Installation and Configuration Guide

iPlanet Trustbase Transaction Manager

Version 2.2.1

March 2001

Contents

Table of Figures

Chapter 1

Introduction

The following chapter discusses all related documents to this guide.

Overall Layout

The complete documentation set comprises of:

- iTTM2.2-Utility-Guide.pdf that provides some tools for helping with PKI Certificate Management.

- iTTM2.2-Install-Configuration-Guide.pdf (this Document) is designed for operators looking to produce applications that utilise the iPlanet Trustbase Transaction Manager framework. It is designed to provide information for operators looking to install the iPlanet Trustbase Transaction Manager platform. This guide identifies hardware and software required prior to installation, how to install iPlanet Trustbase Transaction Manager from CD-ROM

- iTTM2.2-Developer-Guide.pdf that indicates how to build and deploy your own services.

This manual Covers:

- Overview of the Installation
- Detailed Installation procedures
- Hardware Architectural Considerations
- Dynamic Configuration

Related Documents

Solaris 8 and Java Development Kit 1.2.1

http://docs.sun.com

http://java.sun.com/products/jdk/1.1/docs/index.html

iPlanet Application Server 4.1

http://docs.iplanet.com/docs/manuals/ias.html

iPlanet Web Server 6.0

http://docs.iplanet.com/docs/manuals/enterprise.html

iPlanet Certificate Management System

http://docs.iplanet.com/docs/manuals/cms.html

Oracle 8i Installation and Configuration Guides

http://www.oracle.com

Hardware Security nCipher KeySafe 1.0 and CAFast

http://www.ncipher.com

Identrus Message Specifications

http://www.identrus.com

Transaction Coordinator requirements (IT-TCFUNC)

Core messaging specification (IT-TCMPD)

Certificate Status Check Messaging specification (IT-TCCSC)

Chapter 2

Installation Worksheet

Installation Worksheet provides the user with a pre-requisite checklist of all the main features to a successful iPlanet™ Trustbase Transaction Manager installation. It lists software that is included, what isn't included, what must be downloaded and how it should be installed and configured.

Installation Outline

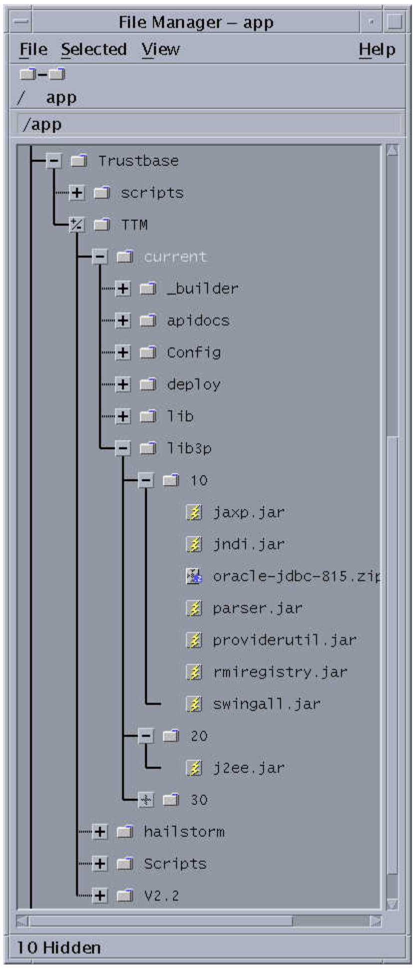
The following steps need to be carried out:

- Check and meet software pre-requisites
- Download any software that has not been included with iPlanet™ Trustbase Transaction Manager.
- Install iPlanet™ Web Server v4.1
- Install iPlanet™ Application Server v6.0
- Install iPlanet™ Trustbase Transaction Manager v2.2 with Identrus Extensions
- Setup nFast Hardware and configure iPlanet™ Trustbase Transaction Manager to use it
- Setup Oracle 8i database schema
- Setup site specific Identrus settings
- Start iPlanet™ Trustbase Transaction Manager
- Acquire Identrus Certificates and Keys using CertManager

SW pre-requisites

The following software should be installed prior to running iPlanet™ Trustbase Transaction Manager.

Figure 1 Third Party Library jar files



```
Trustbase
  scripts
  TTM
    current
      _builder
      apidocs
      Config
      deploy
      lib
      lib3p
        10
          jaxp.jar
          jndi.jar
          oracle-jdbc-815.zip
          parser.jar
          providerutil.jar
          rmiregistry.jar
          swingall.jar
        20
          j2ee.jar
        30
    hailstorm
    Scripts
    V2.2
```

Pre-requisites

- Microsoft's Browser: Internet Explorer 4.0 or above for Web configuration or Netscape 4.0 and higher.
- Oracle 8i.
- The iPlanet™ Trustbase Transaction Manager 2.2 requires the Solaris 8 Operating Environment system and the JDK 1.2 environment or the Java™ Runtime Environment 1.2.
- The iPlanet™ Trustbase Transaction Manager 2.2 requires the use of JDK 1.2 environment. This can be obtained from the Sun Microsystems Web site http://www.javasoft.com
- JDBC™ for Oracle 8i http://www.oracle.com/java/jdbc/html/jdbc.html
- Java™ Servlet supporting WebServer
    - iPlanet™ Web Server 4.1 http://www.iplanet™com/products/infrastructure/web_servers/index.html
- Application Server
    - iPlanet™ Application Server 6.0 http://www.iplanet™com/products/infrastructure/app_servers/index.html
- An Identrus Compliant Validation Authority
- An Identrus Compliant Certificate Authority
- Hardware Security Module
    - nCipher KeySafe 1.0 http://www.ncipher.com

Packages included

The following packages are included with iPlanet™ Trustbase Transaction Manager:

- iPlanet™ Application Server 6.0 http://www.iplanet™com/products/infrastructure/app_servers/index.html
- iPlanet™ Web Server 4.1 http://www.iplanet™com/products/infrastructure/web_servers/index.html
- Java™ API for XML Parsing http://java.sun.com/xml

Packages not included

The following software must be downloaded before Installation:

- JDBC™ -Thin / 100% Java API for JDK™ 1.1.x http://technet.oracle.com/software/download.htm oracle-jdbc-815.zip.
- The Solaris 8 operating system environment incorporating the JDK ™ 1.2 environment

Certificate Prerequisites

Before you install iPlanet™ Trustbase Transaction Manager, you will need to know the location of your level 1 Certificate Authority PEM encoded CA certificate. This certificate is referred to from this point forward as the L1CA certificate.

Note All third party software should be placed in lib3p/10 as illustrated in Figure 1 Third Party Library jar files

System Resources

- Determine hostname

```
hostname
domainname
```

- Verify disk space to be greater than 1GB.

```
df -k
```

- Verify sufficient memory is not less than 256MB and preferably the recommended 1GB

```
prtconf | grep Mem
```

- Check Solaris version is 8

```
uname -a
```

- Check Java Version is 1.2

```
java -version
```

Solaris Installation

Before iPlanet™ Trustbase Transaction Manager can be installed, a working web server and application server must be available.

IPlanet Web Server v4.1 Installation

- Logon as root, locate the 'setup' script depending on distribution
- Start the installation using the ‘setup’ script.
- Select a directory <install_directory> to install the webserver into, this will need to be the same directory you wish to use for the iPlanet™ Application Server installation later.

```
# cd /cdrom/cdrom0
# cd iWS
#./setup
```

- Install all elements of the web server and select the option that changes their ownership/group to ‘nobody’. Select the option that runs the webserver as ‘root’. Do not use an existing Directory service. Select the web server document directory to be the ‘docs’ subdirectory of your chosen installation location. Do not use your own JDK when prompted.

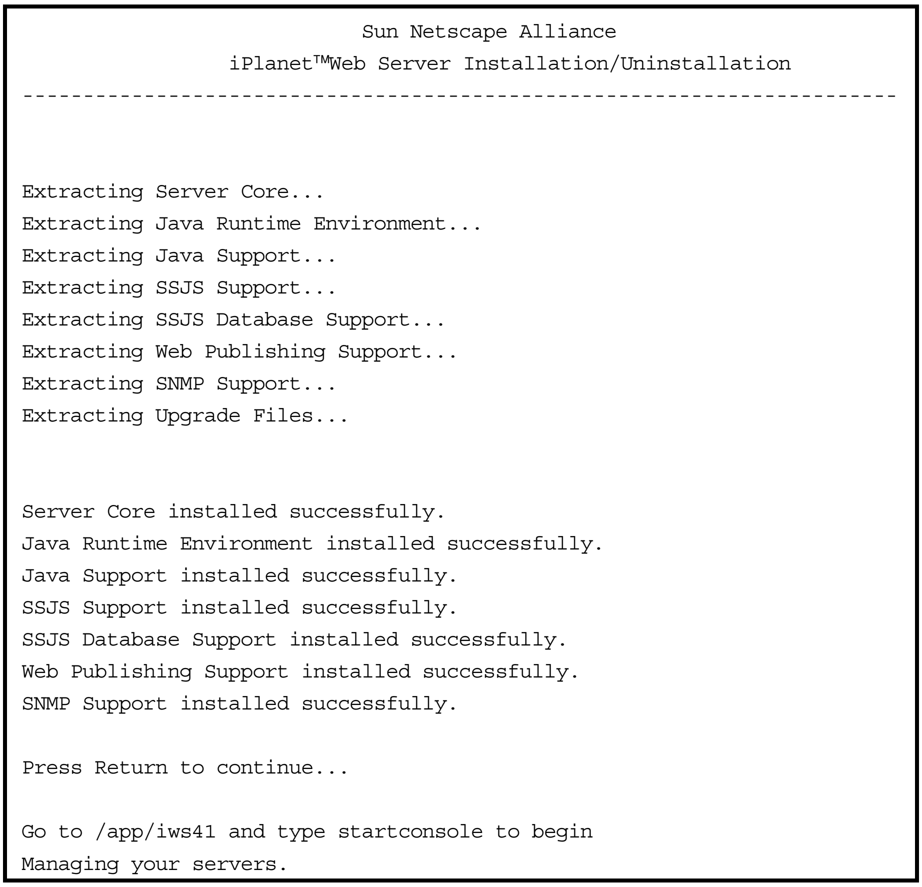
Figure 2 Installing iPlanet™Web Server

```
Would you like to continue with installation? [Yes]: Yes
Do you agree to the license terms? [Yes]: Yes
Choose an installation type [2]: 2
Install location [/usr/netscape/server4]: /app/iws41
Specify the components you wish to install [A] A
Specify the components to install [1, 2, 3, 4, 5, 6, 8]: 1,2,3,4,5,6,8
Computer name [rainstorm.jcp.co.uk]: rainstorm.jcp.co.uk
System User [nobody]: nobody
System Group [nobody]: nobody
Run iWS Administration Server as [root]: root
IWS Admin Server User Name [admin]: admin
IWS Admin Server Password:
IWS Admin Server Password (again):
IWS Admin Server Port [8888]: 8888
Web Server Port [80]: 80
Do you want to register this with an existing Directory Server [No]: No
Web Server Content Root [/app/iws41/docs]:
Do you want to use your own JDK [No]: No
```

Note You should make a note of these settings. Particularly port numbers since you may need them later.

- The following output should appear:

Figure 3 iPlanet™Web Server Installed



```
                            Sun Netscape Alliance
                 iPlanet™Web Server Installation/Uninstallation
------------------------------------------------------------------------



Extracting Server Core...
Extracting Java Runtime Environment...
Extracting Java Support...
Extracting SSJS Support...
Extracting SSJS Database Support...
Extracting Web Publishing Support...
Extracting SNMP Support...
Extracting Upgrade Files...


Server Core installed successfully.
Java Runtime Environment installed successfully.
Java Support installed successfully.
SSJS Support installed successfully.
SSJS Database Support installed successfully.
Web Publishing Support installed successfully.
SNMP Support installed successfully.

Press Return to continue...

Go to /app/iws41 and type startconsole to begin
Managing your servers.
```

Note Please consult your iPlanet™ Web Server Installation Guide for more information on this. Selecting <return> takes the default.

Starting iPlanet™ Web Server 4.1

Change into the directory that contains your Web Server instance amd run the start script. This directory takes the form of https-<machine-name>.domain.

For instance:

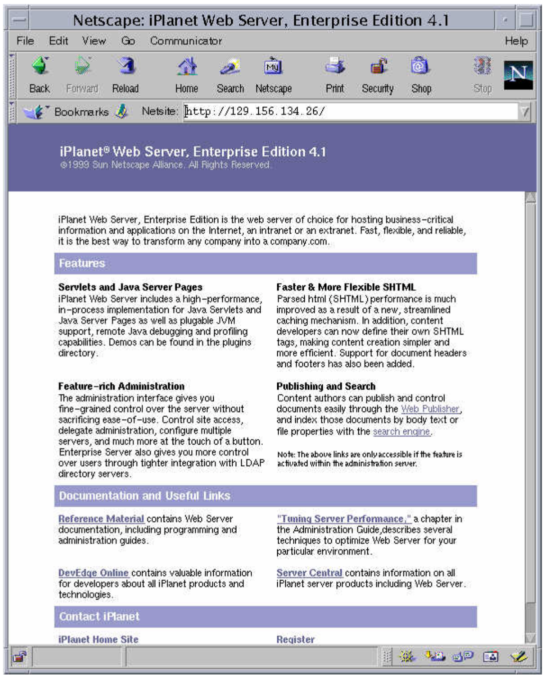
```
cd /app/iws41/https-whelk.jcp.co.uk
./start
```

Note If in doubt you should consult the first chapter of the iPlanet™ Web Server configuration Guide.

Verifying iPlanet Web Server 4.1

Check iPlanet™ Web Server is working by opening a browser window to http://localhost. If its working you'll see the main page as illustrated below:

Figure 4 iPlanet Web Server, Enterprise Edition 4.1



http://129.156.134.26/

iPlanet® Web Server, Enterprise Edition 4.1
©1999 Sun Netscape Alliance. All Rights Reserved.

iPlanet Web Server, Enterprise Edition is the web server of choice for hosting business-critical information and applications on the Internet, an intranet or an extranet. Fast, flexible, and reliable, it is the best way to transform any company into a company.com.

Features

Servlets and Java Server Pages
iPlanet Web Server includes a high-performance, in-process implementation for Java Servlets and Java Server Pages as well as plugable JVM support, remote Java debugging and profiling capabilities. Demos can be found in the plugins directory.

Feature-rich Administration
The administration interface gives you fine-grained control over the server without sacrificing ease-of-use. Control site access, delegate administration, configure multiple servers, and much more at the touch of a button. Enterprise Server also gives you more control over users through tighter integration with LDAP directory servers.

Faster & More Flexible SHTML
Parsed html (SHTML) performance is much improved as a result of a new, streamlined caching mechanism. In addition, content developers can now define their own SHTML tags, making content creation simpler and more efficient. Support for document headers and footers has also been added.

Publishing and Search
Content authors can publish and control documents easily through the Web Publisher, and index those documents by body text or file properties with the search engine.

Note: The above links are only accessible if the feature is activated within the administration server.

Documentation and Useful Links

Reference Material contains Web Server documentation, including programming and administration guides.

DevEdge Online contains valuable information for developers about all iPlanet products and technologies.

"Tuning Server Performance," a chapter in the Administration Guide,describes several techniques to optimize Web Server for your particular environment.

Server Central contains information on all iPlanet server products including Web Server.

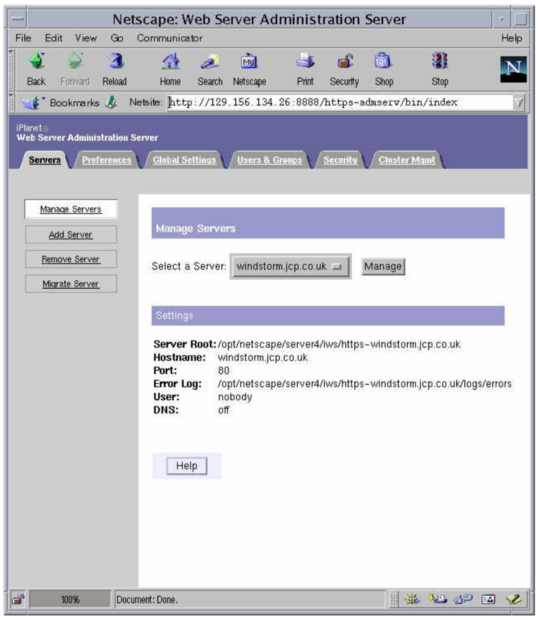
Contact iPlanet

iPlanet Home Site

Register

Or alternatively going straight to the Administration Server console:

Figure 5 iPlanet Web Server Administration Server



http://129.156.134.26:8888/https-admserv/bin/index

Manage Servers

Select a Server: windstorm.jcp.co.uk

Settings

Server Root: /opt/netscape/server4/iws/https-windstorm.jcp.co.uk
Hostname: windstorm.jcp.co.uk
Port: 80
Error Log: /opt/netscape/server4/iws/https-windstorm.jcp.co.uk/logs/errors
User: nobody
DNS: off

iPlanet Application Server v6.0 Installation

- Ensure that the iPlanet Web Server is running before you follow this procedure.

- Logon as root, locate the 'setup' script depending on distribution (e.g. unzip the tar file and the 'setup' file should be in the top directory)

```
# cd /cdrom/cdrom0
# cd iAS
# ./setup
```

- Start the installation using the ‘setup’ script. And answer the questions as follows:

Figure 6 Example iPlanet Application Server Script

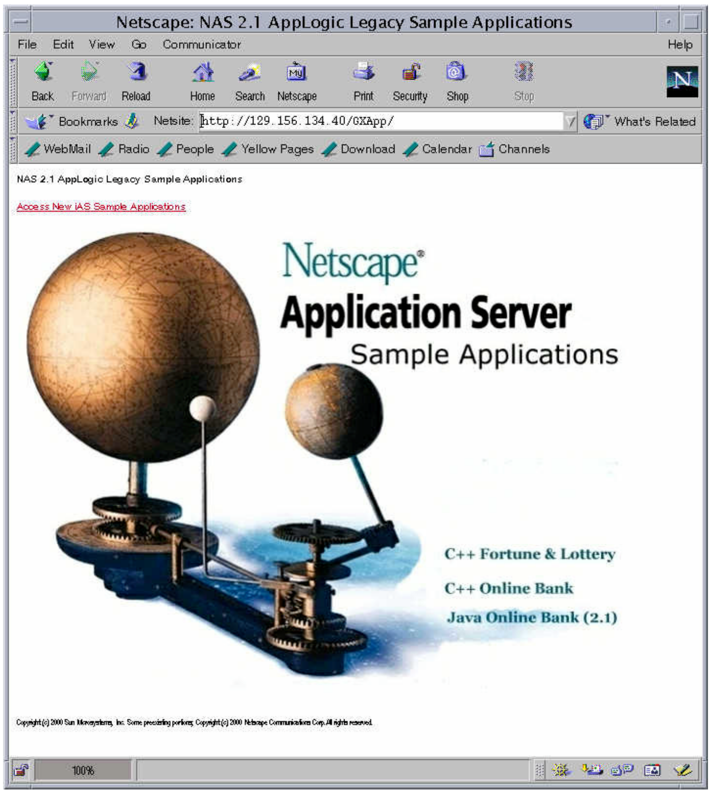
```
Would you like to continue with installation? [Yes]: Yes
Do you agree to the license terms? [No]: Yes
Select the component you want to install [1]: 1
Choose an installation type [2]: 2
Install location [/usr/iplanet/ias6]: /app/ias6
iPlanet Server Products components:  Specify the components to install [All]: All
iPlanet Server Family Core: Specify the components to install [1, 2, 3]: 1,2,3
iPlanet Directory Suite components: Specify the components to install [1, 2]: 1,2
Administration Services components: Specify the components to install [1, 2]: 1,2
iPlanet Application Server Suite components: Specify the components you wish to install
[1, 2, 3, 4]: 1,2,3,4
Computer name [rainstorm.jcp.co.uk]: rainstorm.jcp.co.uk
System User [nobody]: nobody
System Group [nobody]: nobody
Netscape configuration directory server? [No]: No
Do you want to use another directory to store your data? [No]: No
Directory server network port [389]: 389
Directory server identifier [rainstorm]: rainstorm
administrator ID [admin]: admin
Password:
Password (again):
Suffix [o=co.uk]: o=iplanet.com
Directory Manager DN [cn=Directory Manager]: cn=Directory Manager
Password:
Password (again):
Admin Domain [iplanet.com]:  iplanet.com
Administration port [12816]: 12816
Run Administration Server as [root]: root
Product Key: 1111111111-3333333333
Enter the location of your webserver: /app/iws41/https rainstorm.jcp.co.uk
Do you want to enable the user to access the registry and plugin libraries ?  [y]  y
Do you want to continue with the iAS installation ?  [y]  y
Username [admin]: admin
Password:
Password (again):
Do you want to enable I18N support for iAS? [No]: No
Username does not match [No]: Yes
```

Note Please consult your iPlanet™ Application Server Installation Guide for more information on this. You should also make a note of these settings since you may need them later. Selecting <return> takes the default.

Post iPlanet Web Server and iPlanet Application Server Installation Steps

- To check that the Application Server installation has been successful, use a browser to contact the following URL: http://machine_name/GXApp Select the 'Java Fortune' application, if the reply indicates that the servlet 'Greets You' then the web server and application server are functioning correctly. You should also consult your iPlanet Application Server Installation Documentation. This is now illustrated below:

Figure 7 Verifying iPlanet Application Server



Netsite: http://129.156.134.40/GXApp/

NAS 2.1 AppLogic Legacy Sample Applications

Access New iAS Sample Applications

C++ Fortune & Lottery

C++ Online Bank

Java Online Bank (2.1)

Copyright (c) 2000 Sun Microsystems, Inc. Some preexisting portions Copyright (c) 2000 Netscape Communications Corp. All rights reserved.

- Having completed the installation, all processes must be shutdown:

- Logon as root

- Application Server Shutdown <install_directory>/ias/bin/KIVAes.sh stop

```
# cd /app/ias6/ias/bin
# ./KIVAes.sh stop
# ps -ef | grep k.s
```

Note: Immediately after installation, if this script fails to work, use 'ps –ef | grep k.s' to show all iPlanet Application Server processes and then 'kill –9 <pid>' to stop all of them.

- Directory Server Shutdown <install_directory>/slapd-<machine_name>/stop-slapd

```
# cd /app/ias6/slapd-<hostname>
# ./stop-slapd
# ps -ef | grep slap
```

- Web Server Shutdown

  - <install_directory>/https-<machine_name>/stop

  - and: <install_directory>/https-admserv/stop

```
# ./app/iws41/https-<machine_name>/stop
# ./app/iws41/https-admserv/stop
```

- Once all the above scripts have been run check that all processes have been terminated using ‘ps –ef | grep <install_directory>’. Use ‘kill –9 <pid>’ on all remaining processes.

Enabling SSL Connection logging

In order for iPlanet Trustbase Transaction Manager to fully log an SSL Connection, the following procedure needs to be adopted:

- Start kregedit

```
..../ias6/ias/bin/kregedit
```

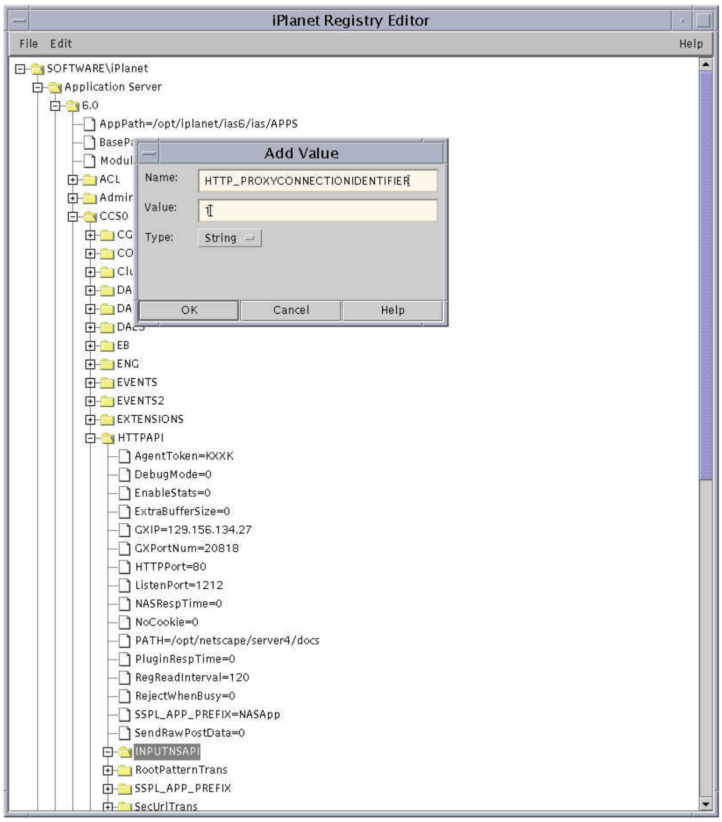
- Select the following node:

```
SOFTWARE\iPlanet\Application Server\6.0\CCS0\HTTPAPI\INPUTNSAPI
```

- Use the Edit menu to "Add Value" with the following attributes (Case Sensitive):

```
Name=HTTP_PROXYCONNECTIONIDENTIFIER
Value=1
Type=String
```

Figure 8 Kregedit and ConnectionId



```
SOFTWARE\iPlanet
  Application Server
    6.0
      AppPath=/opt/iplanet/ias6/ias/APPS
      BaseP
      Modul
      ACL
      Admir
      CCS0
        CG
        CO
        Clu
        DA
        DA
        DA
        EB
        ENG
        EVENTS
        EVENTS2
        EXTENSIONS
        HTTPAPI
          AgentToken=KXXK
          DebugMode=0
          EnableStats=0
          ExtraBufferSize=0
          GXIP=129.156.134.27
          GXPortNum=20818
          HTTPPort=80
          ListenPort=1212
          NASRespTime=0
          NoCookie=0
          PATH=/opt/netscape/server4/docs
          PluginRespTime=0
          RegReadInterval=120
          RejectWhenBusy=0
          SSPL_APP_PREFIX=NASApp
          SendRawPostData=0
          INPUTNSAPI
          RootPatternTrans
          SSPL_APP_PREFIX
          SecUrlTrans
```

Name: HTTP_PROXYCONNECTIONIDENTIFIER
Value: 1
Type: String

- Exit kregedit.

