

# This tutorial will teach you how to test Orbix SSL server with UCS.

## Use Orbix SSL bank demo as an example

When Orbix6 was installed, there will be a bank demo.

%Orbix\_HOME%\asp\6.3\demos\corba\tls\bank

If you want to run this demo with SSL, you need to configure following:

```
bank_server
{
    # This scope is used for the security unaware demos/tls/bank/cxx_server
    # application
    # This server is taking responsibility for setting up its own credentials.
    # This is a fully secure server that does not authenticate clients.
    orb_plugins = ["iiop_profile", "giop", "iioptls", "local_log_stream"];
    policies:target_secure_invocation_policy:requires = ["Confidentiality"];
    policies:target_secure_invocation_policy:supports = ["NoProtection","Confidentiality",
        "Integrity", "DetectReplay", "DetectMisordering", "EstablishTrustInTarget"];
    principal_sponsor:use_principal_sponsor = "true";
    principal_sponsor:auth_method_id = "pkcs12_file";
    principal_sponsor:auth_method_data =
["filename=% {product_dir}/asp/6.3/etc/tls/x509/certs/demos/bank_server.p12",
    "password=bankserverpass"];
};

bank_client
{
    # This scope is used for the security unaware demos/tls/bank/cxx_client
    # application
    # This client does not use any credentials
    # This is a fully secure client, it will authenticate servers it contacts.
    orb_plugins = ["iiop_profile", "giop", "iioptls", "local_log_stream"];
    x509_cert_root = "% {product_dir}/asp/6.3/etc/tls/x509";
    policies:trusted_ca_list_policy =
"% {product_dir}/asp/6.3/etc/tls/x509/trusted_ca_lists/ca_list1.pem";
    principal_sponsor:use_principal_sponsor = "true";
    policies:client_secure_invocation_policy:requires = ["Confidentiality"];
    policies:client_secure_invocation_policy:supports = [
    "NoProtection","Confidentiality", "Integrity", "DetectReplay",
    "DetectMisordering", "EstablishTrustInClient", "EstablishTrustInTarget"];
};
```

Then you can run this demo with following commands:

```
server -ORBname bank_server
```

```
client -ORBname bank_client
```

```
C:\WINDOWS\system32\cmd.exe - cxx_client\client -ORBname bank_client
2 - find_account
Selection [0-2]: ^C
D:\orbix633\asp\6.3\demos\corba\tls\bank>cxx_client\client -ORBname bank_client
Initializing ORB
Reading object reference from ../bank.ior

0 - quit
1 - create_account
2 - find_account
Selection [0-2]: 1
Enter account name: tony
Using account named tony

0 - quit
1 - get the name
2 - get the balance attribute
3 - call deposit operation
4 - call withdraw operation
Selection [0-4]:

C:\WINDOWS\system32\cmd.exe - cxx_server\server -ORBname bank_server
D:\orbix633\asp\6.3\demos\corba\tls\bank>cxx_server\server -ORBname bank_serv
Initializing the ORB
Creating the Account POA
Writing stringified object reference to ../bank.ior
Activating the POA Manager
Giving control to the ORB to process requests
create_account: Created account with name: tony
name: returning value tony
```

## Import Orbix server's certificate

In above example, the bank demo uses a certificate named bank\_server.p12. This is a pk12 format certificate. You have to change it to jks format that UCS can recognize. Fortunately, UCS shipped this kind of tools.

```
java -classpath ./lib/CorbaMNQ.jar com.corba.mnq.ssl.PKCS12Import bank_server.p12 keystore.jks
```

```
C:\WINDOWS\system32\cmd.exe - java -classpath ./lib/CorbaMNQ.jar com.corba.mnq.ssl.PKCS12Imp...
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.

d:\myjava\ucs>java -classpath ./lib/CorbaMNQ.jar com.corba.mnq.ssl.PKCS12Import
bank_server.p12 keystore.jks
Enter input keystore passphrase: _
```

Input bankserverpass as password.

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.

d:\myjava\ucs>java -classpath ./lib/CorbaMNQ.jar com.corba.mnq.ssl.PKCS12Import
bank_server.p12 keystore.jks
Enter input keystore passphrase: bankserverpass
Enter output keystore passphrase: bankserverpass
Alias 0:
Adding key for alias

d:\myjava\ucs>
```

Now you can get a jks format certificate named keystore.jks.

