đường dẫn



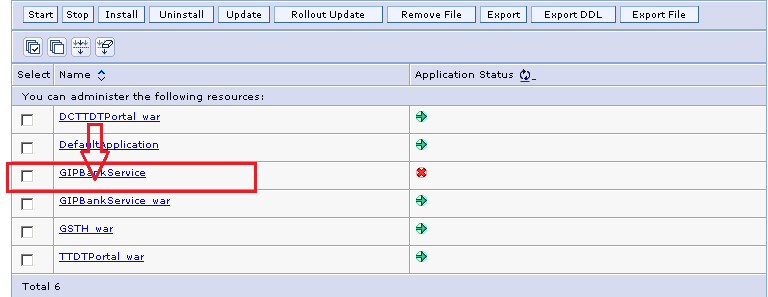
Click finish



Chờ quá trình install -> sau đó sẽ thấy kết quả như hình dưới-> click save



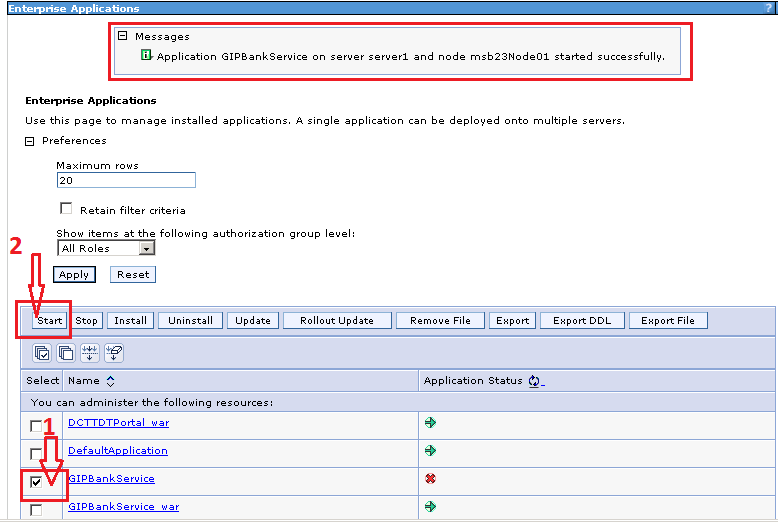
Click vào aplication mới deploy lên server để xem thông tin



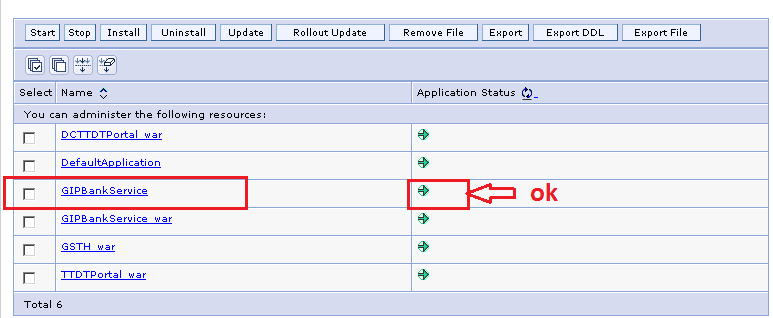
* xem các thông tin về ứng dụng.sau đó click-> ok ->và chọn save ở màn hình tiếp theo



Tích chọn ứng dụng rồi nhấn start



Nếu trạng thái của ứng dụng có màu xanh nghĩa là ứng dụng đã được start thành công



## Kiểm tra ứng dụng GIPBankSevice kết nối cổng thuế

Kiểm tra URL trên IE nếu thành công sẽ có hình như bên dưới:

<http://10.1.3.23:9081/gip/GIPBankServiceService/WEB-INF/wsdl/GIPBankServiceService.wsdl>



## Kiểm tra ứng dụng service kết nối hải quan lấy thông tin

Gõ vào IE URL <http://10.1.3.23:9081/tt/TTDTPortalService/WEB-INF/wsdl/TTDTPortalService.wsdl> nếu thành công sẽ có giao diện như hình dưới



## Kiểm tra sevice kết nối hải quan để đối chiếu

Gõ vào IE URL <http://10.1.3.23:9081/dc/DCTTDTPortalService/WEB-INF/wsdl/DCTTDTPortalService.wsdl>

Nếu thành công sẽ có giao diện như bên dưới