- This will not take effect until iPlanet Web Server and the iPlanet Application Server have been restarted. If you are following through these installation procedures this will be done in the Restart procedure on page 39

iPlanet Trustbase Transaction Manager Installation Process

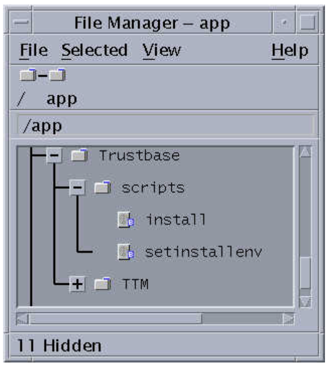
Now that iPlanet™ Web Server and iPlanet™ Application Server are installed the iPlanet™ Trustbase Transaction Manager installation can proceed.

The installation is provided as a "compress"-ed tar file. The installation program is designed for Unix Solaris 8. iPlanet™ Trustbase Transaction Manager currently requires JDK1.2 to be installed on your machine to operate correctly. To ensure iPlanet™ Trustbase Transaction Manager is installed correctly it is advised that you install JDK1.2 before iPlanet™ Trustbase Transaction Manager. Allow 100MB of Disc space for JDK 1.2 and iPlanet™ Trustbase Transaction Manager.

- Logon as root
- Change directory to a location where the iPlanet™ Trustbase Transaction Manager hierarchy is to be created
- Extract the compressed tar file to the current directory.

```
zcat iTTM-2.2.tar.Z | tar -xvpf -
cd Trustbase/scripts
```

Figure 9 Finding the install script



- Make sure the directory server for iPlanet Application Server is running before you install Trustbase. For example,

```
cd /app/ias6/slapd-<machine-name>
./start-slapd
```

- run ‘install’ and follow the instructions – when prompted for the iPlanet™ Application Server location – enter the directory used above <install_directory> In the example above this is /app/Trustbase/scripts

```
./install
```

Figure 10 Installing iPlanet™ Trustbase Transaction Manager illustrates how to install iPlanet™ Trustbase Transaction Manager:

Figure 10 Installing iPlanet™ Trustbase Transaction Manager

```
zcat iTTM-2.2.tar.Z | tar -xvpf -‘
cd Trustbase/scripts
./install

Copyright (C) 2000 Sun Microsystems, Inc. All rights reserved. Use of
this product is subject to license terms. Federal Acquisitions:
Commercial Software
--- Goverment Users Subject to Standard License Terms and Conditions.

Sun Microsystems, The Sun Logo, iPlanet Trustbase and Java are
trademarks or registered trademarks of Sun Microsystems, Inc. In The
United States and other countries.

Running Installation on sunstorm should I install Trustbase TTM [y/n] y
Trustbase Transaction Manager V2.2 installation script.
Where is your iPlanet Application Server 6.0 installation located?
/app/ias6
Where is your iPlanet Web Server 4.1 documents directory?
/app/iws41/docs
What is the Database User Name which will be used by Trustbase?
tbase
What is the Database Password which will be used by Trustbase?
tbase
On what host is your database stored? sunstorm.jcp.co.uk
On what port is your database running? 1521
On what SID is your database? orcl
What Cryptographic provider do you want to use: NCIPHER or JCP? JCP
On what URL is your local OCSP responder?
http://windstorm.jcp.co.uk:8080
What is the AIA of this TC? https://windstorm.jcp.co.uk
```

Note If you are installing the Proxy on a separate machine the AIA of this TC should point to the hostname of the Proxy and not the TC. See also the Section about Configuring the SSLproxy Separately on page 53

- iPlanet™ Trustbase Transaction Manager is now installed. Some further configuration is now required to establish the local settings and Identrus setup – see the following sections.

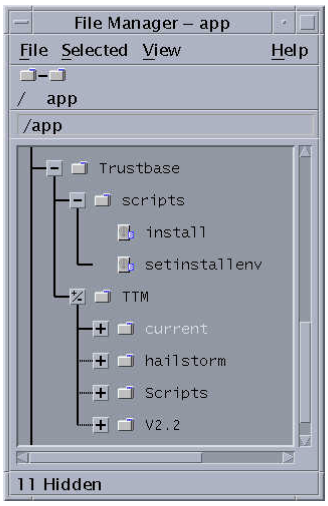
Note Select <Enter> to include the default. You should make a note of these settings you have selected since you may need them later.

Installation Structure

Once the installation has completed the following directory structure and support files will exist:

- iPlanet™ Trustbase Transaction Manager

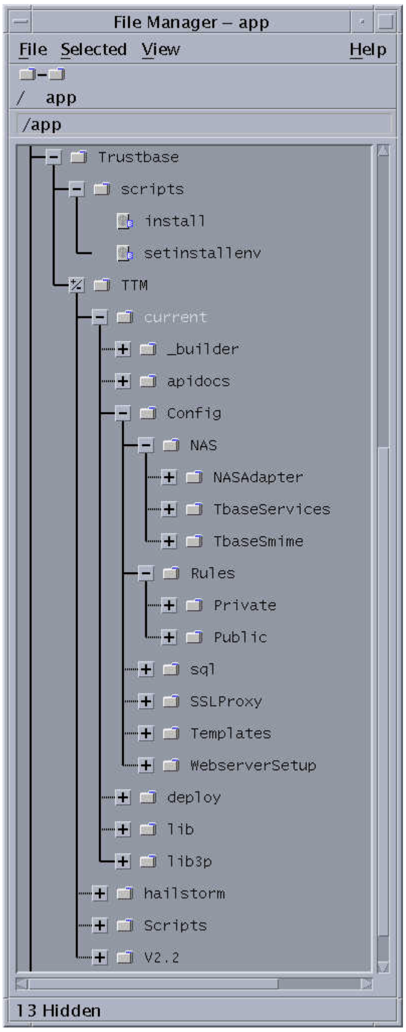
Figure 11 iPlanet Trustbase Transaction Manager Directory Overview



- TTM

iPlanet™ Trustbase Transaction Manager contains all configuration and Library files, the SQL directory containing various database setup scripts.

Figure 12 iPlanet Trustbase Transaction Manager Overview Directory

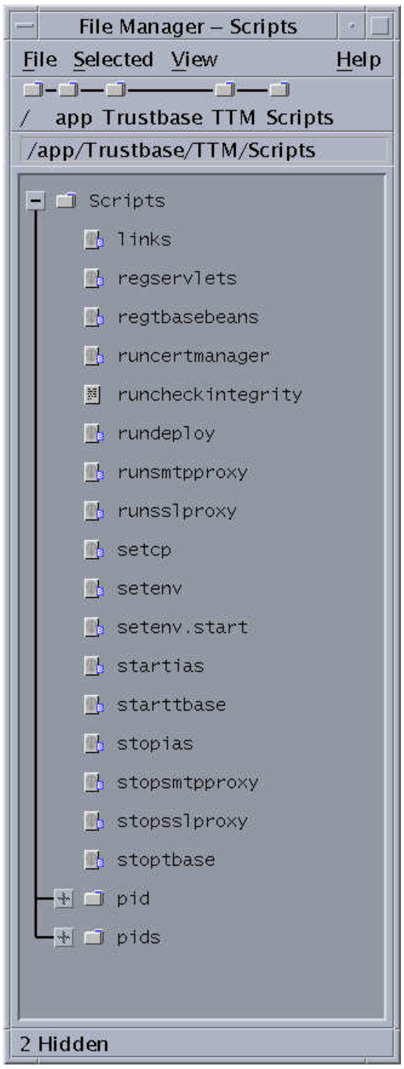


```
Trustbase
    scripts
        install
        setinstallenv
    TTM
        current
            _builder
            apidocs
            Config
                NAS
                    NASAdapter
                    TbaseServices
                    TbaseSmime
                Rules
                    Private
                    Public
                sql
                SSLProxy
                Templates
                WebserverSetup
            deploy
            lib
            lib3p
        hailstorm
        Scripts
        V2.2
```

13 Hidden

- Scripts
  This directory contains all of the scripts needed to start and stop iPlanet Trustbase Transaction Manager

Figure 13 iPlanet Trustbase Transaction Manager Commonly Used Scripts



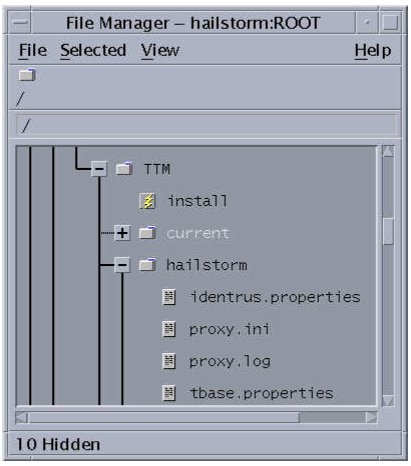
/app/Trustbase/TTM/Scripts

```
Scripts
    links
    regservlets
    regtbasebeans
    runcertmanager
    runcheckintegrity
    rundeploy
    runsmtpproxy
    runsslproxy
    setcp
    setenv
    setenv.start
    startias
    starttbase
    stopias
    stopsmtpproxy
    stopsslproxy
    stoptbase
  + pid
  + pids
```

2 Hidden

- <machine_name>
  This directory contains all of the configuration files for this installation. i.e. tbase.properties, nFast.properties, identrus.properties and proxy.ini These files should not be modified directly but can be accessed via the configuration screens in this manual.

Figure 14 iPlanet Trustbase Transaction Manager Initialisation Files



- V2.2
  This directory contains all of the TTM binaries and support files

All other directories are not needed.

Post Installation Steps

Before starting iPlanet™ Trustbase Transaction Manager for the first time it is necessary to do some further configuration steps, in each of the following configuration steps refer to the installation structure section above to locate the necessary files:

- nCipher Security setup – see section HSM Configuration on page 30
- Oracle Database setup – see section Oracle Database Configuration on page 33
- Identrus site specific setup – see section Identrus Configuration on page 35

HSM Configuration

This is an optional feature since alternative cryptographic mechanisms are in place if you wish to configure iPlanet™ Trustbase Transaction Manager without a Hardware Security Module. This is mandatory for Identrus compliant sites.

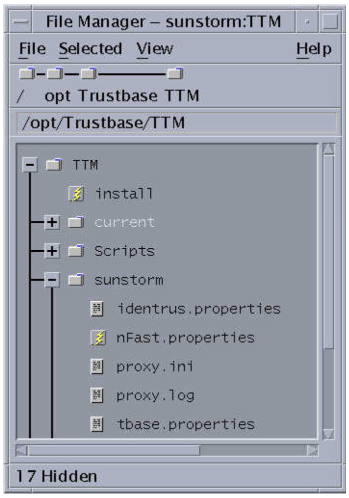
Pre-requisite

Make sure, when installing iPlanet Trustbase Transaction Manager, you answer the following question:

```
What Cryptographic provider do you want to use: NCIPHER or JCP? NCIPHER
```

When the iPlanet Trustbase Transaction Manager installation is complete check that nfast.properties is located in the directory <install_directory>/Trustbase/TTM/<machine_name> as illustrated below:

Figure 15 Locating nfast.properties



nCipher Initialisation.

For each group of nCipher modules that will be sharing a common key database, the following setup procedure must be adopted.

- Install the nCipher hardware as described in the supplied documentation, making sure that each unit is set to be in pre-initialisation mode. The nCipher documentation describes the process of installing and setting up the "Security World" on a module (See nCiphers: KeySafe user guide).

- The nFast module will only accept connections from the local host. Therefore the nFast module must be located on the same hardware drive used to run the TC.

- Create a “Security World” on one module, using the nCipher KeySafe tool.

- Copy this “Security World” to the other modules, and install this world using the “restore” function in KeySafe.

- The nfast startup script must be modified to ensure the nFast server can communicate with the iPlanet™ Trustbase Transaction Manager nFast stub via TCP. To do this, the environment variable

NFAST_SERVER_PORT must be defined and exported in /etc/init.d/nfast. The iPlanet™ Trustbase Transaction Manager stub has a default value for this port of 9000, but it can be set to any available port.

- Once these settings have been made, the server should be restarted. If the nCipher software has been installed in the default location the commands to do this are:

```
/app/nfast/sbin/init.d-nfast stop
/app/nfast/sbin/init.d-nfast start
```

Note If the NFAST_SERVER_PORT value is anything other than 9000, the nFast.properties file in the iPlanet™ Trustbase Transaction Manager install directory (/app/Trustbase/TTM/<machine name>) must be modified such that the StandardPort property is consistent.

nCipher module setup and usage.

Once the Security world is installed, the following points should be noted:

- The nFast stub and the NCIPHER JCE provider both read certain settings from a properties file "nFast.properties". This should contain the following values:

  - AServerAddress. The ServerAddress property should be set to the local host. If set to other values the server may refuse connection attempts on unix systems. On NT systems, the server will accept connections from clients elsewhere than "localhost". The default value is 127.0.0.1

  - StandardPort. The StandardPort property contains the number of the port on which the server is listening for standard connections. By default this value is 9000.

  - StandardConnections. The StandardConnections property contains the number of standard connections that will be maintained with the nFast module. Low values for this property will not allow the module to make best use of its parallel processing capabilities. By default, this value is obtained from the module itself.

  - module.key. The module.key property contains the identifying number of the module key to be used for encrypting keys for storage outside the box. If the standard install procedure has been followed, and the Security World has been correctly set up, the module keys installed on the box are:

    - KM0 - the randomly generated module key that is never exported in any form. If this key is used as the default, archived keys may only ever be used on that specific module. If the module is replaced for any reason, all the keys must be regenerated.

    - KM1 - a well known module key used for bootstrapping of the recovery keys. This module key should NOT be used.

    - KM2 - the security world key. This is the module key that should be used.

    - By default, KM0 is used, i.e. a value of 0, as this is the only module Key guaranteed to be present on the module. In any running system this should always be set to '2'.

```
ServerAddress = localhost
ServerPort = 9000
StandardConnections = 10
PrivilegedConnections = 0
module.key = 2
```

Oracle Database Configuration

Both TTM and the Identrus Extensions require access to a database with a pre-configured schema. The installation comes with SQL scripts that must be executed in the database user's tablespace that was specified at installation time. The following sections explain how to create the user and generate the correct schema for that user.

- The generation of users and the tablespaces defined may differ for individual sites – contact the site DBA for advice. Only one Certstore is utilised for each Trustbase Installation. The following parameters must be defined: Oracle login name, Oracle login password, PBEPassword set the same as Oracle login password, Oracle hostname, Oracle port number and Oracle SID.

Installation Pre-requisite

```
cd /app
cp oracle-jdbc-815.zip /app/Trustbase/TTM/current/lib3p/10
```

Running the iPlanet Trustbase Transaction Manager SQL Scripts

- You may need to ask your DBA to create your username and password. The following procedure should be followed.

- Switch to the Oracle user and run server manager:

```
myhost> su – oracle
Password:
myhost> cd ../Trustbase/TTM/V2.2/Config/sql
myhost> svrmgrl

Oracle Server Manager Release 3.1.5.0.0 - Production

(c) Copyright 1997, Oracle Corporation.  All Rights Reserved.

Oracle8i Enterprise Edition Release 8.1.5.0.0 - Production
With the Partitioning and Java options
PL/SQL Release 8.1.5.0.0 - Production

SVRMGR> connect internal
Connected.
```

- The database must be enabled to support the UTF8 character set. The following script is an example of how to achieve this.

```
SVRMGR> SHUTDOWN;
SVRMGR> STARTUP MOUNT;
SVRMGR> ALTER SYSTEM ENABLE RESTRICED SESSION;
SVRMGR> ALTER SYSTEM SET JOB_QUEUE_PROCESSES=0;
SVRMGR> ALTER DATABASE OPEN;
SVRMGR> ALTER DATABASE CHARACTER SET UTF8;
SVRMGR> SHUTDOWN;
SVRMGR> STARTUP;
```

- Create a iPlanet™ Trustbase Transaction Manager user – you may need to change the username, password and default tablespaces depending on site policy:

```
SVRMGR> CREATE USER tbase IDENTIFIED BY tbase DEFAULT TABLESPACE USERS
TEMPORARY
 TABLESPACE TEMP;
Statement processed.
SVRMGR> GRANT CONNECT TO tbase;
Statement processed.
SVRMGR> GRANT RESOURCE TO tbase;
Statement processed.
SVRMGR> ALTER USER tbase QUOTA UNLIMITED ON USERS;
Statement processed.
SVRMGR> quit
Server Manager complete.
```

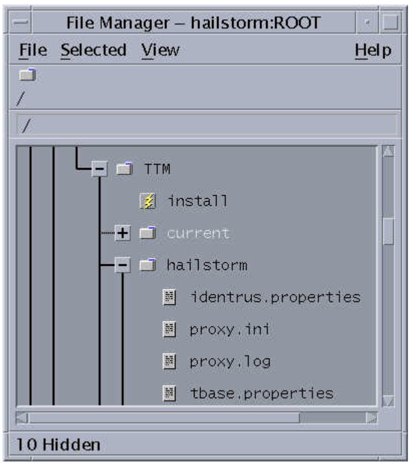
- Connect as the iPlanet™ Trustbase Transaction Manager user and run the scripts:

```
sunstorm% su - oracle
sunstorm% cd /app/Trustbase/TTM/current/Config/sql
sunstorm% sqlplus
SQL*Plus: Release 8.1.5.0.0 - Production on Fri Sep 22 12:07:11 2000
(c) Copyright 1999 Oracle Corporation.  All rights reserved.
Enter user-name: tbase
Enter password:
Error accessing PRODUCT_USER_PROFILE
Warning:  Product user profile information not loaded!
You may need to run PUPBLD.SQL as SYSTEM

Connected to:
Oracle8i Enterprise Edition Release 8.1.5.0.0 - Production
With the Partitioning and Java options
PL/SQL Release 8.1.5.0.0 - Production

SQL> @tbase2.sql
```

Identrus Configuration

A Transaction Coordinator (TC) comprises of all Identrus Services that have been deployed within the iPlanet™ Trustbase Transaction Manager. The file identrus.properties needs to be edited to change settings appropriately. It can be found in <install_directory>/Trustbase/TTM/<machine_name>as illustrated below:

Figure 16 identrus.properties file location



- Normally, only the locations of OurAIA and LocalOCSPResponderLocation need to change. For instance:

```
OurAIA = https://rp
LocalOCSPResponderLocation = http://rp:8080
```

- The following illustrates an example identrus.properties file.

Figure 17 Example Identrus.properties

```
[CSC]
; OID's for OCSP and TC
TCOID=1.2.840.114021.4.1
OCSPResponderOID=1.3.6.1.5.5.7.48.1

;CaCertificateRole=
;EndEntityCertificateRole=
;SigningCertificateRole=
;RootCertificateRole=

; Local OCSP Responder Communication
SignLocalOCSPRequests=false
OCSPResponderSigningCertificateRole=L1_OCSP_SC
LocalOCSPResponderLocation = identrus_local_resp_url

OurAIA = identrus_our_aia
DNOfAuthority=

; Response Cache Parameters
ApprovedResponseMaxAge=60
ApprovedResponseMaxKeep=60
DebugMode=true
;OCSPRequestorName=CN=KENCO
```

Other settings can be modified:

- OID's

    - TCOID: This is ASN object ID for the "authority info access" attribute for Identrus Transaction Coordinator 's (default acceptable). All Identrus Certificates will have this and are supplied by Identrus with the ID of 1.2.840.114021.4.1.

    - OCSPOID: This is ASN object ID for the "authority info access" attribute for OCSP responder's (default acceptable).

- Certificate Role's

    - CaCertificateRole: This is the certificate attribute used for the Transaction Coordinator CA certificate. (Default is acceptable).

    - EndEntityCertificateRole: This is the certificate attribute used for the Transaction Coordinator end entity signing certificate (default acceptable).

    - SigningCertificateRole: This is the certificate attribute used for the Transaction Coordinator inter participant signing certificate (default acceptable).

    - RootCertificateRole: This is the certificate attribute used as by the Identrus Transaction Coordinator to identify the Identrus root (default acceptable).

- Local OCSP Responder Communication

    - SignLocalOCSPRequests: boolean – unsigned Local OCSP requests have a parameter set to “no” and signed Local OCSP requests have this parameter set to “yes”.

    - OCSPResponderSigningCertificateRole: This is the certificate used to verify OCSP responses (only used if signLocalOCSPrequests is true).

    - LocalOCSPResponderLocation: The URL for the local OCSP responder.

- Misc settings

    - OurAIA: The Access Information Authority (AIA) of this Identrus Transaction Coordinator.

    - DNOfAuthority: This is the Distinguished Name (DN) of the Identrus root signing certificate. This is for internal use only.

- Response Cache Parameters

To avoid repeated calls to the Identrus root, an institution can contact the root about the status of its own certificates and store them for a cached period. Whenever a message is sent to another party, it will include this cached response. It is then up to the other institution to decide whether this cached response is acceptable or if it wants to contact the root itself. If a relying customer wants to ensure that cached responses are not used anywhere in an Identrus transaction then that customer can supply a nonce in the outgoing OCSP requests. This nonce is then used as a signal to the institutions not to use the cached response.

Caching prevents the need for repeated access to the Identrus Root. Each institution holds a value for how long its own cached certificate statuses are kept for. It also holds a maximum acceptable age of received certificate statuses. The following parameters must be defined:

- ApprovedResponseMaxAge: number of seconds to allow a cache entry to persist for.

- ApprovedResponseMaxKeep: number of seconds that a response provided to use can be acceptable.

- DebugMode: internal debug on/off

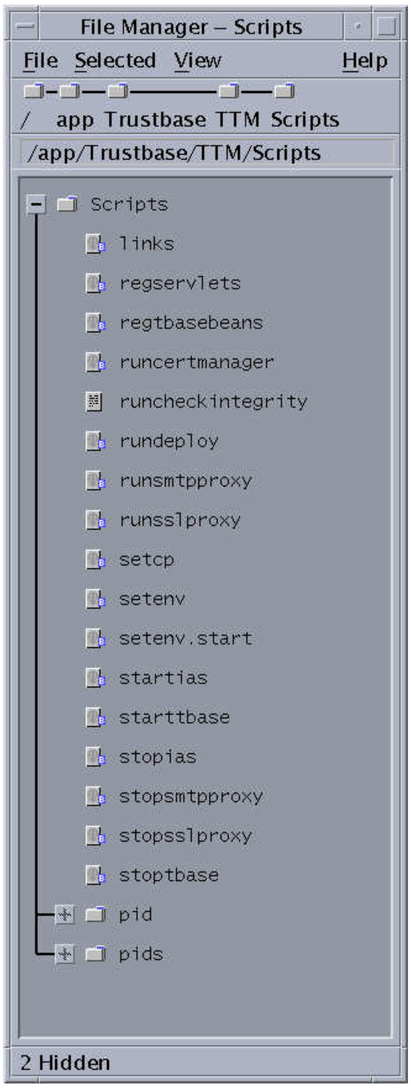
- OCSPRequestorName: name to use when talking to an OCSP responder. It should be noted that this must be set to the Distinguised name (DN) of the certificate used to sign OCSP if signing is set to true (i.e. SignLocalOCSPRequests=true). In the example provided, the common name (CN) is used as the distinguished name since the distinguished name is made up of the common name and the organisation unit (OU).

Start iPlanet Trustbase Transaction Manager

Having completed the installation and configuration iPlanet™ Trustbase Transaction Manager can be controlled using the scripts available in:

- /app/Trustbase/TTM/Scripts

Figure 18 iPlanet Trustbase Transaction Manager Commonly Used Scripts



```
/app/Trustbase/TTM/Scripts

Scripts
    links
    regservlets
    regtbasebeans
    runcertmanager
    runcheckintegrity
    rundeploy
    runsmtpproxy
    runsslproxy
    setcp
    setenv
    setenv.start
    startias
    starttbase
    stopias
    stopsmtpproxy
    stopsslproxy
    stoptbase
  pid
  pids
```

The main scripts used to stop and start iPlanet™ Application Server and TTM components, that need to be executed as 'root' inside the Scripts directory:

- ./startias
  Starts the iPlanet™ Application Server

- ./starttbase
  This script starts the iPlanet™ Trustbase Configuration Manager, SSL Proxy and SMTP Proxy

- ./stopias

- ./stoptbase

Other useful scripts in this directory are:

- ./setcp
  If this script is executed as follows, then the CLASSPATH environment variable is set to be that required for TTM execution. Execute it using '. ./setcp' as 'root' in the Scripts directory.

- ./runcertmanager to configure your certificates

- ./runcheckintegrity used for verifying the integrity of the log (see Archiving for Raw Data and Init Table on page 109)

Note bourne shell (/bin/sh) uses '. ./setcp' and c shell (/bin/csh) uses './setup'

ShutDown procedure

The following procedure stops the system.

- Logon as root

```
#!/bin/sh
cd /app/Trustbase/TTM/Scripts
/app/Trustbase/TTM/Scripts/stopias
/app/Trustbase/TTM/Scripts/stoptbase

/app/ias6/slapd-hailstorm/stop-slapd
/app/iws41/https-hailstorm.uk.sun.com/stop
/app/iws41/https-admserv/stop
```

Restart procedure

The following procedure restarts the system:

- logon as root and run the following shell:

```
#!/bin/sh
/app/ias6/slapd-hailstorm/start-slapd
/app/iws41/https-hailstorm.uk.sun.com/start
/app/iws41/https-admserv/start

cd /app/Trustbase/TTM/Scripts
/app/Trustbase/TTM/Scripts/startias
/app/Trustbase/TTM/Scripts/starttbase
```

Reinstallation

If the responses given during the execution of the Trustbase installation script were incorrect you can rerun the install script without damaging any other changes you have made. When re-executing the install scripts the installer will remember the responses you entered previously and offer them as defaults.

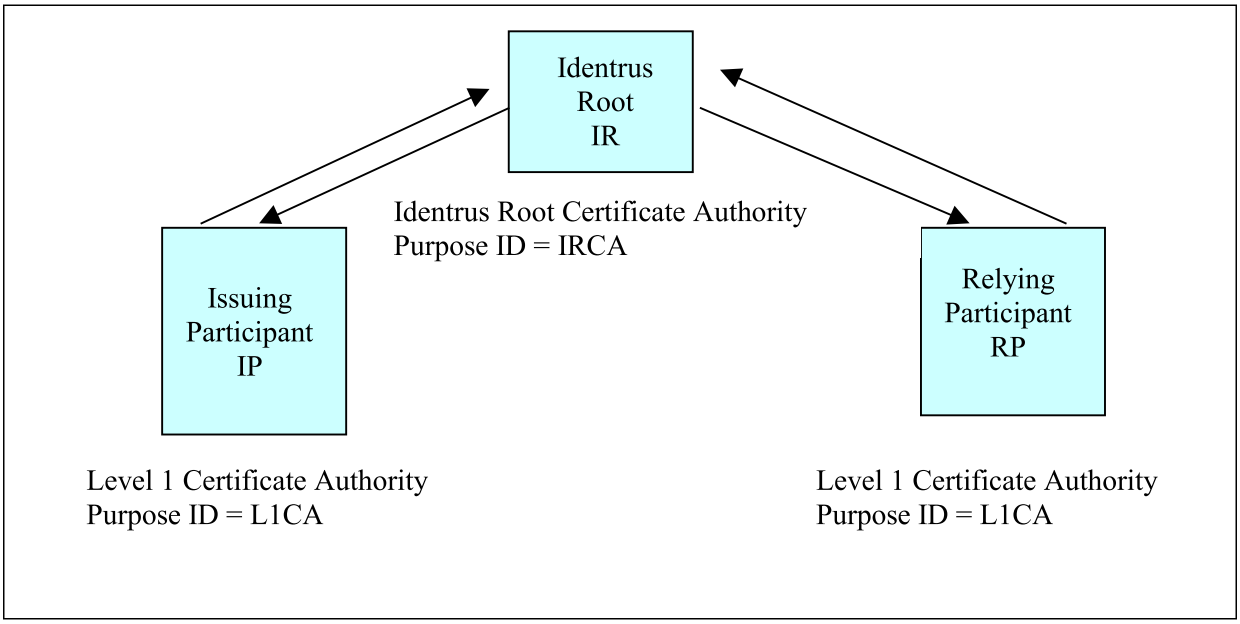
```
sunstorm% cd /app/Trustbase/scripts
sunstorm% ./install
```

Please consult the iPlanet Application Server Installation, iplanet Web Server, Oracle and nCipher documentation for procedures on how to reinstall.

Certificate Management

Before installing certificates, you must have a CA set up with its CA certificate created and signed by the appropriate Identrus Certificate Authority. You then need to place your CA Certificate into the appropriate positions within the iPlanet™ Trustbase Transaction manager CertStore using the Certmanager utility.

Figure 19 Setting CA certificates



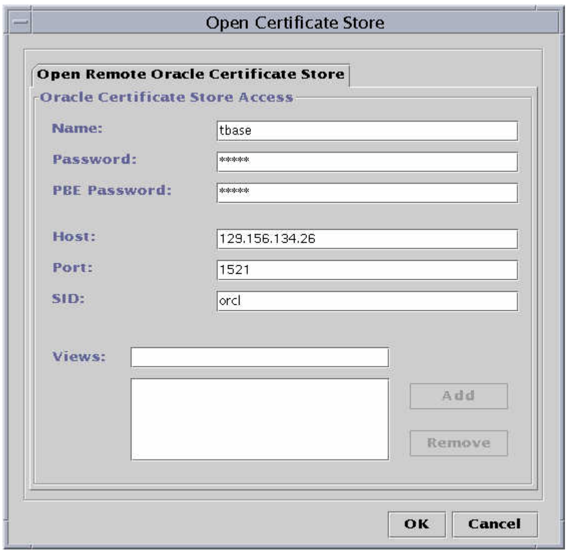
Running Certmanager

- Run CertManager

```
# cd /app/Trustbase/TTM/Scripts
# ./runcertmanager
```

- Open the Store, as illustrated below

Figure 20 Open Certificate Store



Open Certificate Store
Open Remote Oracle Certificate Store
Oracle Certificate Store Access
Add
Remove
OK
Cancel

Name: tbase

Password: *****

PBE Password: *****

Host: 129.156.134.26

Port: 1521

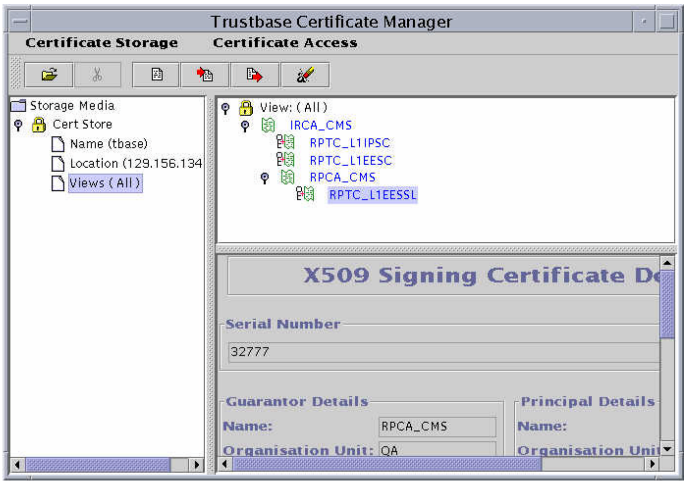
SID: orcl

Views:

Generating PKCS10 requests

- Create The Identrus PKI hierarchy as illustrated below

Figure 21 Identrus PKI hierarchy



Serial Number

32777

Name: RPCA_CMS

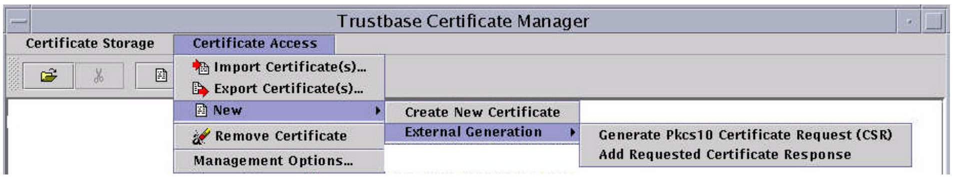
Organisation Unit: QA

- This is a two stage process involving pasting data that you have generated from CertManager into the website of the certificate authority that generates a response:

  - "Generate PKCS10 certificate Request (CSR)" for generating PKCS-10 certificate requests

  - "Add Requested Certificate Response" collects the corresponding response from the certificate Authority (sometimes referred to as a PEM Response).

Figure 22 Generating PKCS10 requests

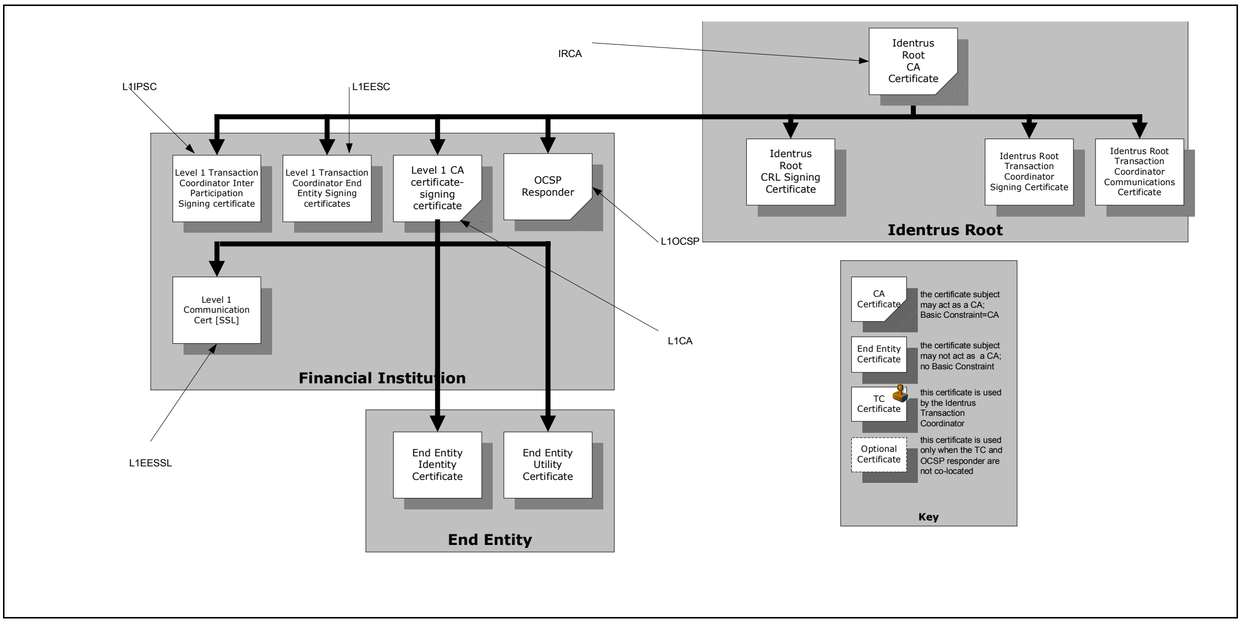


Note More details about how to use CertManager can be found in the Utility Guide

Assigning Attributes to Certificates

In order that iPlanet™ Trustbase Transaction Manager can recognise these certificates, they must be assigned an attribute view from within CertManager. The following Attribute view/ purpose ID/ purpose attributes must be defined:

Figure 23 Purpose Attribute views and the Identrus PKI hierarchy


IRCA
L1IPSC
L1EESC
Identrus Root CA Certificate
Level 1 Transaction Coordinator Inter Participation Signing certificate
Level 1 Transaction Coordinator End Entity Signing certificates
Level 1 CA certificate-signing certificate
OCSP Responder
Identrus Root CRL Signing Certificate
Identrus Root Transaction Coordinator Signing Certificate
Identrus Root Transaction Coordinator Communications Certificate
Identrus Root
L1OCSP
Level 1 Communication Cert [SSL]
L1CA
Financial Institution
End Entity Identity Certificate
End Entity Utility Certificate
End Entity
L1EESSL
CA Certificate
the certificate subject may act as a CA; Basic Constraint=CA
End Entity Certificate
the certificate subject may not act as a CA; no Basic Constraint
TC Certificate
this certificate is used by the Identrus Transaction Coordinator
Optional Certificate
this certificate is used only when the TC and OCSP responder are not co-located
Key

- the purpose attribute L1CA should be assigned to the certificate RPCA-CMS since in this case the relying particpant is the Level 1 CA. L1CA is the purpose ID for CA certificates.

- the purpose attribute L1EESC should be assigned to the certificate RPTC_L1EESC. L1EESC is the purpose ID of Certificate used for bank/RC or bank/SC message signing.

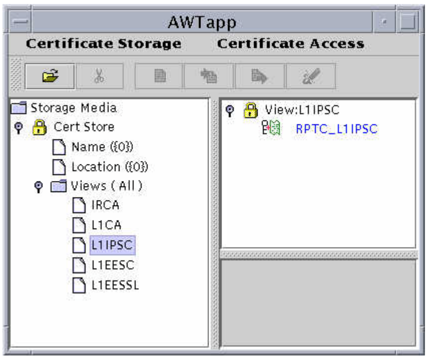
- the purpose attribute L1EESSL should be assigned to the certificate RPTC_L1EESSL. L1EESSL is the purpose ID of Certificate used for bank/RC or bank/SC SSL connections - as server.

- the purpose attribute L1IPSC should be assigned to the certificate RPTC_L1IPSC. L1IPSC is the purpose ID of Certificate used for interbank message signing.

- the purpose attribute IRCA should be assigned to the certificate IRCA_CMS. IRCA is the certificate for the Identrus root.

This is illustrated within iPlanet™ Trustbase Transaction Manager's CertManager Utility in Figure 24 Purpose Attributes below.

Figure 24 Purpose Attributes

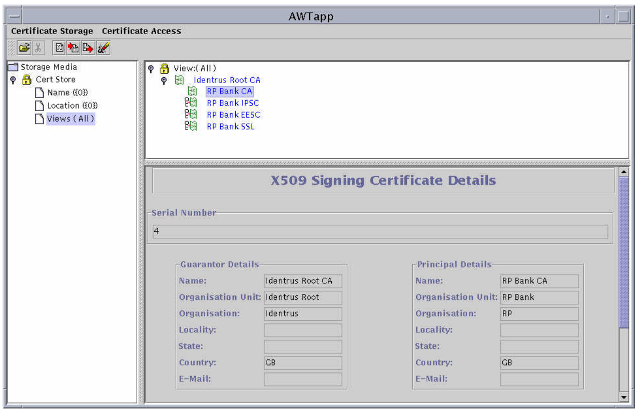


Note Consult your Utility guide on how to create Attribute views for certificates. When viewed on the screen through CertManager this is referred to as an attribute view. When deployed within iPlanet™ Trustbase Transaction Manager as a transaction processing requirement, this is referred to as a purpose attribute or purpose ID. See, for instance, the Utility Guide section headed Certificate View on page 25.

Identrus Authorisation

In order to send Identrus Messages to iPlanet Trustbase Transaction Manager you will need to create an Authorisation for your own customers that allows the sending of Identrus Enabled Messages. These are illustrated in the next three figures:

Figure 25 A Certificate that enables you to send Identrus Messages

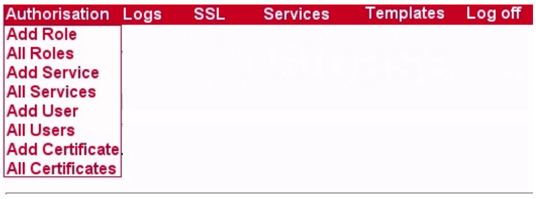


X509 Signing Certificate Details

Serial Number: 4

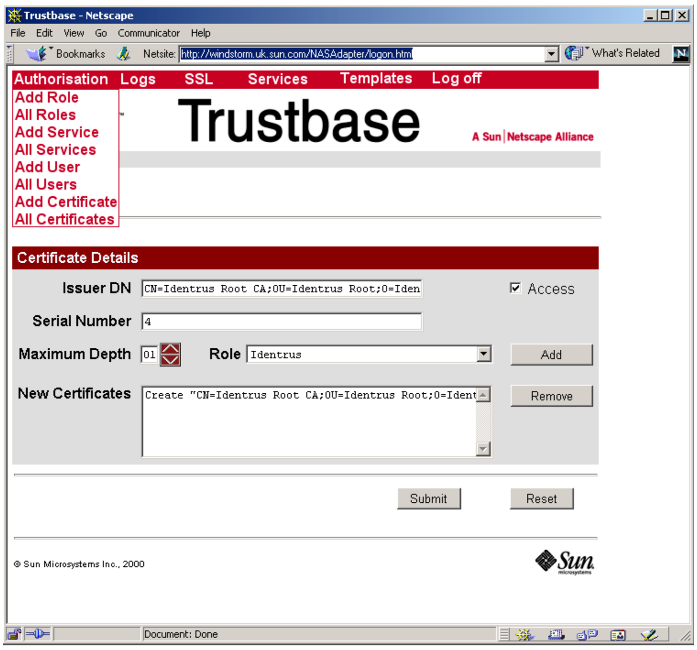
Guarantor Details		Principal Details	
Name:	Identrus Root CA	Name:	RP Bank CA
Organisation Unit:	Identrus Root	Organisation Unit:	RP Bank
Organisation:	Identrus	Organisation:	RP
Locality:		Locality:	
State:		State:	
Country:	GB	Country:	GB
E-Mail:		E-Mail:	

- Select <Authorisation> <Add Certificate>



- For this example enter the issuer Distinguised Name “CN=Identrus Root CA;OU=Identrus Root;O=Identrus;C=GB” and the serial number of the RP Bank CA which is 4. Set the Max Depth to 1 and the Role to Identrus (see page Adding a Certificate on page 66 for more information on this) This is illustrated below:

Figure 26 Installing a Certificate so as to send Identrus Messages within Trustbase



Certificate Details

Issuer DN: CN=Identrus Root CA;OU=Identrus Root;O=Iden

☑ Access

Serial Number: 4

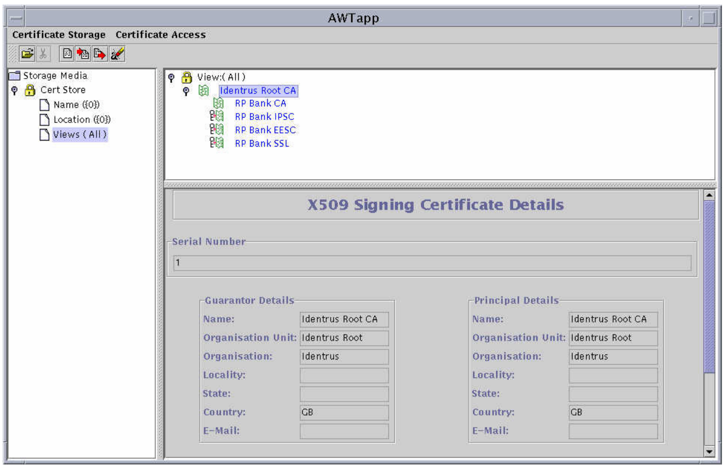
Maximum Depth: 01

Role: Identrus

New Certificates: Create "CN=Identrus Root CA;OU=Identrus Root;O=Ident

You will also need to create an additional Authorisation for other banks to send Identrus Enabled messages to you. These are illustrated in the next three figures:

Figure 27 A certificate that enables you to send Identrus Messages to other banks

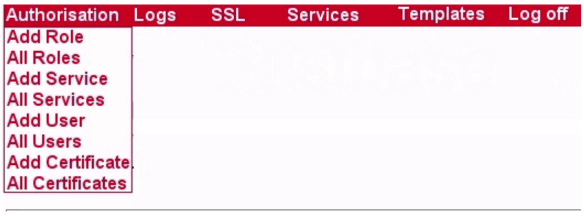


X509 Signing Certificate Details

Serial Number: 1

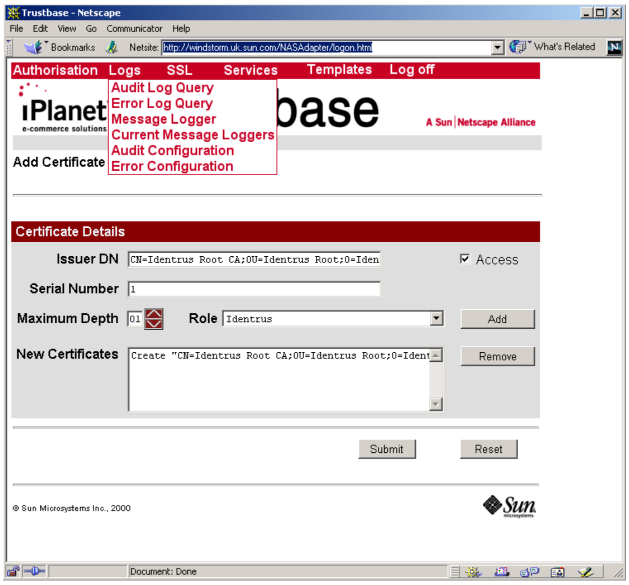
Guarantor Details		Principal Details	
Name:	Identrus Root CA	Name:	Identrus Root CA
Organisation Unit:	Identrus Root	Organisation Unit:	Identrus Root
Organisation:	Identrus	Organisation:	Identrus
Locality:		Locality:	
State:		State:	
Country:	GB	Country:	GB
E-Mail:		E-Mail:	

- Select <Authorisation> <Add Certificate>



- Enter the Distinguised Name “CN=Identrus Root CA;OU=Identrus Root;O=Identrus;C=GB” and the serial number of the RP Bank CA which is 1. Set the Max Depth to 1 and the Role to Identrus (see page Adding a Certificateon page 66 for more information on this) This is illustrated below:

Figure 28 Installing a Certificate within Trustbase that enables you to send Identrus Enabled Messages



Issuer DN: CN=Identrus Root CA;OU=Identrus Root;O=Iden

☑ Access

Serial Number: 1

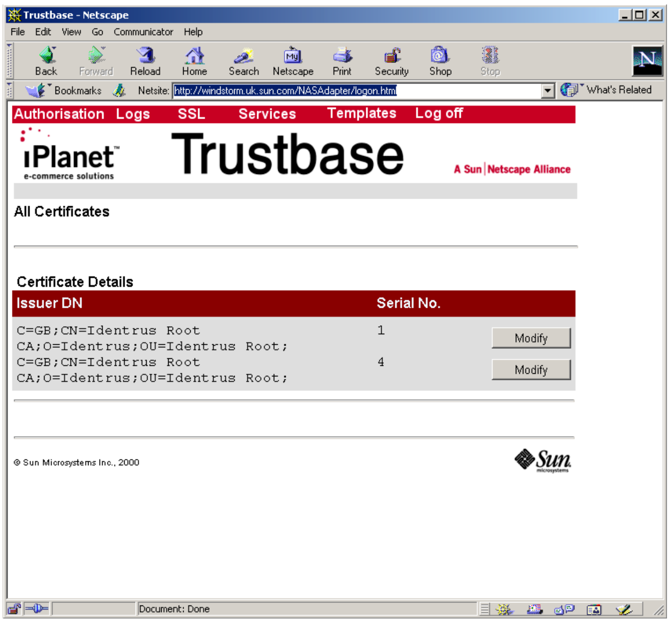
Maximum Depth: 01

Role: Identrus

New Certificates: Create "CN=Identrus Root CA;OU=Identrus Root;O=Ident

Finally you should restart iPlanet Trustbase Transaction Manager for the setting to take effect and you should make sure both certificates are installed within iPlanet Tustbase Transaction manager as illustrated below:

Figure 29 Identrus Enabled Messages installed within Trustbase


Trustbase - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Shop Stop
Bookmarks Netsite: http://windstorm.uk.sun.com/NASAdapter/logon.html
What's Related
Authorisation Logs SSL Services Templates Log off
iPlanet e-commerce solutions
Trustbase
A Sun | Netscape Alliance
Modify
Modify
Document: Done

All Certificates

Certificate Details

Issuer DN	Serial No.
C=GB;CN=Identrus Root CA;O=Identrus;OU=Identrus Root;	1
C=GB;CN=Identrus Root CA;O=Identrus;OU=Identrus Root;	4

© Sun Microsystems Inc., 2000

OCSP Responders and Validating signed OCSP Responses

When a message is sent to any node a response comes back. That response needs to be verified in such a way that the sender of the response is who they say they are. This is an optional feature in that it can be assumed that responses are trusted. OCSP Responders that are used locally are unlikely to require this signing validation process as their communication can be considered secure. However OCSP Responders on non-local or insecure lines should have this feature configured.

When an RP bank communicates with an IP that does not have an iPlanet™ Trustbase Transaction Manager Transaction Coordinator and fails it will need an OCSP Responder. This is sometimes referred to as OCSP fallback.

In order to verify an OCSP response we need to input the signing Certificate into the iPlanet™ Trustbase Transaction Manager certificate store. Once the OCSP signing Certificate has been successfully imported into the iPlanet™ Trustbase Transaction Manager Oracle Certificate Store, a purpose attribute needs to be defined as follows:

- L1OCSP

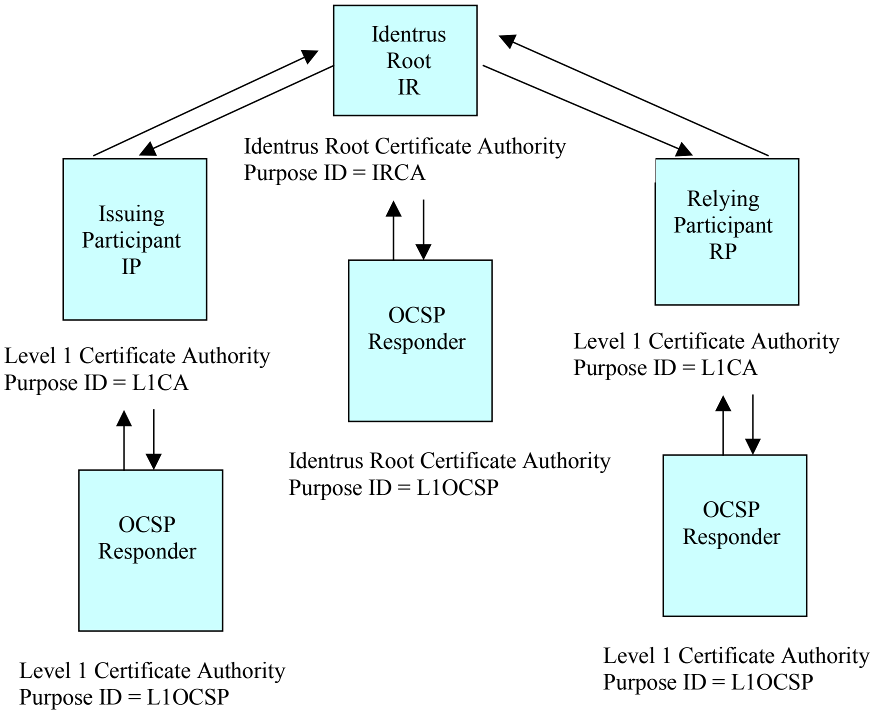
iPlanet™ Trustbase Transaction Manager will use the Certificate with this attribute value to verify the digital signature when it receives a signed OCSP response.

There are a number of ways to obtain this certificate

- Use the certificate with IRCA purpose attribute. However this can only be used if the Validating Authority certificate was issued by the IRCA certificate.

- Get it from your OCSP Responder e.g. Valicert or any other Validation Authority that is Identrus compliant.

Figure 30 OCSP Responders



Chapter 3

Architectural Configuration

iPlanet™ Trustbase Transaction Manager can be deployed over a variety of hardware configurations:

- It may be configured on single and clustered iPlanet™ Application Server installations
- It has a variety of configuration issues within the DMZ environment
- It can also be configured using Hardware Security Modules

iPlanet Application Server configuration

iPlanet™ Application Server may be used in a wide variety of configurations to support differing requirements for:

- Scalability
- Throughput
- Failover

The iPlanet™ Trustbase Transaction Manager has been designed to take advantage of these facilities and has been tested on two of the main configurations, these being:

- Single iPlanet™ Application Server
- Clustered iPlanet™ Application Servers

A single iPlanet™ Application Server is the most likely configuration option for low volume pre-operational Transaction Manager environment. This is considered a standard iPlanet™ Trustbase Transaction Manager installation and requires no specific configuration options other than those outlined in the iPlanet™ Application Server installation guide. The recommended settings for iPlanet™ Application Server are:

- Single KJS for each CPU on the host machine
- Minimum 8 and Maximum 64 Threads per KJS

The iPlanet™ Trustbase Transaction Manager is generally a CPU bound processing environment. This means that installing a greater number or faster CPU's will improve performance.

The iPlanet™ Trustbase Transaction Manager utilises Oracle databases extensively. Oracle itself is both CPU and disk intensive. If possible, Oracle should be located on a separate computer to the iPlanet™ Trustbase Transaction Manager installation.

Clustered iPlanet™ Application Server installations provide a means of improving Scalability, throughput and fail-over over a single iPlanet™ Application Server running the iPlanet™ Trustbase Transaction Manager. Prior to installing a clustered iPlanet™ Application Server the following items require consideration:

- Each Machine running iPlanet™ Application Server can have an nCipher HSM. This is a requirement for Identrus Compliance.
- A clustered iPlanet™ Application Server environment may provide slower response times in marginal loading conditions

Note for further information about performance tuning and effective deployment consult:

- iTTM (this Guide) can also be tuned in terms of the number of connections (see SSLProxy configuration) and the length of time caching takes place (see Identrus Configuration).
- Oracle 8i Administrators Reference Manual Chapter 2
- SQL tuning can also be found in the Oracle 8i programmers Guide
- Tuning Server Performance is discussed within the iPlanet™ Web Server 4.1 Administration Guide
- Application Deployment is discussed within the iPlanet™ Application Server 6.0 Administration and Deployment Guide

Using a DMZ

The general architectural model for deploying an iPlanet™ Trustbase Transaction Manager is to place the application server within a Demilitarised Zone (DMZ) created using a proxy machine between two firewalls. This configuration provides a means of ensuring that an outside user cannot directly access or modify the logic that forms the application in order to circumvent the authentication and authorisation requirements.

The DMZ primary firewall must offer two unauthorised open ports to support SSL access and SMTP access. These ports are generally:

- SSL - Port 443
- SMTP - Port 25

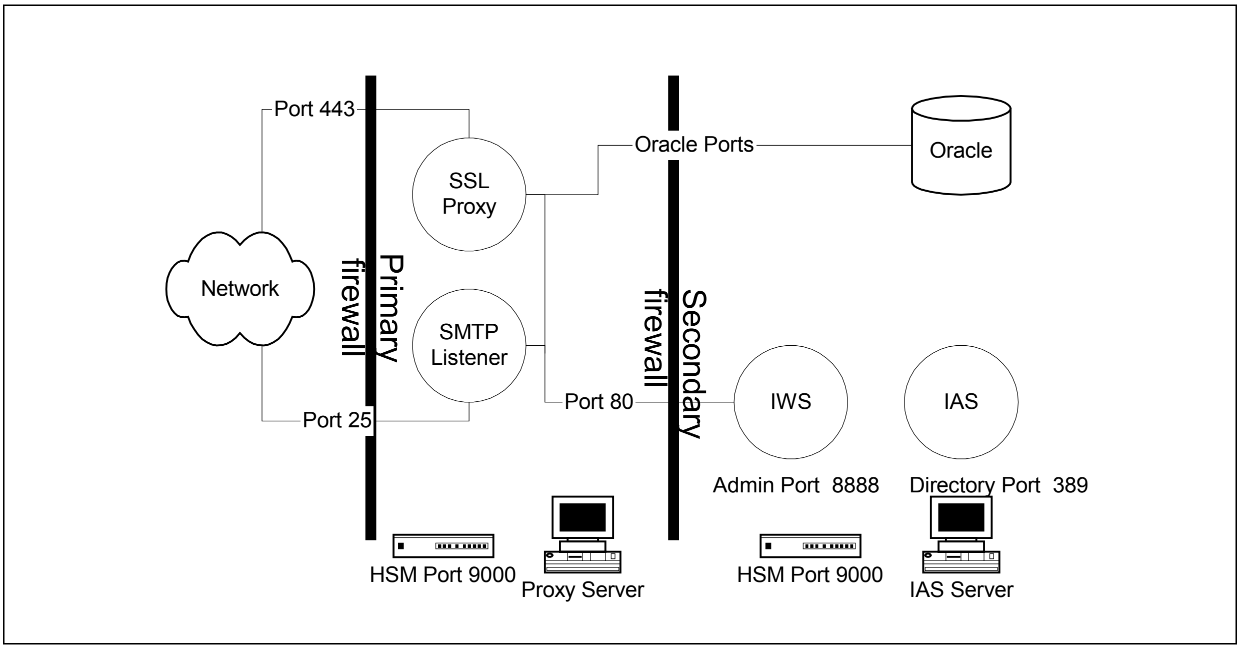
Behind this firewall is a single machine that runs the SSL proxy, the SMTP listener, and the iPlanet™ Web Server. The secondary firewall has three ports open configured for the DMZ machine only. These three ports are:

- iPlanet™ Application Server Directory Port 389
- iPlanet™ Web Server
    - HTTP - Port 80
    - Admin - Port 8888
- Oracle

Note Oracle uses many ports. Consult your Oracle DBA about this.

The HTTP port is used by the SSL and SMTP proxies to communicate to the iPlanet™ Web Server located behind the secondary firewall. Both the SSL and SMTP listeners use the Oracle port to store information about connections as well as receive their configuration. The architecture is shown below.

Figure 31 DMZ Architecture



Using this configuration the systems administrators may use the HTML based configuration screens without the need for SSL certificates. This does not circumvent the authentication mechanisms as the configuration management mechanisms are authenticated using a Username and Password based authentication mechanism.

Note The default configuration is such that it all runs on one machine. When you install iPlanet™ Application Server 6.0 and iPlanet™ Web Server 4.1 it installs a directory server that has a default port of 389 and an administrator port of 8888

Machine Installations

In some instances it may be necessary to install product component software on different machines. The following table summarises possible combinations:

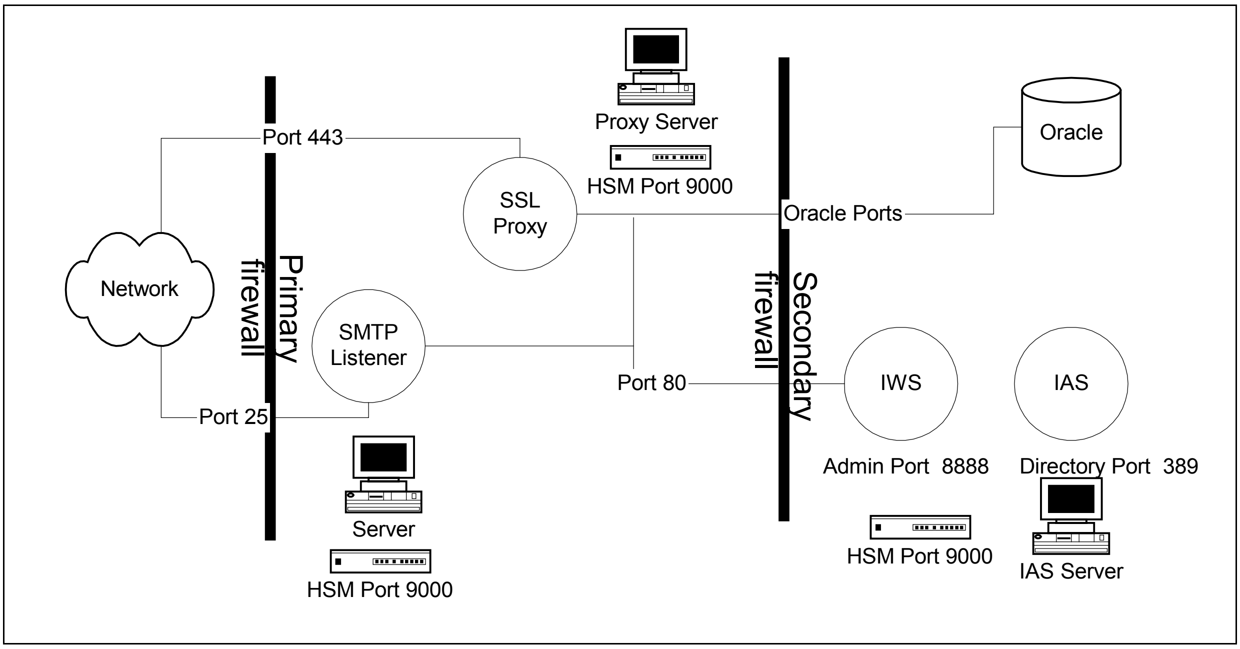
Figure 32 Acceptable Machine Installations

Product Component to be separated	Separate Machine Installation?	Considerations
iTTM separated from IAS	Not Possible	If IAS and IWS are installed on Separate machines make sure iTTM is installed with IAS
IWS separated from IAS	Yes	See Section on Configurator Plug-in http://docs.iplanet.com/docs/manuals/ias.html
Oracle separated from iTTM	Yes	See Section Oracle Database Configuration on page 33
SSL Proxy separated from iTTM	Yes	See Section Configuring the SSLproxy Separately on page 53
SMTP Proxy separated from iTTM	Yes	See Configuring the SMTP Proxy Separately on page 54
IAS with other Web Servers	Not Supported	

Configuring the SSLproxy Separately

In some situations it may be more convenient to place the SSLproxy on a separate machine.

Figure 33 DMZ Architecture for separating the SSLProxy



Using this configuration the systems administrators need to do the following.Configure nCipher Security world so that the nCipher boxes share the nCipher security world. A separate script is needed to ensure the appropriate iPlanet Trustbase Transaction Manager software is on both machines by performing the following steps:

1) Create a tar of a completed single machine install by typing tar –cvf Trustbase.tar Trustbase from the installation directory (/app)

2) Unpack this tar file on the computer you wish to run the proxy on. Unpack it into the same install directory structure as the original computer. (e.g /app). Do not install iPlanet Trustbase Transaction Manager, iPlanet Web Server or iPlanet Application Server on this new machine.

3) Enter the directory <new_install directory>/Trustbase/TTM and rename the directory that is named after the hostname of the computer and ensure it is the same as the new host. If the <new_install_directory> is different, edit the file <new_install_directory>/Trustbase/TTM/Scripts.setenv and change the directories names in TBASE_INSTALL and TBASE_HOME to refer to the <new_install_directory>

4) To start the proxy on its own, enter this new hostname directory <new_install directory>/Trustbase/TTM/Scripts. Run the ./runsslproxy script.

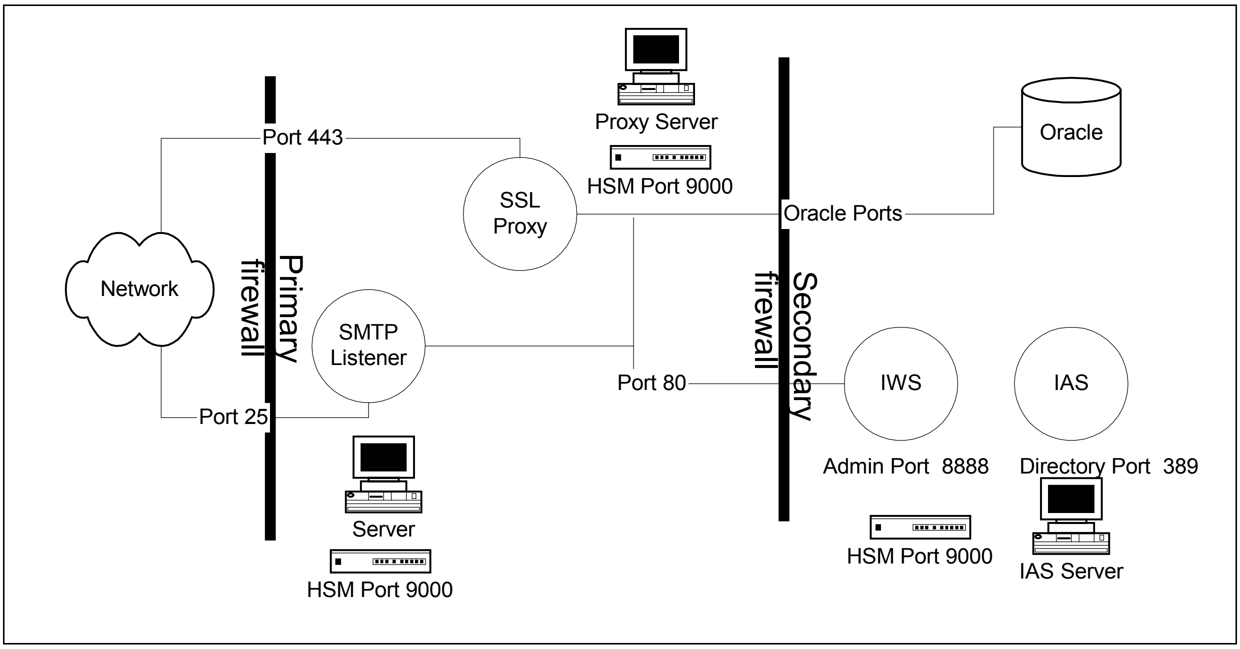
5) On the host that is now no longer running the ssl proxy, edit the script in <install directory>/Trustbase/TTM/Scripts entitled ./starttbase and remove the reference to the SSL Proxy. You will want to do the same with the ./stoptbase script.

It is not necessary to change the configuration settings from within the administration console since the proxy communicates with iPlanet Trustbase Transaction manager and not the other way round. The transaction Co-ordinator field AIA for all certificates of all end users must also point to this new host of the SSLProxy.

Configuring the SMTP Proxy Separately

In some situations it may be more convenient to place the SMTP proxy on a separate machine.

Figure 34 DMZ Architecture for separating the SMTP Proxy



Using this configuration the systems administrators need to do the following.Configure nCipher Security world so that the nCipher boxes share the nCipher security world. A separate script is needed to ensure the appropriate iPlanet Trustbase Transaction Manager software is on both machines by performing the following steps:

1) Create a tar of a completed single machine install by typing tar –cvf Trustbase.tar Trustbase from the installation directory (/app)

2) Unpack this tar file on the computer you wish to run the proxy on. Unpack it into the same install directory structure as the original computer. (e.g /app). Do not install iPlanet Trustbase Transaction Manager, iPlanet Web Server or iPlanet Application Server on this new machine.

3) Enter the directory <new_install directory>/Trustbase/TTM and rename the directory that is named after the hostname of the computer and ensure it is the same as the new host. If the <new_install_directory> is different, edit the file <new_install_directory>/Trustbase/TTM/Scripts.setenv and change the directories names in TBASE_INSTALL and TBASE_HOME to refer to the <new_install_directory>

4) Edit the script <new_install_directory>/Trustbase/TTM/Scripts/runsmtpproxy to change the localhost to the machine hostname where iPlanet Trustbase Transaction Manager has been installed, as illustrated below:

```
#!/bin/sh
. ./setcp
ulimit -n 128
echo $$ > pids/runsmtpproxy.pid
cd $TBASE_INSTALL
exec java uk.co.jcp.tbaseimpl.smtp.server.SmtpServer -debug 6 -url
http://hailstorm.uk.sun.com/NASApp/TbaseSmime/SmimeServlet –timeout
120000
```

5) To start the proxy on its own, enter this new hostname directory <new_install directory>/Trustbase/TTM/Scripts. Run the ./runsmtpproxy script.

6) On the host that is now no longer running the SMTP proxy, edit the script in <install directory>/Trustbase/TTM/Scripts entitled ./starttbase and remove the reference to the SMTP Proxy. You will want to do the same with the ./stoptbase script.

HSM support

In order to become Identrus compliant, the iPlanet™ Trustbase Transaction Manager must be dependent on the availability of an nCipher HSM to perform private key cryptographic operations. The iPlanet™ Trustbase Transaction Manager communicates with the nCipher Hard Server process using TCP/IP sockets. As part of the nCipher security features the Hard Server will only accept connections from the local machine. This means that an nCipher HSM must be locally available on each machine running an iPlanet™ Trustbase Transaction Manager Process. The default settings for the iPlanet™ Trustbase Transaction Manager to use the nCipher HSM are:

- HSM must be in Socket mode - See nCipher documentation
- Port 9000 configured in both the Hard Server configuration and Trustbase.properties files - See installation section

Each iPlanet™ Trustbase Transaction Manager installation (Proxies and iPlanet™ Application Server processes) stores the key material (In encrypted form) in a shared Oracle repository. By default nCipher HSM's cannot share this key material and must be configured using the nCipher security world software to allow this. The process for sharing keys using module keys held on smart cards is documented in the iPlanet™ Trustbase Transaction Manager installation guide.

The nCipher security world configuration provides a means of adding additional or replacement HSM devices to an installation. In order to configure a new machine with an HSM capable of using the iPlanet™ Trustbase Transaction Manager key material the following process should be followed:

- The new HSM device must be attached to the new machine
- The security world files from the original installation must be copied to the new machine
- The Smart Cards from the original HSM installation must be used to generate the module key on the new installation.

This process is documented as part of the nCipher KeySafe product users manual.

Chapter 4

Logging on

Once you have completed your iPlanet™ Trustbase Transaction Manager Installation you are ready to logon on and consider all your various configuration options. This involves authorising services, users, roles and certificates. Defining your logging options. Setting your SSL transport configuration options. Deploying your services and defining configuration interaction options via templates.

Configuration Management overview

In order to inspect or modify items within a iPlanet™ Trustbase Transaction Manager installation the administrator must log in using the HTML Logon form:

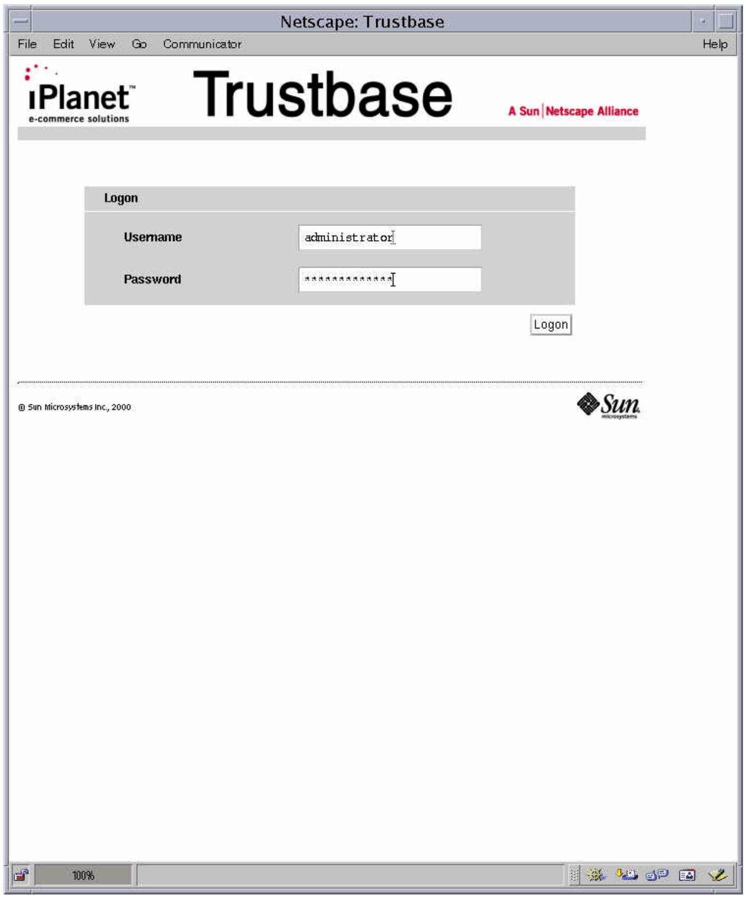
```
http://<hostname>/NASAdapter/logon.html
```

The Administrator may perform a variety of configuration operations each time returning to the appropriate home screen. Selecting logout on the Home Screen will terminate the operator's session and require re-authentication to use any of the configuration screens. Once logged out of a session it is not possible to configure iPlanet™ Trustbase Transaction Manager using HTML screens cached in the browser as the administration authentication context has been removed from the iPlanet™ Trustbase Transaction Manager server. If an administrator leaves the session logged in for longer than several minutes without any activity, the session is automatically terminated and the administrator must re-authenticate using the login screen to gain access to the system. If the session times out, operating any buttons on the configuration screens will result in a server error being returned to the users browser. It is necessary to login to iPlanet™ Trustbase Transaction Manager again.

Logon Screen

The iPlanet™ Trustbase Transaction Manager is installed with one standard username. All administrators enter the system using the Logon Screen shown below:

Figure 35 Logon Screen



Logon

Username administrator

Password *************

Logon

The username and password have been set as illustrated below. This can be changed by selecting the appropriate menu option (see section Adding users to roles on page 65).

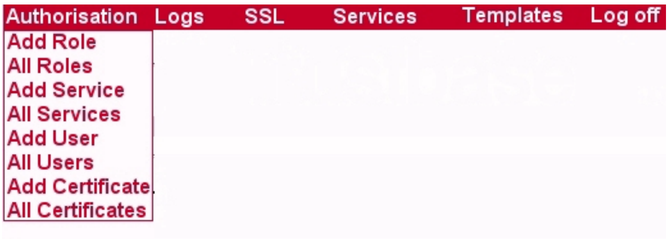
```
Username Administrator
Username Administrator
```

Note this password has the same implications as a root password on a Solaris machine and as such should not be lost.

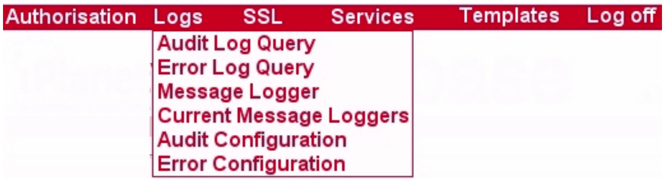
Configuration Options

The following Options are available:

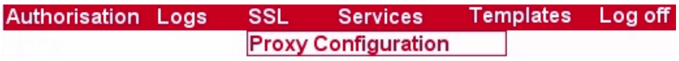
- Authorisation - that defines roles , services, users and Certificates



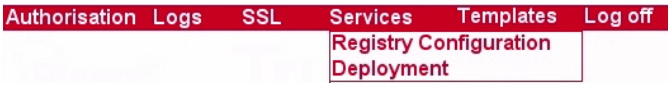
- Logs - that allows you to query, configure and view messages that are thrown round the system



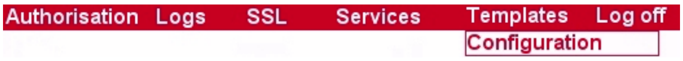
- SSL - Configures your proxy by defining which certificate store settings it is using, its server address and port, the cryptographic algorithm used at the SSL Layer and the number of connections permitted at any one time.



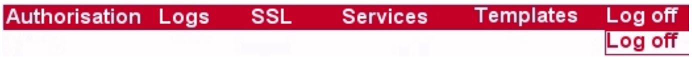
- Services - allows you to register and deploy services



- Templates - that define what kinds of message protocol are acceptable to the system



- Log Off - that allows you to exit from the configuration screens.



Chapter 5

Authorisation

Authorisation revolves around the idea of authenticating a service by assigning a role that can authenticate aspects of a service by linking a certificate to a role. Each certificate is assigned a distinguished name and a role that can authenticate to any number of levels down a certificate hierarchy.

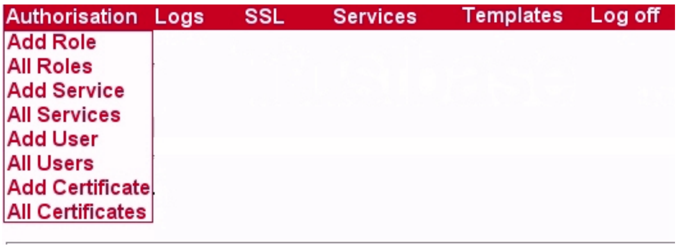
Introduction

The iPlanet™ Trustbase Transaction Manager authorisation facilities provide the operator with the ability to prevent unknown users accessing services. The authorisation management screens allow the operator to modify the set of known users, and the services they are allowed to access. Changes in the authorisation screens modify the iPlanet™ Trustbase Transaction Manager authorisation database and are made immediately.

The iPlanet™ Trustbase Transaction Manager will perform an authorisation check on every request that starts a new user session e.g. when the operator logs on to the system or when a CSC is received. This check maps a username or certificate to a role, and this role is passed around the system with the request. Prior to the router invoking a service the authorisation database is checked to see which roles are allowed to access the service. If the roles match then the operation is allowed. If there is a mismatch then the router will log an authorisation failure and the request will be rejected.

All of the facilities required to organise the authorisation parameters are accessible from the main authorisation menu shown below.

Figure 36 Authorisation Main Menu



Authorising users to access a service

Authorising users for a particular service is a multistage process. The steps are:

- Define a role - Create a group under which the users will be identified
- Add users to the role - Identify the individuals that will be members for the group
- Map the role to the service - Provide an authorisation to use a service if they hold a particular role
- Allocate a certificate to each role.

The following sections describe this process in more detail.

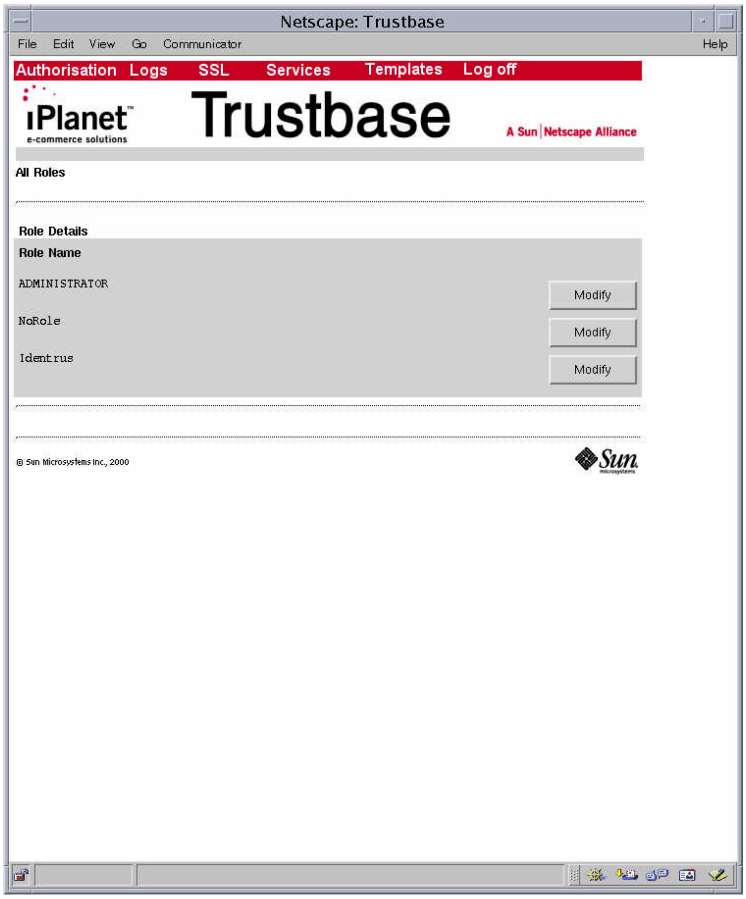
Defining a role

Selecting <Add role> from the main menu will provide a form that contains the following:

- Name - The text label for the new role
- Description - Free text description of the role. This is not used by the authorisation mechanisms, but is useful for describing the use of a particular role
- Active - Unchecked means the router will throw an unauthorised response even if the role to service link is correct.

Submitting the form will update the authorisation tables immediately. After adding a new role, using the view role option from the authorisation menu will contain the updates immediately. The view roles option on the main menu allows the operator to select an existing role and modify the original values. By default the iPlanet™ Trustbase Transaction Manager has three pre-set roles that map to specific users.

Figure 37 List of default Roles


Netscape: Trustbase
File Edit View Go Communicator Help
Authorisation Logs SSL Services Templates Log off
iPlanet e-commerce solutions
Trustbase
A Sun | Netscape Alliance

All Roles

Role Details

Role Name	
ADMINISTRATOR	Modify
NoRole	Modify
Identrus	Modify

© Sun Microsystems Inc, 2000

- Administrator This role allows Administration access to all configuration screens.
- NoRole	This is a role that is not active and is currently for internal use only. It is a holder for assigning "items" no role.
- Identrus	This role allows access to Identrus Services. At present there is one main service IdentrusCSCService that performs certificate status

checks and forms the basis of all Validation, verification , integrity and authentication.

Note: The iPlanet™ Trustbase Transaction Manager contains a default Role 'NoRole'. This is used internally by the iPlanet™ Trustbase Transaction Manager Services and should not be modified of removed.

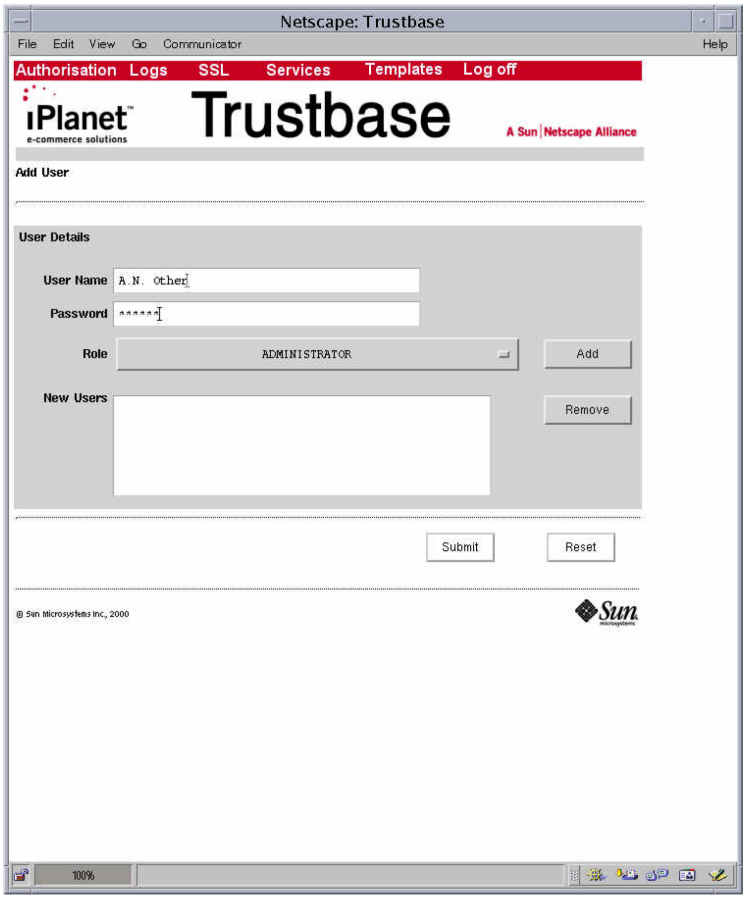
Adding users to roles

Users may be identified in one of two ways:

- Username and Password
- Certificate

The username and password authorisation is generally used for operational management of the iPlanet™ Trustbase Transaction Manager. This allows operators to log onto the systems and interact with the management screens as shown in this manual.

Figure 38 Add New User


Netscape: Trustbase
File Edit View Go Communicator Help
Authorisation Logs SSL Services Templates Log off
iPlanet e-commerce solutions
Trustbase
A Sun | Netscape Alliance
Add User
User Details
Add
Remove
Submit
Reset
© Sun Microsystems Inc., 2000
Sun microsystems
100%

User Name: A.N. Other

Password: ******

Role: ADMINISTRATOR

New Users:

New usernames can be added using the <New user> button on the Authorisation home page. The following input is required for each user:

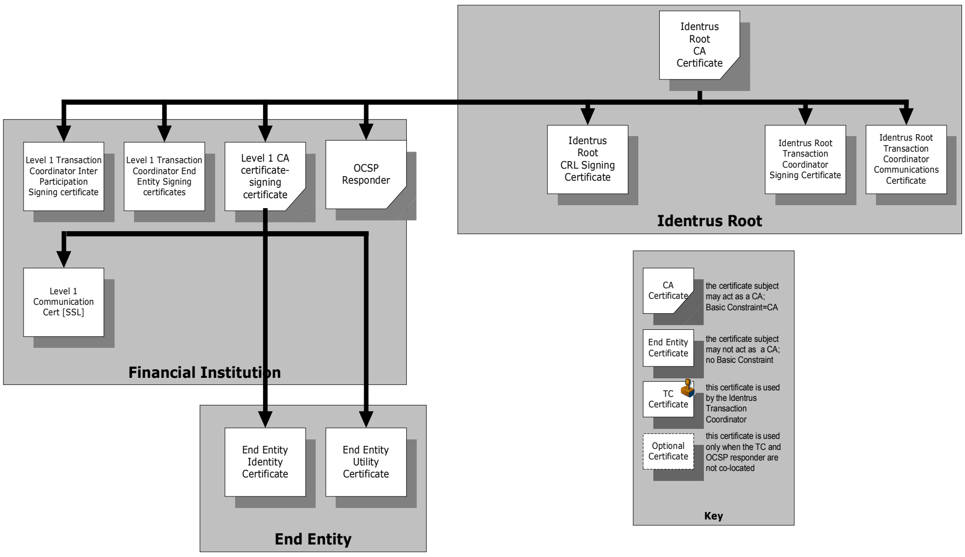
- Username
- Password
- Role - This is only from the selection of existing roles

A number of users may be added prior to submitting the form. Once a set of users have been added they immediately become active in the Authorisation tables and are capable of using the role assigned to them.

Adding a Certificate

Certificate authentication is used for Identrus messages, and before a third party may interact with the iPlanet™ Trustbase Transaction Manager they must have the certificate details entered in the Authorisation system. iPlanet™ Trustbase Transaction Manager removes the need to enter every known certificate in the Authorisation table by allowing the use of parent certificates in lieu of the actual certificate.

Figure 39 Identrus PKI hierarchy


Identrus Root CA Certificate
Level 1 Transaction Coordinator Inter Participation Signing certificate
Level 1 Transaction Coordinator End Entity Signing certificates
Level 1 CA certificate-signing certificate
OCSP Responder
Identrus Root CRL Signing Certificate
Identrus Root Transaction Coordinator Signing Certificate
Identrus Root Transaction Coordinator Communications Certificate
Identrus Root
Level 1 Communication Cert [SSL]
Financial Institution
End Entity Identity Certificate
End Entity Utility Certificate
End Entity
CA Certificate
the certificate subject may act as a CA; Basic Constraint=CA
End Entity Certificate
the certificate subject may not act as a CA; no Basic Constraint
TC Certificate
this certificate is used by the Identrus Transaction Coordinator
Optional Certificate
this certificate is used only when the TC and OCSP responder are not co-located
Key

In the Identrus PKI hierarchy the End Entity Identity certificates issued by the Level 1 CA are used by the Relying Customer to sign requests to the iPlanet™ Trustbase Transaction Manager. The Level 1 Transaction Manager Inter-Participant Signing Certificate is used to sign requests made between the various iPlanet™ Trustbase Transaction Managers during a certificate status check.

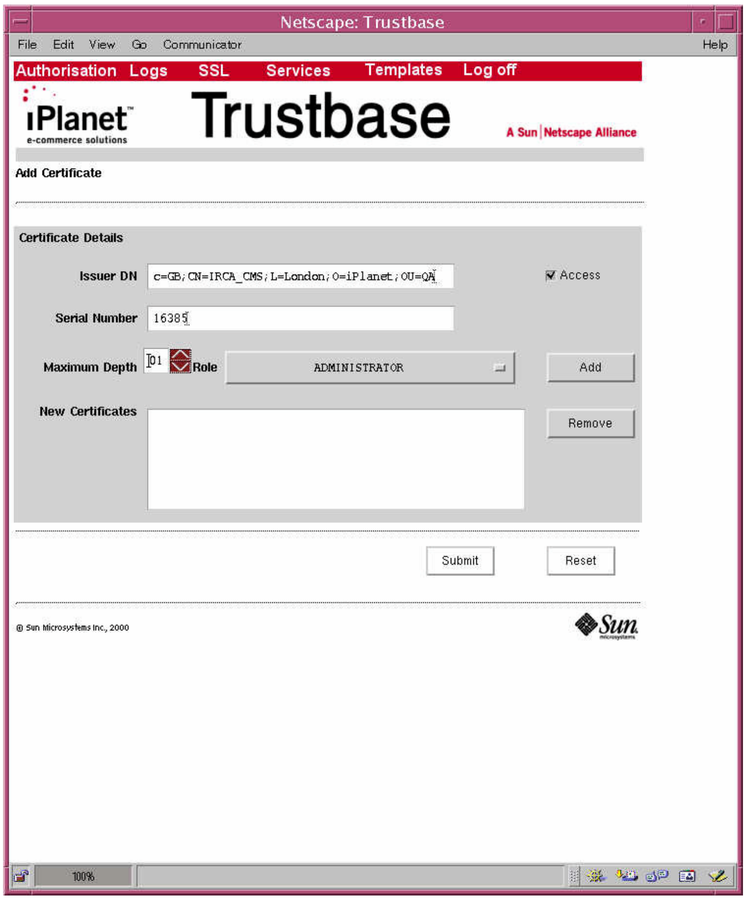
The complete set of Identrus operations may be authorised by placing a single certificate in the authorisation system. This certificate is the Identrus Root CA Certificate. This Root CA certificate must be entered with a Maximum Depth value of 2. This indicates that certificates issued up to 2 levels below the Root CA certificate i.e. The Level 1 Transaction Manager End Entity Signing Certificate, and the Inter-Participant Signing Certificate(s) will be mapped onto the same Role as the Identrus Root CA certificate.

To add an authorisation based on a certificate select <Add Certificates> on the Authorisation main page. The form presented requires the following information for each certificate:

- Issuer DN - This field is case sensitive and DN information entered in the incorrect case will case an authorisation failure for the certificate.

- Serial Number
- Maximum depth - Maximum length of the chain between this certificate and the child certificate capable of using this role.
- Role - Selected from the list of previously defined roles
- Access - Toggle on for this certificate to be active

Figure 40 Adding a Certificate


Netscape: Trustbase
File Edit View Go Communicator Help
Authorisation Logs SSL Services Templates Log off
iPlanet e-commerce solutions
Trustbase
A Sun|Netscape Alliance
Submit
Reset
Add
Remove
© Sun Microsystems Inc., 2000
Sun microsystems
100%

Add Certificate

Certificate Details

Issuer DN: c=GB;CN=IRCA_CMS;L=London;O=iPlanet;OU=QA

☑ Access

Serial Number: 16385

Maximum Depth: 01

Role: ADMINISTRATOR

New Certificates:

The active toggle allows the operator to explicitly override an inherited authorisation. This means that a parent certificate may be used to authorise a large number of issued certificates except those that have an explicit entry in the Authorisation table with the Access toggle off. This mechanism is useful in situations where a certificate requires suspension for a period of time prior to the CA revoking it.

Mapping roles to Services

Having created a role and mapped a set of users to the role the final step is to define the set of services that may be accessed using the role.

Each service is capable of being accessed by a single role. This requires some design and thought to the authorisation mappings prior to modifying an existing authorisation mechanism. By default the iPlanet™ Trustbase Transaction Manager contains an existing set of role to service mappings that allow the following:

- Operators to configure the installation using the configuration facilities described in this guide. This maps onto the “Administrator” role name.

- Holders of End Entity Certificates to access the approved set of Identrus service subject to mapping the certificate details onto the “Identrus” role.

To map a new service to a role select new service on the Authorisation main menu. The form requires the following information:

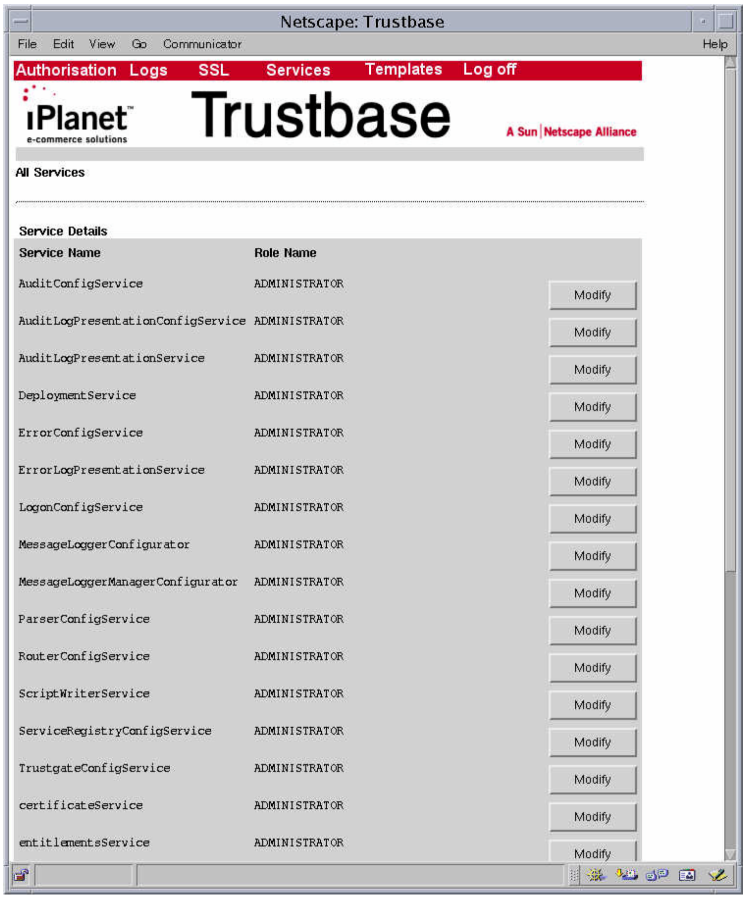
- Service name - The short name of the service found in the tbase.properties file

- Role – The name of the role

A number of service to role mappings may be added to the list at the bottom of the form prior to submitting the form. Once the mappings have been submitted to the authorisation database they are effective immediately.

To modify an existing service to role mapping, select the edit services from the Authorisation main menu. This presents a list of the entire role to service mapping database for inspection. Selecting the Modify link on a particular item in the list will allow the details of the specific entry to be updated.

Figure 41 Services to role mapping list



All Services

Service Details

Service Name	Role Name	
AuditConfigService	ADMINISTRATOR	Modify
AuditLogPresentationConfigService	ADMINISTRATOR	Modify
AuditLogPresentationService	ADMINISTRATOR	Modify
DeploymentService	ADMINISTRATOR	Modify
ErrorConfigService	ADMINISTRATOR	Modify
ErrorLogPresentationService	ADMINISTRATOR	Modify
LogonConfigService	ADMINISTRATOR	Modify
MessageLoggerConfigurator	ADMINISTRATOR	Modify
MessageLoggerManagerConfigurator	ADMINISTRATOR	Modify
ParserConfigService	ADMINISTRATOR	Modify
RouterConfigService	ADMINISTRATOR	Modify
ScriptWriterService	ADMINISTRATOR	Modify
ServiceRegistryConfigService	ADMINISTRATOR	Modify
TrustgateConfigService	ADMINISTRATOR	Modify
certificateService	ADMINISTRATOR	Modify
entitlementsService	ADMINISTRATOR	Modify

Chapter 6

Logs

Logs allow you to maintain control over messaging in terms of what errors are being generated together with an audit. These can be viewed. Options are available to configure the level of detail that can be seen on the screen.

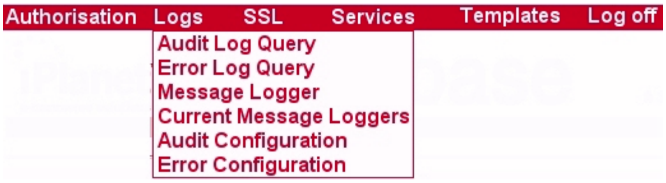
There is also a raw log that provides detail of all message transactions that take place. These can be viewed using any standard Oracle tool.

Introduction

iPlanet™ Trustbase Transaction Manager allows configuration of three kinds of Logs, two of which are directly viewable:

- The Audit log contains entries about the flow of a message as it passes through the iPlanet™ Trustbase Transaction Manager framework (e.g. message handler, Router). This log can be useful in diagnosing problems in configurations.
- The Error log contains entries of any runtime problems both from the iPlanet™ Trustbase Transaction Manager framework and the Identrus specific components.
- The Raw log is only used for Logging Identrus messages both received and sent. This log is not directly viewable.

Figure 42 Logs Main Menu



Audit log

Audits can be configured in terms of their types. They can also be queried. The following audit types are available:

Trustbase Audits:

- ROUTER_ABORT_ROUTING
  This audit occurs when the rule based router aborts routing due to illegal rules.

- ROUTER_CONFIG
  This audit occurs when a change is made to the rules via the rule configuration screens.

- ROUTER_CONSTRUCTION
  This audit occurs when new rule sets are constructed at start up.

- ROUTER_CONTEXT_DIRECTIVE
  This audit occurs whenever the router executes one of the following router directives: EndContext, StartContext or ReturnToUser.

- ROUTER_ROUTE_MESSAGE
  This audit occurs whenever a message is routed to a service.

- ROUTER_START
  This audit occurs whenever the rule based router component is initialized.

- CONFIGURATION_CHANGE
  This audit occurs whenever a Trustbase configuration is changed.

- OPERATION_ABORT
  This audit occurs whenever a service has to abort the processing of a message.

- OPERATION_BEGIN
  This audit occurs whenever a service begins processing a message.

- OPERATION_COMPLETE
  This audit occurs whenever a service successfully completes the processing of a message.

- PARSER_STARTUP
  This audit occurs whenever the Message Analyzer component is started.

- SECURITY_CHANGE
  This audit occurs whenever a generic security related event occurs.

- TAS_SHUTDOWN
  This audit occurs when Trustbase is shutdown.

- TAS_STARTUP
  This audit occurs when Trustbase is started.

- ROLE_SERVICE_MAPPING_CHANGED
  This audit occurs whenever a mapping between a service and a role is changed or added in the entitlements configuration.

- DEFAULT_SECURITY_ROLE_USED
  This audit occurs whenever the authentication component cannot find a specific mapping between a user and a role – it indicates that the default security role has been applied to that user.

- CERT_BASED_ROLE_MAPPING_CHANGED
  This audit occurs whenever a mapping between a certificate and a security role is made in the entitlements configuration.

- USER_PASS_BASED_ROLE_MAPPING_CHANGED
  This audit occurs whenever a mapping between a username/password and a security role is made in the entitlements configuration.

Identrus Transaction Co-ordinator Audits:

- CSC_PROCESSING

  This audit occurs whenever a Certificate Status Check is being made.

- CSC_DEBUGGING

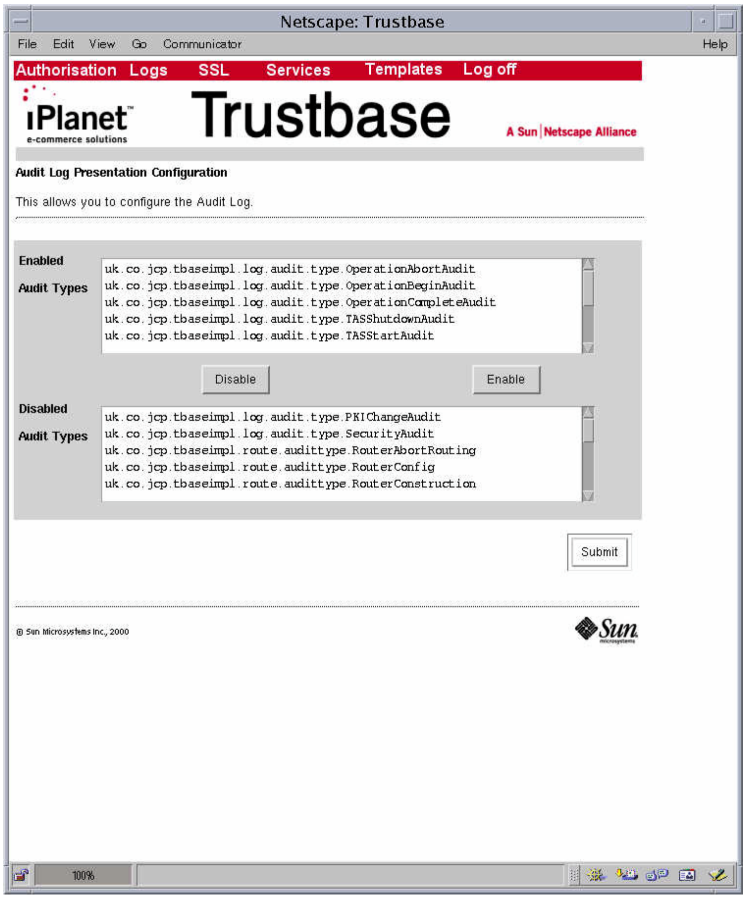
  This audit occurs if you wish to debug a certificate Status Check.

Audit Configuration

Audit Log Configuration allows you to select which audit types are physically viewable. Audit types are either enabled, i.e. they are logged and can be viewed, or disabled, i.e. no information is logged about these types.

In order to configure what gets logged: Select <Audit Configuration> from the main Log Menu.

Figure 43 Configure Audit



Netscape: Trustbase
File Edit View Go Communicator Help
Authorisation Logs SSL Services Templates Log off
iPlanet e-commerce solutions
Trustbase
A Sun | Netscape Alliance

Audit Log Presentation Configuration

This allows you to configure the Audit Log.

Enabled Audit Types

```
uk.co.jcp.tbaseimpl.log.audit.type.OperationAbortAudit
uk.co.jcp.tbaseimpl.log.audit.type.OperationBeginAudit
uk.co.jcp.tbaseimpl.log.audit.type.OperationCompleteAudit
uk.co.jcp.tbaseimpl.log.audit.type.TASShutdownAudit
uk.co.jcp.tbaseimpl.log.audit.type.TASStartAudit
```

Disabled Audit Types

```
uk.co.jcp.tbaseimpl.log.audit.type.PKIChangeAudit
uk.co.jcp.tbaseimpl.log.audit.type.SecurityAudit
uk.co.jcp.tbaseimpl.route.audittype.RouterAbortRouting
uk.co.jcp.tbaseimpl.route.audittype.RouterConfig
uk.co.jcp.tbaseimpl.route.audittype.RouterConstruction
```

- Mouse <Left Click> on the audit type you wish to enable/disable.

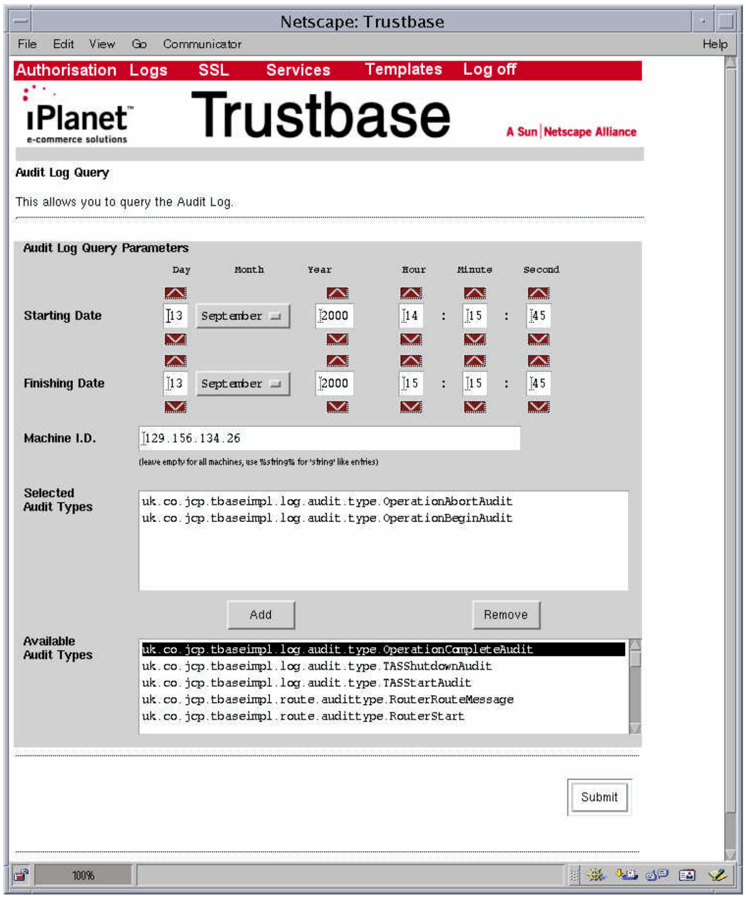
- Select <enable> or <disable>

Audit viewing

You can view the audit log by selecting a date range (Start and end date) and machine ID (IP Address). The machine I.D. refers in this case to the machine that is making the log. You can restrict or expand your view by removing or making available the appropriate audit types. Having made your selection the Date, Machine ID, Audit type and message content are displayed on the output screen.

In order to select what you want to view: Select <Audit Log Query> from Main Log menu

Figure 44 Audit View


Netscape: Trustbase
File Edit View Go Communicator
Help
Authorisation Logs SSL Services Templates Log off
iPlanet™
e-commerce solutions
Trustbase
A Sun | Netscape Alliance
100%

Audit Log Query

This allows you to query the Audit Log.

Audit Log Query Parameters

	Day	Month	Year	Hour	Minute	Second
Starting Date	13	September	2000	14	15	45
Finishing Date	13	September	2000	15	15	45

Machine I.D. 129.156.134.26

(leave empty for all machines, use %string% for 'string' like entries)

Selected Audit Types

```
uk.co.jcp.tbaseimpl.log.audit.type.OperationAbortAudit
uk.co.jcp.tbaseimpl.log.audit.type.OperationBeginAudit
```

Add Remove

Available Audit Types

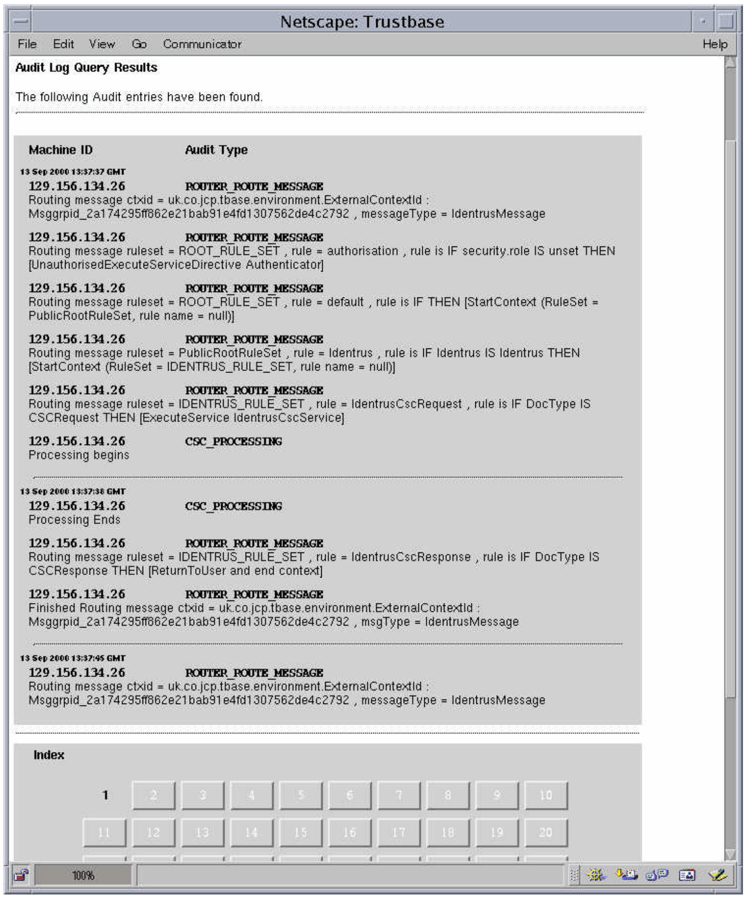
```
uk.co.jcp.tbaseimpl.log.audit.type.OperationCompleteAudit
uk.co.jcp.tbaseimpl.log.audit.type.TASShutdownAudit
uk.co.jcp.tbaseimpl.log.audit.type.TASStartAudit
uk.co.jcp.tbaseimpl.route.audittype.RouterRouteMessage
uk.co.jcp.tbaseimpl.route.audittype.RouterStart
```

Submit

For more detailed log viewing, as all information is stored in a standard Oracle database, any third party database reporting tool may also be used.

The screen, as illustrated in Figure 45 Audit Results, might produce an output similar to the following audit:

Figure 45 Audit Results



Audit Log Query Results

The following Audit entries have been found.

```
Machine ID          Audit Type
13 Sep 2000 13:37:37 GMT
129.156.134.26      ROUTER_ROUTE_MESSAGE
Routing message ctxid = uk.co.jcp.tbase.environment.ExternalContextId :
Msggrpid_2a174295ff862e21bab91e4fd1307562de4c2792 , messageType = IdentrusMessage

129.156.134.26      ROUTER_ROUTE_MESSAGE
Routing message ruleset = ROOT_RULE_SET , rule = authorisation , rule is IF security.role IS unset THEN
[UnauthorisedExecuteServiceDirective Authenticator]

129.156.134.26      ROUTER_ROUTE_MESSAGE
Routing message ruleset = ROOT_RULE_SET , rule = default , rule is IF THEN [StartContext (RuleSet =
PublicRootRuleSet, rule name = null)]

129.156.134.26      ROUTER_ROUTE_MESSAGE
Routing message ruleset = PublicRootRuleSet , rule = Identrus , rule is IF Identrus IS Identrus THEN
[StartContext (RuleSet = IDENTRUS_RULE_SET, rule name = null)]

129.156.134.26      ROUTER_ROUTE_MESSAGE
Routing message ruleset = IDENTRUS_RULE_SET , rule = IdentrusCscRequest , rule is IF DocType IS
CSCRequest THEN [ExecuteService IdentrusCscService]

129.156.134.26      CSC_PROCESSING
Processing begins

13 Sep 2000 13:37:38 GMT
129.156.134.26      CSC_PROCESSING
Processing Ends

129.156.134.26      ROUTER_ROUTE_MESSAGE
Routing message ruleset = IDENTRUS_RULE_SET , rule = IdentrusCscResponse , rule is IF DocType IS
CSCResponse THEN [ReturnToUser and end context]

129.156.134.26      ROUTER_ROUTE_MESSAGE
Finished Routing message ctxid = uk.co.jcp.tbase.environment.ExternalContextId :
Msggrpid_2a174295ff862e21bab91e4fd1307562de4c2792 , msgType = IdentrusMessage

13 Sep 2000 13:37:45 GMT
129.156.134.26      ROUTER_ROUTE_MESSAGE
Routing message ctxid = uk.co.jcp.tbase.environment.ExternalContextId :
Msggrpid_2a174295ff862e21bab91e4fd1307562de4c2792 , messageType = IdentrusMessage
```

Index

1 2 3 4 5 6 7 8 9 10
11 12 13 14 15 16 17 18 19 20

If results do not fit on one page there is an index tab, as illustrated at the bottom of the screen. Users intending to search using SQL should refer to the sql table AUDITDATA.

Raw Logging

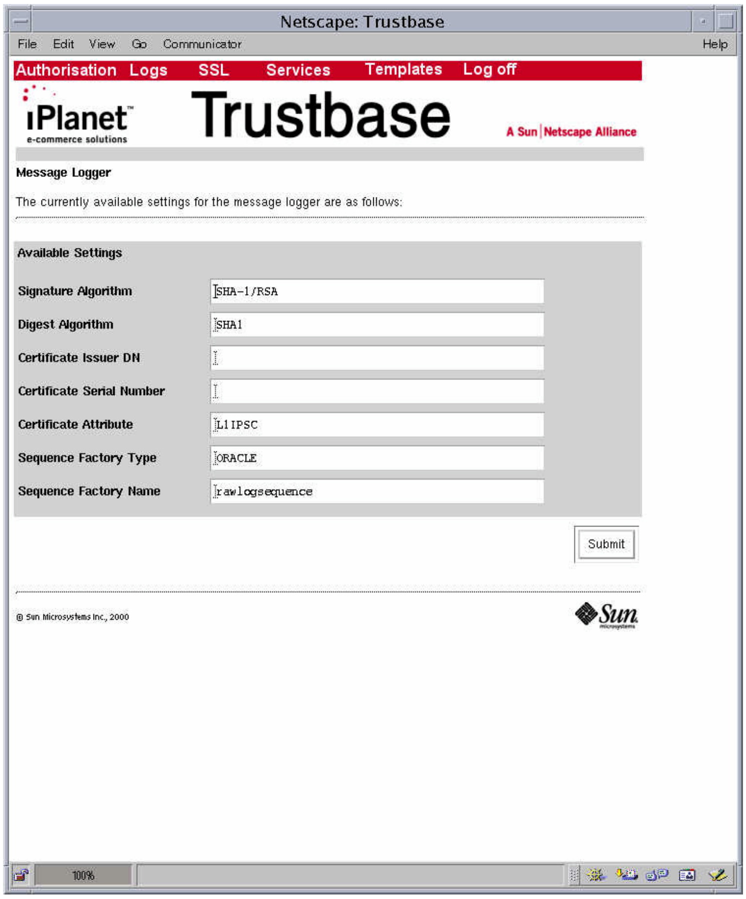
As part of being an Identrus member, you are required to maintain and archive a raw log. The goals fulfilled by logging the raw data are:

- Non Repudiation support – a complete transactional log that provides evidentiary support for transactions.

- Auditing – a complete transactional log that assists auditing the activities of iPlanet™ Trustbase Transaction Manager.

There are a number of ways this can be configured. In particular this feature allows you to define how messages are written, in terms of your security policy, via the Message logger.

Figure 46 Message logging settings



Netscape: Trustbase
File Edit View Go Communicator Help
Authorisation Logs SSL Services Templates Log off
iPlanet™ e-commerce solutions
Trustbase
A Sun|Netscape Alliance

Message Logger

The currently available settings for the message logger are as follows:

Available Settings

Signature Algorithm	SHA-1/RSA
Digest Algorithm	SHA1
Certificate Issuer DN	
Certificate Serial Number	
Certificate Attribute	L1IPSC
Sequence Factory Type	ORACLE
Sequence Factory Name	rawlogsequence

Submit
© Sun Microsystems Inc., 2000
Sun microsystems
100%

Normally these options, listed below, do not need to be changed:

- Signature Algorithm - By default the SHA-1/RSA algorithm is used to sign entries in the raw log. The options depend on the cryptographic security provider being utilised.

- Digest Algorithm - By default the SHA-1 algorithm is used to digest entries in the raw log. The digest is used as part of the raw log mechanism that ensures no tampering of the log contents.

- Certificate Issuer DN - This option is only used if the certificate attribute option is left blank. It allows the specification of the distinguished name for the certificate to be used for signing the raw log.

- Certificate Serial Number - This option is used in conjunction with the issuer DN option above, to specify the serial number of the certificate used to sign the raw log.

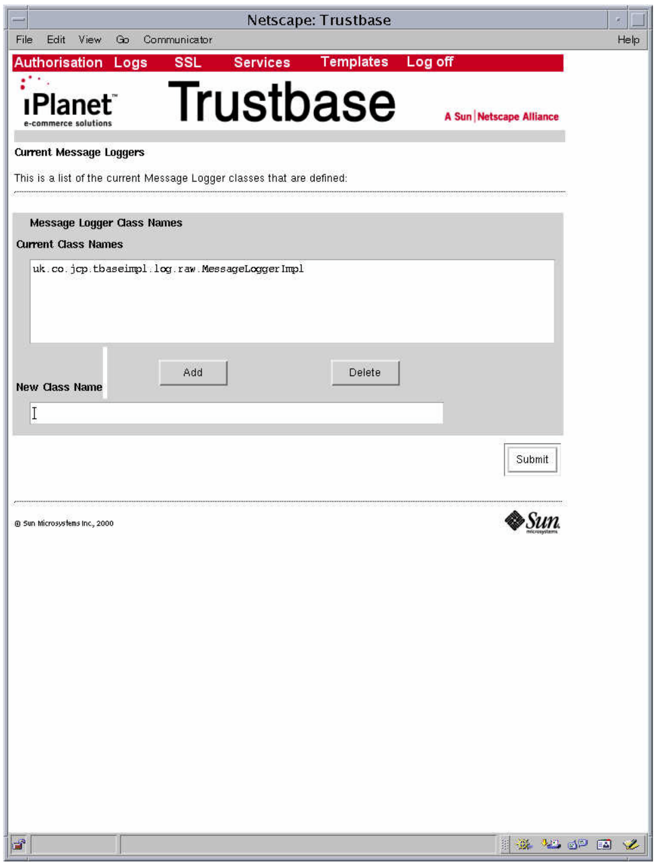
- Certificate Attribute - This option is only used if the issuer DN and serial number fields are blank. By default, this field contains the value L1IPSC that indicates the certificate purpose ID, inter-participant signing certificate.

- Sequence Factory Type - This option should not be changed. It is for internal purpose only and affects the way data is sequenced for different database providers (e.g Oracle).

- Sequence Factory Name - This option should not be changed. It is for internal purpose only and affects the way data is sequenced for different database providers (e.g Oracle).

The message logger places the raw data it receives into the logs for safe-keeping. It will log data for Identrus specific transactions that it supports and for only those transactions. This raw data contains information in plain text and base64 encoding that gets signed by the message logger to provide the kinds of guarantees mentioned previously. At present there is only one Java message logger class implementation and therefore this option should not be changed.

Figure 47 Configuring the Message logger



Current Message Loggers

This is a list of the current Message Logger classes that are defined:

Message Logger Class Names

Current Class Names

uk.co.jcp.tbaseimpl.log.raw.MessageLoggerImpl

New Class Name

© Sun Microsystems Inc, 2000

Note The raw log can be displayed from Oracle using the RAW_DATA table e.g. “ select * from raw_data displaying MSGRPID”.

Errors

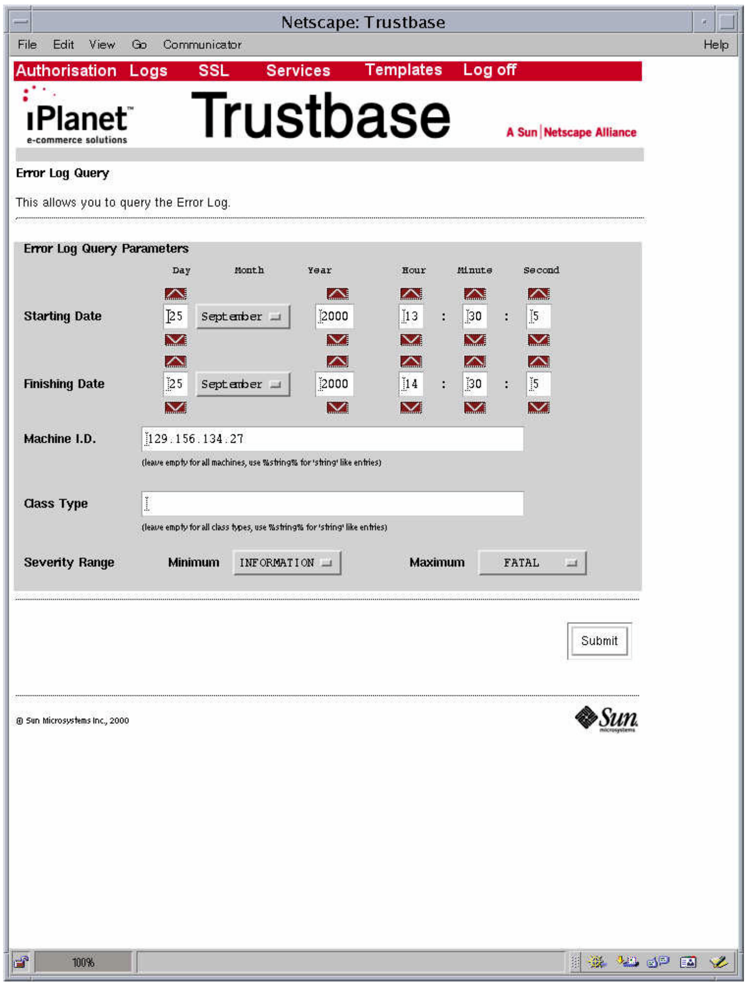
Errors are now discussed in four sections:

- How to view errors
- What the severity of an error means
- Where to find a list of core iPlanet™ TrustbaseTransaction Manager error messages
- A table summary of all Identrus specific error messages

Viewing

You can view the error log by selecting a date range (start and end dates) and machine ID (IP Address). You can restrict or expand your view by specifying a minimum and maximum error severity. Additionally, by specifying a Java class, errors can be viewed that are produced by that class only. Having made your selection the Date, Machine ID, class type and error message are displayed on the output screen. For example the following selection:

Figure 48 Error Log Query



Error Log Query

This allows you to query the Error Log.

Error Log Query Parameters

	Day	Month	Year	Hour		Minute		Second
Starting Date	25	September	2000	13	:	30	:	5
Finishing Date	25	September	2000	14	:	30	:	5

Machine I.D. 129.156.134.27

(leave empty for all machines, use %string% for 'string' like entries)

Class Type

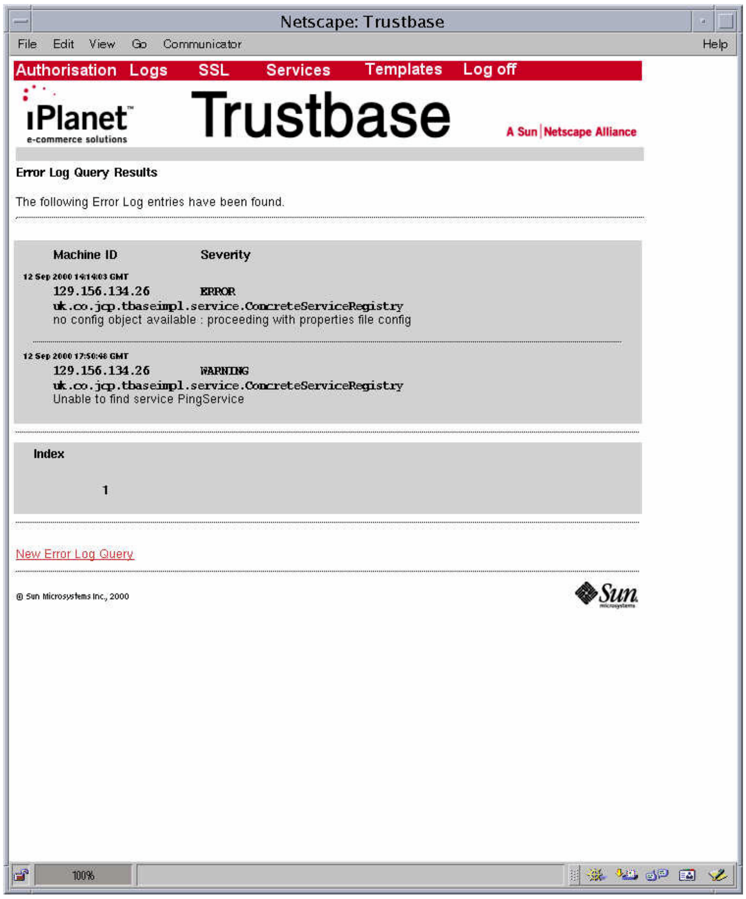
(leave empty for all class types, use %string% for 'string' like entries)

Severity Range Minimum INFORMATION Maximum FATAL

The Error log can be displayed from Oracle using the ERRORVIEW table e.g. " select * from ERRORVIEW"

The screen shown on the previous page might produce an output similar to the following errors:

Figure 49 Error Log Query Results



Netscape: Trustbase
File Edit View Go Communicator Help
Authorisation Logs SSL Services Templates Log off
iPlanet e-commerce solutions
Trustbase
A Sun | Netscape Alliance

Error Log Query Results

The following Error Log entries have been found.

```
    Machine ID           Severity
12 Sep 2000 14:14:03 GMT
    129.156.134.26       ERROR
    uk.co.jcp.tbaseimpl.service.ConcreteServiceRegistry
    no config object available : proceeding with properties file config

12 Sep 2000 17:50:48 GMT
    129.156.134.26       WARNING
    uk.co.jcp.tbaseimpl.service.ConcreteServiceRegistry
    Unable to find service PingService
```

Index

1

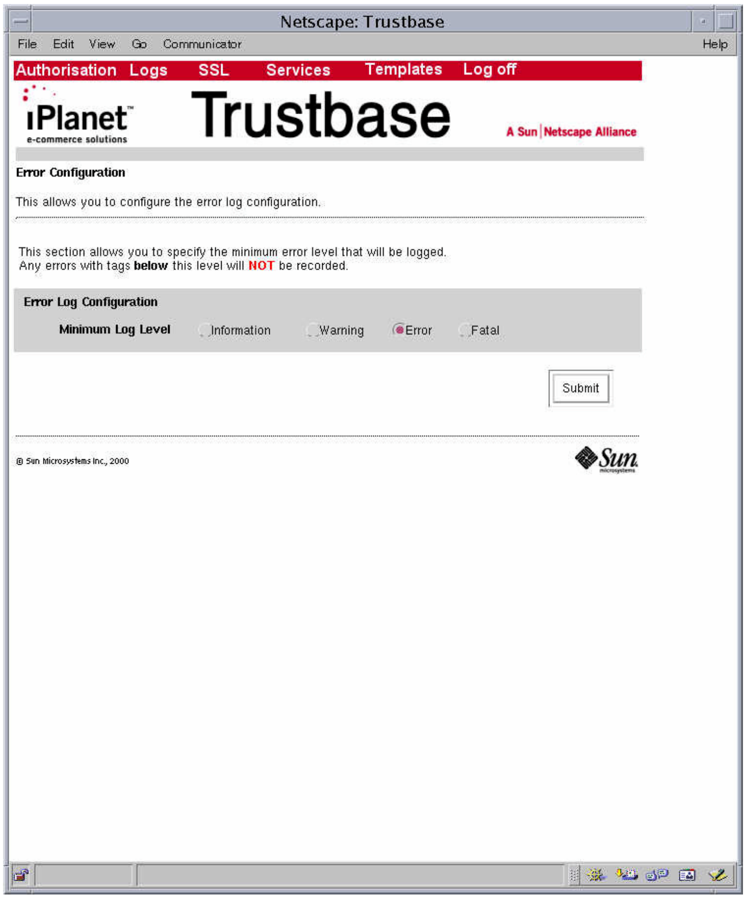
New Error Log Query

© Sun Microsystems Inc., 2000

Configuring Error Event Types

This section allows you to specify the minimum error level that will be logged. Any errors with tags below this level will NOT be recorded.

Figure 50 Error Log Configuration



Netscape: Trustbase
File Edit View Go Communicator Help
Authorisation Logs SSL Services Templates Log off
iPlanet e-commerce solutions
Trustbase
A Sun|Netscape Alliance

Error Configuration

This allows you to configure the error log configuration.

This section allows you to specify the minimum error level that will be logged.
Any errors with tags **below** this level will **NOT** be recorded.

Error Log Configuration

Minimum Log Level ○ Information ○ Warning ● Error ○ Fatal

Submit
© Sun Microsystems Inc., 2000
Sun microsystems

iPlanet™ Trustbase Transaction Manager defines an error as a severity, the class of object defining the error, and a programmer defined message. The default implementation defines four constants that indicate the various severity levels:

- INFORMATION - This constant is to be used to log informational events, which are not necessarily errors - this should be used sparingly.
- WARNING - This constant is to be used for error conditions that are expected and handled, but require logging for behaviour analysis.
- ERROR - This constant is to be used for serious errors which indicate that something is inherently incorrect with the system, but that allow processing to continue, or be retried.
- FATAL - This constant is to be used for fatal errors from which processing cannot recover, these errors would result in the abandoning of processing.

Error Messages

Error messages fall into two categories, those that are produced by the iPlanet™ Trustbase Transaction Manager framework and those produced by Identrus services. For instance, Identrus message codes fall into a number of categories:

- Message Writer Errors
- Message Reader Errors
- Certificate Status Check Errors

Details of what all TTM core iPlanet™ Trustbase Transaction Manager error messages mean can be found in your Oracle Database in a table called error_codes as illustrated below:

Figure 51 Selecting Error codes from your Oracle Database

```
su -
cd /app/Trustbase/TTM/V2.2/Config/sql
sqlplus tbase/tbase
select * from error_codes;
```

Chapter 7

SSL

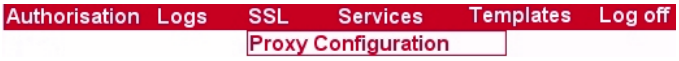
SSL Configuration allows you to define parameters that determine security while messages are being transported over the network. Configuration options include:

- How to change the number of connections and port settings of the proxy
- How to change the SSL protocol settings
- How to change the certificate store used by the SSL proxy
- How to redirect the SSL proxy to use a different Web server

Overview

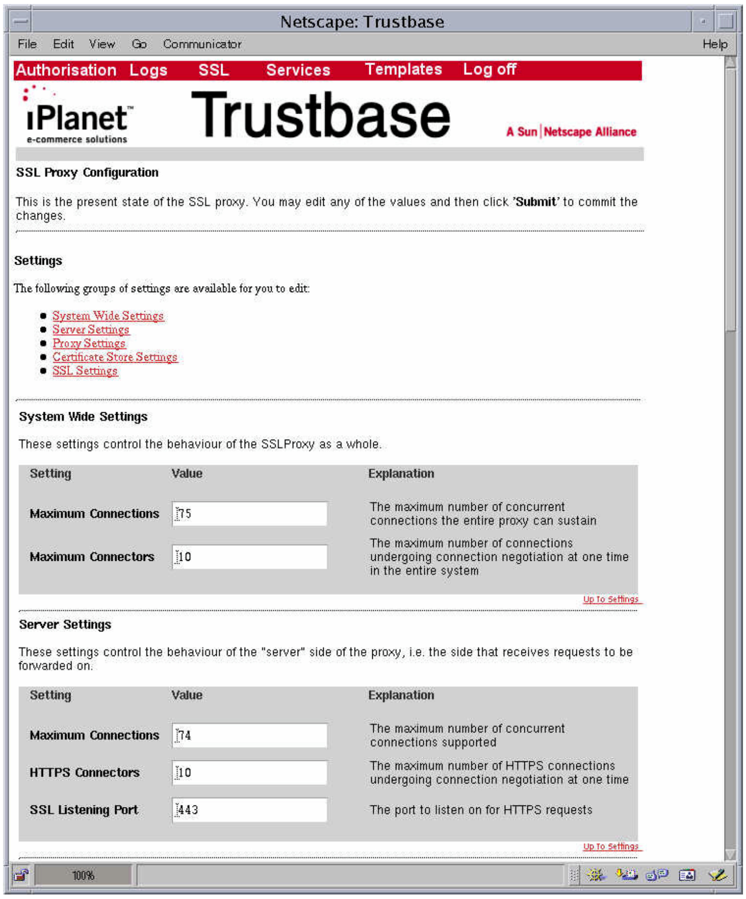
The Proxy may be configured using the security user logon.

Figure 52 SSL Main Menu



- The SSL Proxy selections take you to the SSLProxy configuration home page.

Figure 53 SSL Proxy Settings


Netscape: Trustbase
File Edit View Go Communicator Help
Authorisation Logs SSL Services Templates Log off
iPlanet
e-commerce solutions
Trustbase
A Sun | Netscape Alliance
100%

SSL Proxy Configuration

This is the present state of the SSL proxy. You may edit any of the values and then click '**Submit**' to commit the changes.

Settings

The following groups of settings are available for you to edit:

- System Wide Settings
- Server Settings
- Proxy Settings
- Certificate Store Settings
- SSL Settings

System Wide Settings

These settings control the behaviour of the SSLProxy as a whole.

Setting	Value	Explanation
Maximum Connections	75	The maximum number of concurrent connections the entire proxy can sustain
Maximum Connectors	10	The maximum number of connections undergoing connection negotiation at one time in the entire system

Up to Settings

Server Settings

These settings control the behaviour of the "server" side of the proxy, i.e. the side that receives requests to be forwarded on.

Setting	Value	Explanation
Maximum Connections	74	The maximum number of concurrent connections supported
HTTPS Connectors	10	The maximum number of HTTPS connections undergoing connection negotiation at one time
SSL Listening Port	443	The port to listen on for HTTPS requests

Up to Settings

The SSL proxy options are all contained on the SSL Proxy configuration main page. Selecting the links at the top of the page moves it to individual sections. The details of the input required in these sections are outlined below under the specific task headings.

Any number of modifications may be made prior to submitting the form using the button at the bottom of the page. If the update fails on validation the values that have failed change are reported back. If all of the updates succeed then the operation is reported as successful.

Note At the end of this screen, there is an expert settings section that enable iPlanet™ employees to diagnose problems with the SSL proxy. This should not be used during the normal configuration of the SSL proxy. See also Architectural Configuration on Page 49for more information on how to install the SSLProxy on a separate machine.

Changing incoming connection information

Incoming connection information is changes under the following options from the SSL proxy configuration page:

- Proxy settings
- System wide settings
- Server settings

The SSL proxy listens for incoming connections on a particular TCP/IP port on the local machine. This is generally port 443 and is set during the installation to this default. In order to modify the port the proxy listens on the change must be made under the Proxy Settings option, and the proxy re-started.

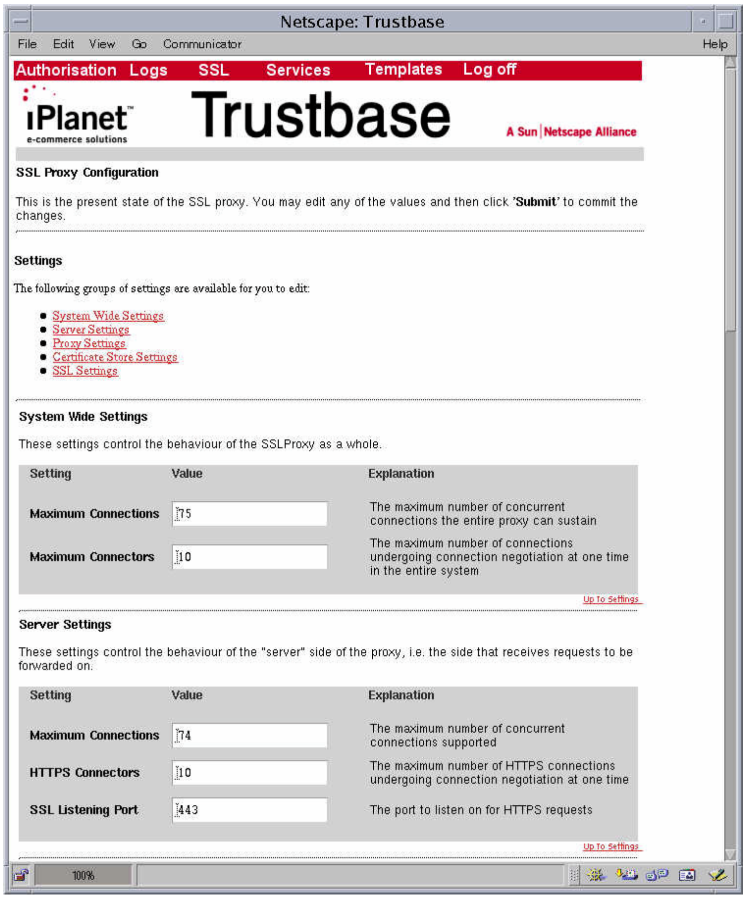
- SSL Listener port – This is the port on which the server will wait for requests – if you are using HTTPS then the default port should be 443.

Note Port 443 is the designated SSL port and changes to the port number will require clients to know the new setting. In the iPlanet™ Trustbase Transaction Manager the port number the client uses is encoded into the certificate AIA. Changing the SSL proxy port number will cause clients or other Transaction Coordinators to fail in contacting the Identrus Transaction Co-ordinator.

One of the main administration requirements for the SSL proxy is to ensure that the load on the proxy machine does not cause the incoming connections to be dropped. Each SSL connection requires significant CPU to negotiate the session parameters (Handshake), and allowing a large number of SSL negotiations at a single time may cause clients to time out. To avoid this situation the SSL proxy may be configured to reject new connections when it is already loaded.

System wide settings

Figure 54 SSL Proxy System Wide Settings


Netscape: Trustbase
File Edit View Go Communicator Help
Authorisation Logs SSL Services Templates Log off
iPlanet e-commerce solutions
Trustbase
A Sun|Netscape Alliance
100%

SSL Proxy Configuration

This is the present state of the SSL proxy. You may edit any of the values and then click '**Submit**' to commit the changes.

Settings

The following groups of settings are available for you to edit:

- System Wide Settings
- Server Settings
- Proxy Settings
- Certificate Store Settings
- SSL Settings

System Wide Settings

These settings control the behaviour of the SSLProxy as a whole.

Setting	Value	Explanation
Maximum Connections	75	The maximum number of concurrent connections the entire proxy can sustain
Maximum Connectors	10	The maximum number of connections undergoing connection negotiation at one time in the entire system

Up To Settings

Server Settings

These settings control the behaviour of the "server" side of the proxy, i.e. the side that receives requests to be forwarded on.

Setting	Value	Explanation
Maximum Connections	74	The maximum number of concurrent connections supported
HTTPS Connectors	10	The maximum number of HTTPS connections undergoing connection negotiation at one time
SSL Listening Port	443	The port to listen on for HTTPS requests

Up To Settings

The options provided under the configuration headings above are:

- Maximum number of proxy connections – The maximum number of connections the proxy will allow. This is a combination of handshaking sessions and sessions in progress, and is generally up to 80 connections depending upon the configuration of the host machine.

- Maximum number of proxy connectors – The maximum number of connections undergoing handshaking at a single point in time. This is generally up to 40 depending upon the configuration of the host machine.

Server Settings.

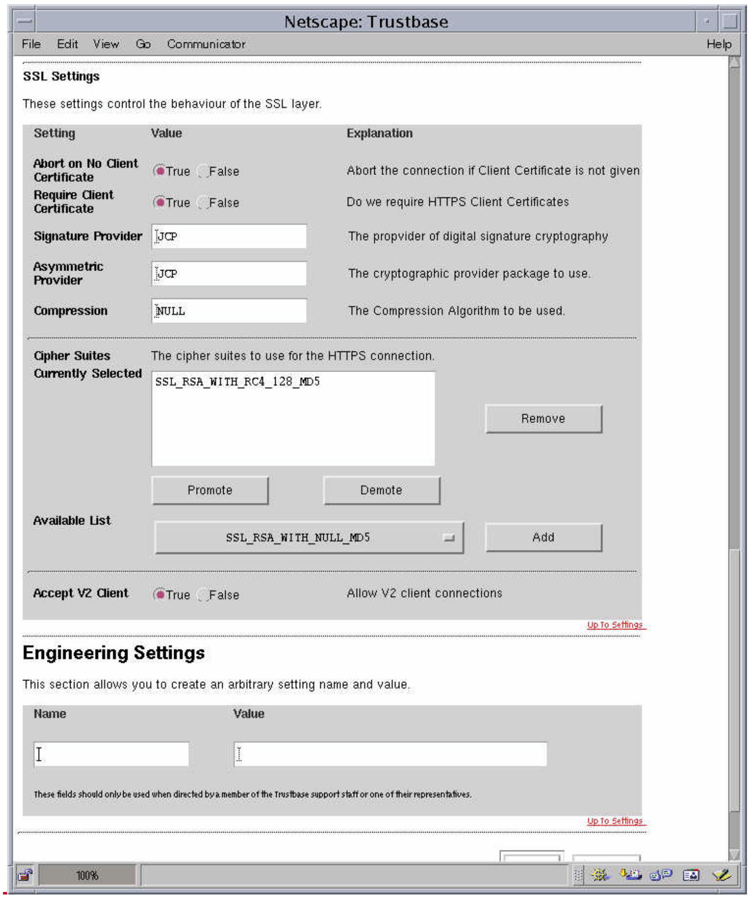
- HTTPS Connectors – This should be set to the same value as maximum number of proxy connections
- Maximum number of connections – This should be set to maximum number of proxy connectors

Note Multiple instances of the SSL proxy are capable of being run in the same JVM for different purposes. The iPlanet™ Trustbase Transaction Manager does not run the SSL proxy in this mode, therefore the server settings must be set to reflect the system wide settings otherwise the minimum values found in either will be used.

SSL protocol & authentication settings

The SSL protocol has a large number of parameters that affect its performance and use. These parameters are may be changed in the SSL settings page.

Figure 55 SSL Settings



SSL Settings

These settings control the behaviour of the SSL layer.

Setting	Value	Explanation
Abort on No Client Certificate	● True ○ False	Abort the connection if Client Certificate is not given
Require Client Certificate	● True ○ False	Do we require HTTPS Client Certificates
Signature Provider	JCP	The propvider of digital signature cryptography
Asymmetric Provider	JCP	The cryptographic provider package to use.
Compression	NULL	The Compression Algorithm to be used.

Cipher Suites Currently Selected: The cipher suites to use for the HTTPS connection.

SSL_RSA_WITH_RC4_128_MD5

Available List: SSL_RSA_WITH_NULL_MD5

Accept V2 Client: ● True ○ False — Allow V2 client connections

Engineering Settings

This section allows you to create an arbitrary setting name and value.

Name	Value

These fields should only be used when directed by a member of the Trustbase support staff or one of their representatives.

The settings may be grouped into:

Protocol settings

- Listener compression – Reserved for future use. Currently set to NULL
- Listener accept V2 client – The SSL proxy implements SSLV3.0. By setting this value to True the proxy will also accept clients using SSLV2.0 hello requests. This provides compatibility for certain types of browser.
- Listener asymmetric provider – The asymmetric provider to use. By default this is NCIPHER for iPlanet™ Trustbase Transaction Manager installations using the nCipher HSM
- Listener cipher suite – The cipher suite to use during SSL Handshake negotiation. By default this is SSL_RSA_WITH_NULL_MD5 for iPlanet™ Trustbase Transaction Manager installations.

Authentication settings

- Listener require client certificate – Set to True for client authenticate SSL sessions.
- Listener abort on bad client certificate – By default set to True to terminate the SSL handshake if the client presents a certificate with an unknown root or an invalid certificate chain.
- Listener abort on no client certificate – Set to True to ensure that the SSL proxy should abort the handshake if the client does not provide a certificate for authentication.

Changing the Certificate Store location

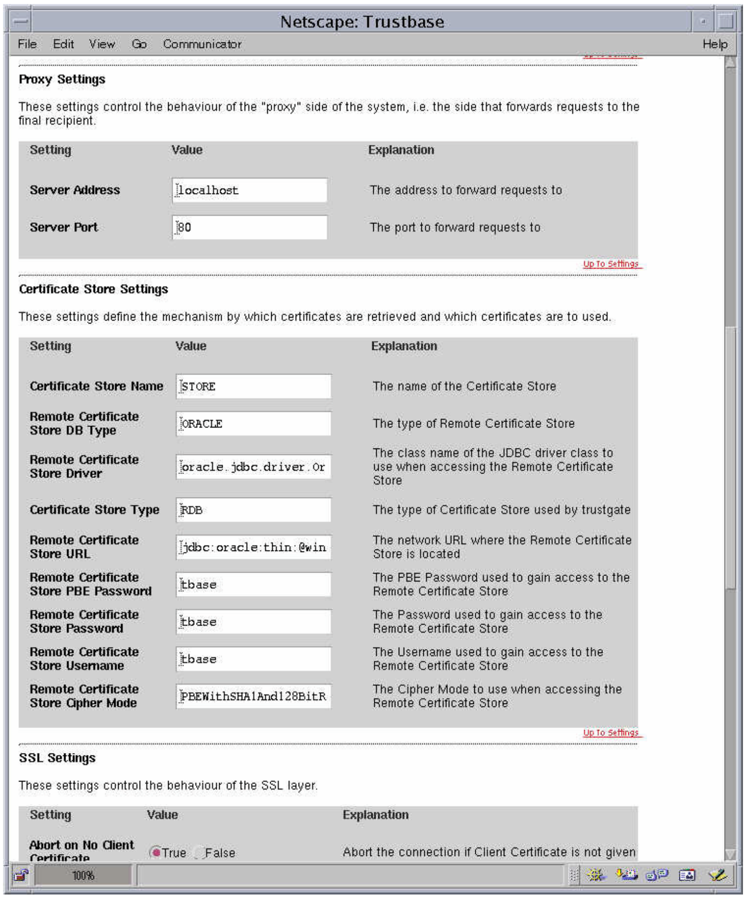
The certificate store used by the SSL proxy is by default the same certificate store used by the iPlanet™ Trustbase Transaction Manager. During the installation process the path to the Oracle database is loaded from the proxy initialisation file into the configuration database, and these value may be changed to allow a proxy to use a local Oracle certificate database rather than the shared certificate database.

In most installations there will be no requirement to use a local database, as this will require the management of certificates and keys in two different locations. In some situations, in particular when an organisation does not wish to open the secondary firewall, these settings may be changed to allow a local certificate database for the SSL proxy.

In order to use a Local certificate store the Oracle user must be known, and the SQL scripts for generating the certificate store tables must have been executed (See Installation guide). The following items may then be changed to point to the new certificate store:

- Listener certstore password – The password to use to unlock the certstore.
- Listener authenticated certificates purpose ID – The purpose ID of set of authenticated certificates.
- Listener server certificates ID – The ID of the server certificate to use.
- Listener cerstore path – The path to the certstore. This is normally set to an Oracle database.

Figure 56 Certificate Store Settings



Proxy Settings

These settings control the behaviour of the "proxy" side of the system, i.e. the side that forwards requests to the final recipient.

Setting	Value	Explanation
Server Address	localhost	The address to forward requests to
Server Port	80	The port to forward requests to

Certificate Store Settings

These settings define the mechanism by which certificates are retrieved and which certificates are to used.

Setting	Value	Explanation
Certificate Store Name	STORE	The name of the Certificate Store
Remote Certificate Store DB Type	ORACLE	The type of Remote Certificate Store
Remote Certificate Store Driver	oracle.jdbc.driver.Or	The class name of the JDBC driver class to use when accessing the Remote Certificate Store
Certificate Store Type	RDB	The type of Certificate Store used by trustgate
Remote Certificate Store URL	jdbc:oracle:thin:@win	The network URL where the Remote Certificate Store is located
Remote Certificate Store PBE Password	tbase	The PBE Password used to gain access to the Remote Certificate Store
Remote Certificate Store Password	tbase	The Password used to gain access to the Remote Certificate Store
Remote Certificate Store Username	tbase	The Username used to gain access to the Remote Certificate Store
Remote Certificate Store Cipher Mode	PBEWithSHA1And128BitR	The Cipher Mode to use when accessing the Remote Certificate Store

SSL Settings

These settings control the behaviour of the SSL layer.

Setting	Value	Explanation
Abort on No Client Certificate	● True ○ False	Abort the connection if Client Certificate is not given

Re-directing the proxy to a web server

The SSL Proxy forwards HTTP data to a Web server located behind the secondary firewall. In some situations it may be necessary to change the location of the Web server (Machine failure etc). When this occurs, the SSL proxy must be re-directed to the location of the new Web server.

This is achieved using the following settings:

- Server address – The name of the machine to forward all received requests too. If the SSL proxy and Web server are located on the same machine then Localhost may be used.

- Server port – The port number of the socket used by the Web server.

Chapter 8

SMTP Proxy Configuration

As part of the SMTP Proxy configuration various S/MIME Settings determine how iPlanet Trustbase Transaction Manager will accept mail based requests as well as the format of the responses. For example: Whether messages should be encrypted or not, or how responses should be signed.

S/MIME Settings

The file <install_directory>/Trustbase/TTM/<machine_name>/tbase.properties contains a number of S/MIME settings that are now discussed:

```
[SmimeServlet]
mail.smtp.host=smtphost.smime.com
mail.from=ttm@smime.com
loopback=false
debug=false
smime.capability.store.impl=com.iplanet.trustbase.security.smime.SimpleS
mimeCapabilityStore
smime.mode=SIGN:ENVELOPE
smime.permit.unencrypted=true
smime.signing.cert=TTMEMAIL
smime.encryption.alg=3DES/CBC/PKCS5
```

- SMTP server. The hostname of your outgoing mail server.

```
mail.smtp.host=smtphost.smime.com
```

- Default From address. This should match the email address in the Distinguished Name (DN) of the default signing certificate.

```
mail.from=ttm@smime.com
```

- Loopback test mode. This setting is for diagnostic purposes and is not normally used.

```
loopback=false
```

- Debug test mode. This setting is for diagnostic purposes and is not normally used.

```
debug=false
```

- This setting for internal use by iPlanet Trustbase Transaction Manager and should not normally be changed.

```
smime.capability.store.impl=com.iplanet.trustbase.security.smime.SimpleS
mimeCapabilityStore
```

- The S/MIME mode parameter takes the form:

MODE ::= [PROT][:PROT]*

PROT ::= SIGN[,KEY] | CLEAR_SIGN[,KEY] | ENVELOPE[,CIPHER]

- S/MIME mode parameter. This parameter is concerned with the outgoing response messages. If an email is signed using the SIGN parameter then if the signature does not verify, the message content cannot be read. However if the CLEAR_SIGN parameter is used then even if the signature does not verify, the content can still be read. The ENVELOPE parameter indicates that the outgoing Trustbase response message will be encrypted.

```
smime.mode=SIGN:ENVELOPE
```

- Allow unencrypted requests. If true, and an ENVELOPE protection has been requested, but there is no key for the recipient, then the message will be sent unencrypted. If false, the message will not be sent.

```
smime.permit.unencrypted=true
```

- S/MIME purpose attribute. This attribute should be assigned to the certificate that will sign and encrypt outgoing responses. To assign an attribute to a certificate in the iPlanet Trustbase Transaction Manager store see section on Assigning Attributes to Certificates on page 43.

```
smime.signing.cert=TTMEMAIL
```

- The default encryption algorithm for outgoing S/MIME responses.

```
smime.encryption.alg=3DES/CBC/PKCS5
```

Chapter 9

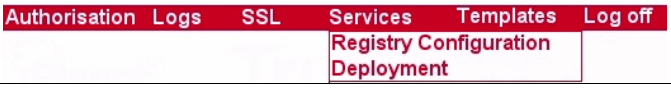
Service Deployment

Services that involve message interaction between one machine and another can be deployed by configuring them in terms of their class files that determine message protocol, the java code that defines the service itself together with some rulesets that define various authorisation mechanisms and a “tbasesvc.properties” file that allows the user to define configuration options for that particular service.

Overview of Deploying a Service

Deploying a service can involve any number of configuration features depending on what kind of service you have to build. Sometimes it may involve defining your own configuration options and in such circumstances you may wish to configure a Template option. In other cases you may require authenticating that service in which case you will have to select your Authorisation options.

Figure 57 Service Main Menu



There are essentially two main requirements for deploying a service:

- You deploy it by loading the services jar file into iPlanet™ Trustbase Transaction Manager.
- You then assign a role to authenticate the service, if necessary.

Note Developing a service prior to deploying it involves a number of steps.

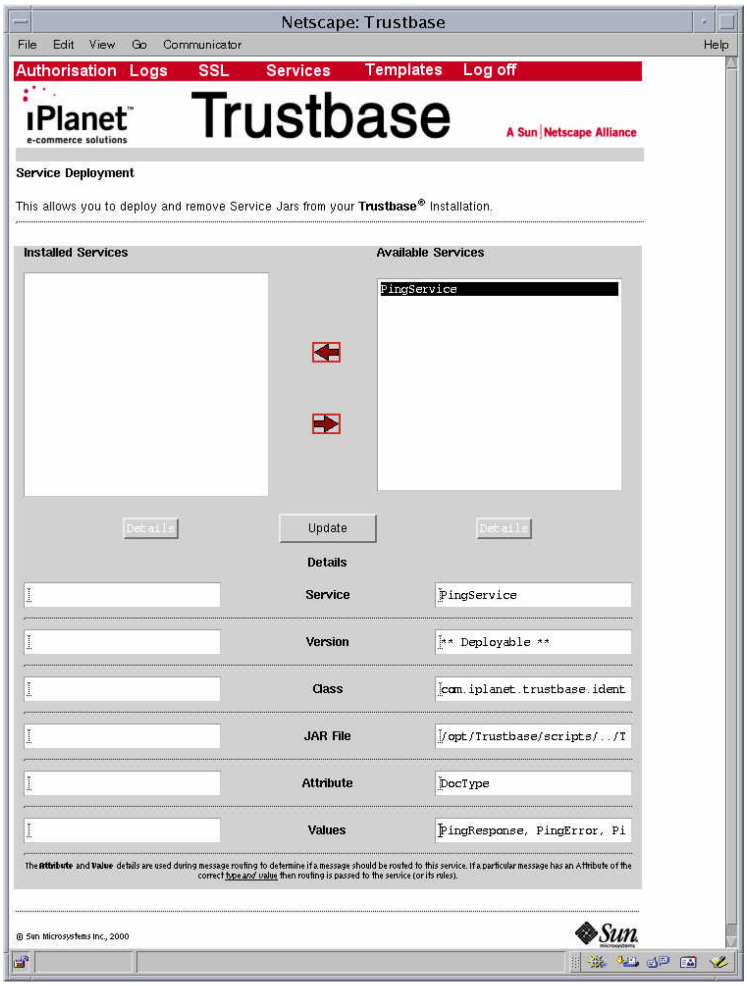
1. Create your DTD definitions that specify the syntactic structure of the messages you wish to send round the system. These DTD's are thrown away once the class files are generated and messages are interpreted from the class files themselves. This has two main benefits: (a) its faster (b) its easier to develop.
2. Use Classgen com.iplanet.trustbase.app.classgen.ClassGen to generate your java classes from your DTD definitions.
3. Write the Java code for the service deploying the Identrus API that assists the Identrus processing and validating of messages, certificates, keys and digital signatures.
4. Deploy the service within iPlanet™ Trustbase Transaction Manager by selecting the relevant configuration options as described below in this guide.
5. Finally, once it has been deployed within iPlanet™ Trustbase Transaction Manager itself you can run your service.

See the Developer Guide for more information on this.

Deploying

- You deploy it by selecting <Services><Deployment>

Figure 58 Service Deployment



Netscape: Trustbase
File Edit View Go Communicator Help
Authorisation Logs SSL Services Templates Log off
iPlanet™ e-commerce solutions
Trustbase
A Sun | Netscape Alliance
Installed Services
Available Services
PingService
Details
Update
Details
Sun microsystems

Service Deployment

This allows you to deploy and remove Service Jars from your **Trustbase**® Installation.

Details

	Service	PingService
	Version	** Deployable **
	Class	com.iplanet.trustbase.ident
	JAR File	/opt/Trustbase/scripts/../T
	Attribute	DocType
	Values	PingResponse, PingError, Pi

The **Attribute** and **Value** details are used during message routing to determine if a message should be routed to this service. If a particular message has an Attribute of the correct type and value then routing is passed to the service (or its rules).

© Sun Microsystems Inc., 2000

- The attribute and value details are used during message routing to determine if a message should be routed to this service. If a particular message has an attribute of the correct type and value then routing is passed to the service (or its corresponding rules).

- The Service is the service name

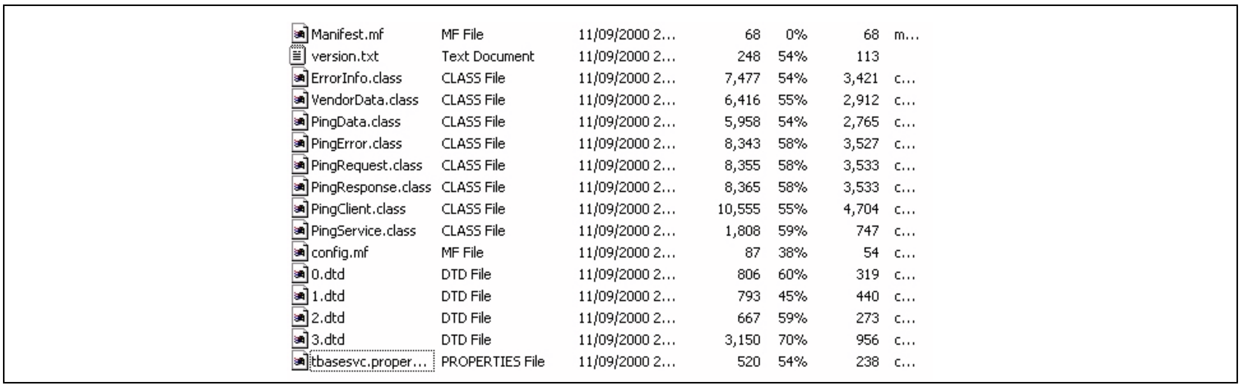
- The Version is the version of the service that is user defined

- The class is the main calling program

- The jar file that contains the service itself with all its associated data.

The service itself contains a jar file, placed in /opt/Trustbase/TTM/V2.2/deploy that has a list of classes that contain the java code associated with the service, the java code that defines the service and a .properties file that defines how the service should be configured. This is illustrated below.

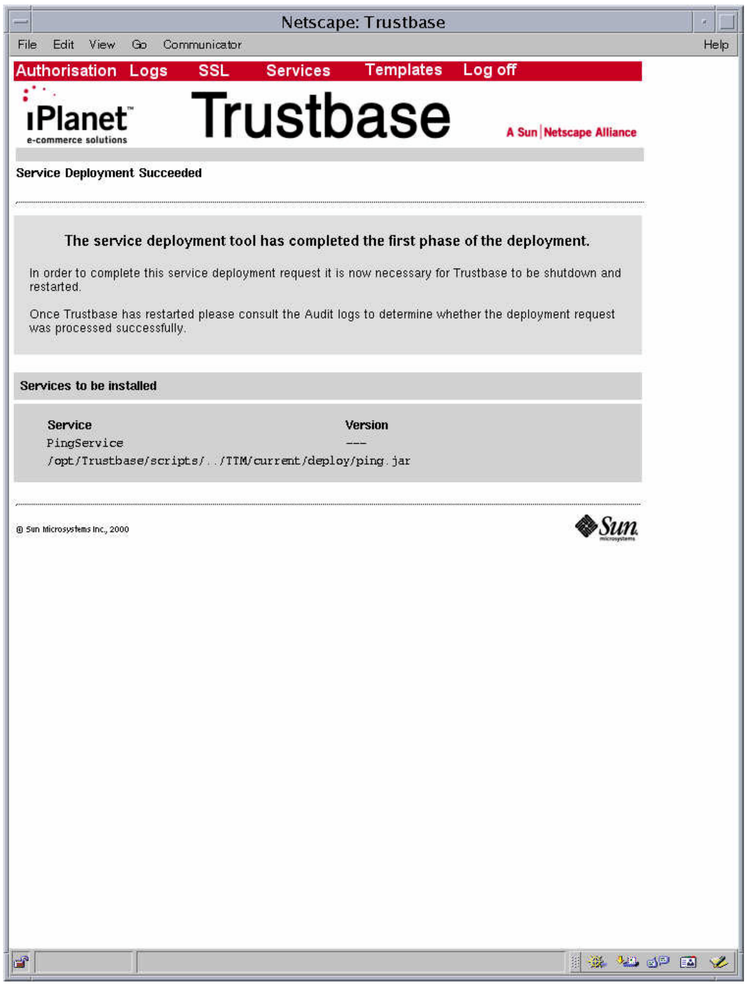
Figure 59 Example jar file of service being deployed



Manifest.mf	MF File	11/09/2000 2...	68	0%	68	m...
version.txt	Text Document	11/09/2000 2...	248	54%	113	
ErrorInfo.class	CLASS File	11/09/2000 2...	7,477	54%	3,421	c...
VendorData.class	CLASS File	11/09/2000 2...	6,416	55%	2,912	c...
PingData.class	CLASS File	11/09/2000 2...	5,958	54%	2,765	c...
PingError.class	CLASS File	11/09/2000 2...	8,343	58%	3,527	c...
PingRequest.class	CLASS File	11/09/2000 2...	8,355	58%	3,533	c...
PingResponse.class	CLASS File	11/09/2000 2...	8,365	58%	3,533	c...
PingClient.class	CLASS File	11/09/2000 2...	10,555	55%	4,704	c...
PingService.class	CLASS File	11/09/2000 2...	1,808	59%	747	c...
config.mf	MF File	11/09/2000 2...	87	38%	54	c...
0.dtd	DTD File	11/09/2000 2...	806	60%	319	c...
1.dtd	DTD File	11/09/2000 2...	793	45%	440	c...
2.dtd	DTD File	11/09/2000 2...	667	59%	273	c...
3.dtd	DTD File	11/09/2000 2...	3,150	70%	956	c...
tbasesvc.proper...	PROPERTIES File	11/09/2000 2...	520	54%	238	c...

- The figure below illustrates a sample output from deploying a service. The effects of deploying a service only occur when iPlanet™ Trustbase Transaction Manager has been restarted.

Figure 60 Service Deployment Results


Netscape: Trustbase
File Edit View Go Communicator Help
Authorisation Logs SSL Services Templates Log off
iPlanet™ e-commerce solutions
Trustbase
A Sun | Netscape Alliance

Service Deployment Succeeded

The service deployment tool has completed the first phase of the deployment.

In order to complete this service deployment request it is now necessary for Trustbase to be shutdown and restarted.

Once Trustbase has restarted please consult the Audit logs to determine whether the deployment request was processed successfully.

Services to be installed

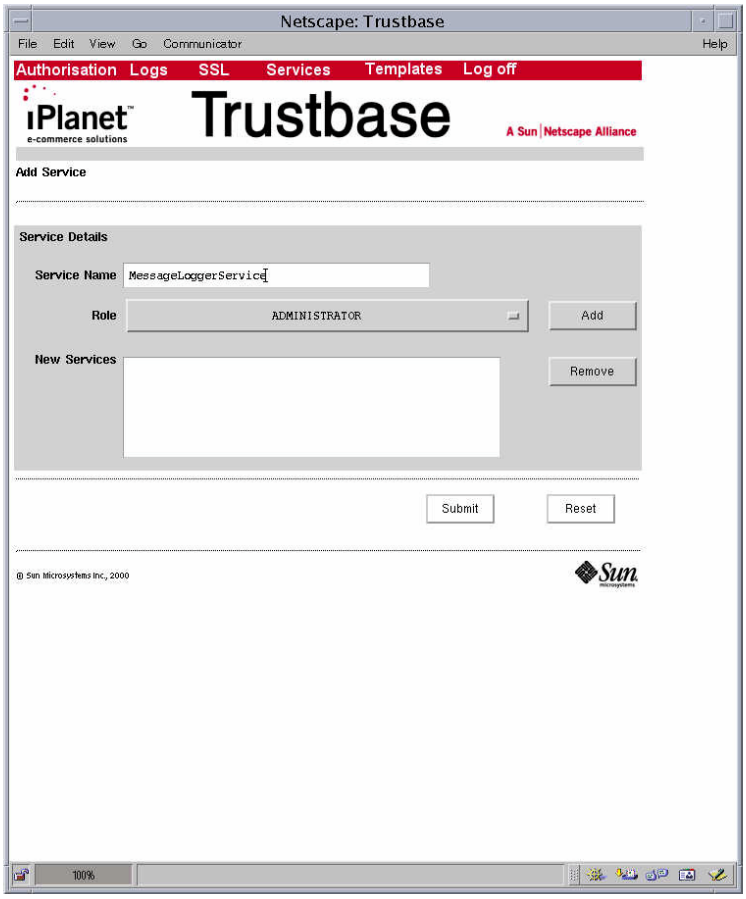
Service	Version
PingService /opt/Trustbase/scripts/../TTM/current/deploy/ping.jar	---

Authorisation Services

If it requires Authorisation you'll need to:

- Add the service by selecting <Add Service>

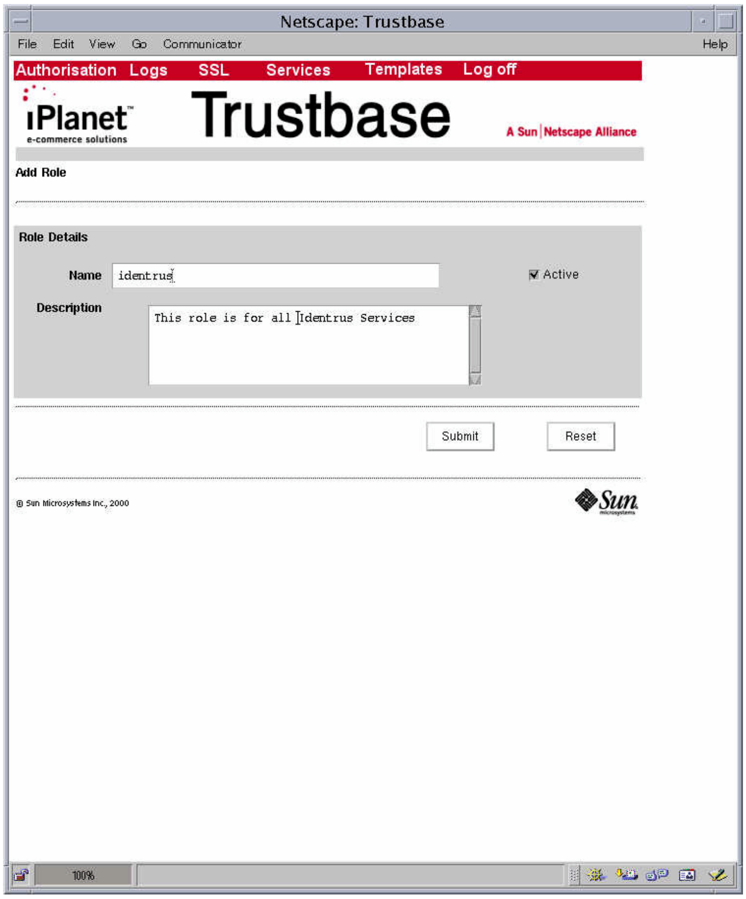
Figure 61 Add Service


Netscape: Trustbase
File Edit View Go Communicator Help
Authorisation Logs SSL Services Templates Log off
iPlanet e-commerce solutions
Trustbase
A Sun | Netscape Alliance
Add Service
Service Details
Add
Remove
Submit
Reset
© Sun Microsystems Inc, 2000
Sun microsystems
100%

Service Name: MessageLoggerService
Role: ADMINISTRATOR
New Services:

- Create a new role for this service by selecting <Add Role>

Figure 62 Add Role


Netscape: Trustbase
File Edit View Go Communicator Help
Authorisation Logs SSL Services Templates Log off
iPlanet™ e-commerce solutions
Trustbase
A Sun|Netscape Alliance
Submit
Reset
100%

Add Role

Role Details

Name: identrus

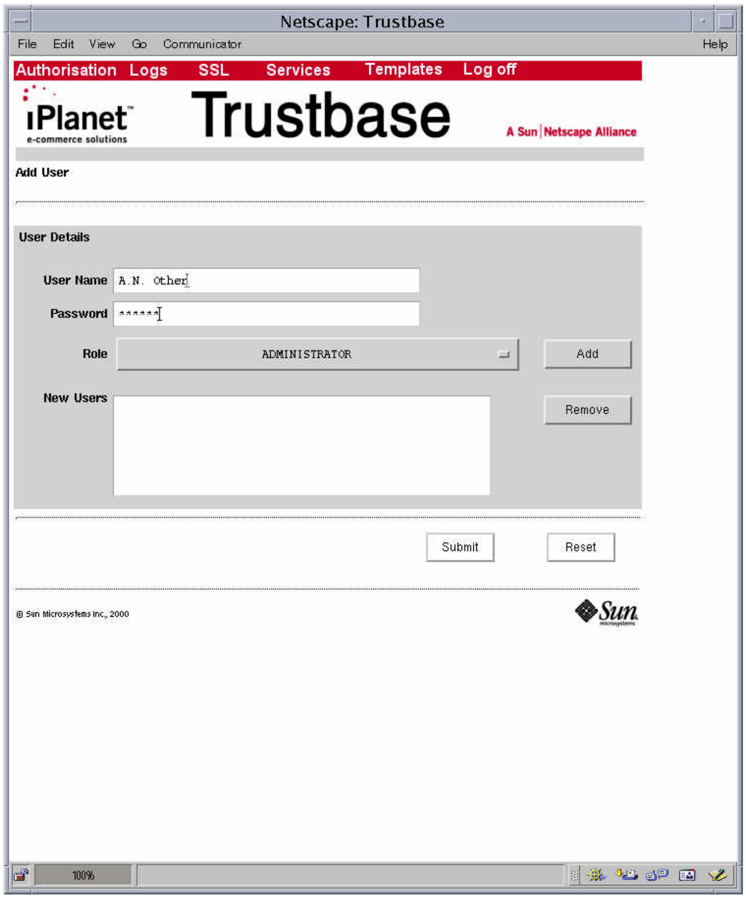
☑ Active

Description: This role is for all Identrus Services

© Sun Microsystems Inc., 2000

- Define some users for this role

Figure 63 Add User


Netscape: Trustbase
File Edit View Go Communicator Help
Authorisation Logs SSL Services Templates Log off
iPlanet e-commerce solutions
Trustbase
A Sun|Netscape Alliance
Add
Remove
Submit
Reset
© Sun Microsystems Inc., 2000
Sun microsystems
100%

Add User

User Details

User Name A.N. Other

Password ******

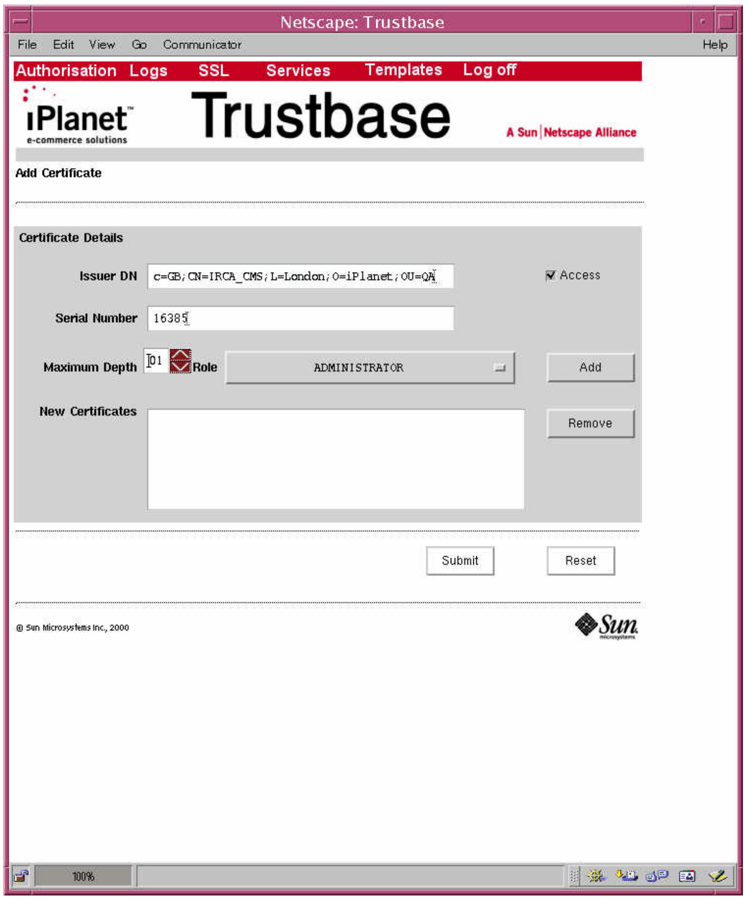
Role ADMINISTRATOR

New Users

- Make sure you select <Add> once you've allocated a role to a user
- Select <Submit>

- Add Certificate and associated Role

Figure 64 Add Certificate



Netscape: Trustbase
File Edit View Go Communicator Help
Authorisation Logs SSL Services Templates Log off
iPlanet e-commerce solutions
Trustbase
A Sun|Netscape Alliance

Add Certificate

Certificate Details

Issuer DN: c=GB;CN=IRCA_CMS;L=London;O=iPlanet;OU=QA

☑ Access

Serial Number: 16385

Maximum Depth: 01

Role: ADMINISTRATOR

New Certificates:

Add
Remove
Submit
Reset
© Sun Microsystems Inc, 2000
Sun microsystems
100%

- Make sure you select <Add> once you’ve allocated a role to a user
- Select <Submit>

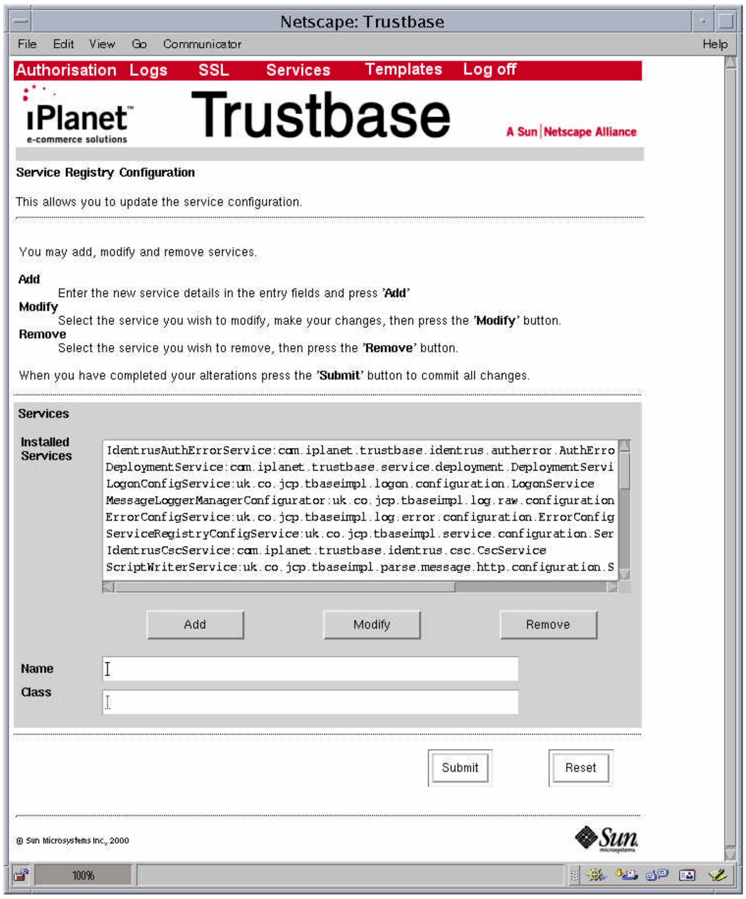
Services not requiring Authorisation

If the service you wish to deploy does not require authorisation simply select the <services> <deployment> and don’t follow the procedure to assign a role for the service.

Registered Services

Finally, you can see which services have been deployed by selecting <Services> <Service Registry> as illustrated below.

Figure 65 Service Registry


Netscape: Trustbase
File Edit View Go Communicator Help
Authorisation Logs SSL Services Templates Log off
iPlanet™ e-commerce solutions
Trustbase
A Sun|Netscape Alliance
Add
Modify
Remove
Submit
Reset
© Sun Microsystems Inc., 2000
Sun microsystems
100%

Service Registry Configuration

This allows you to update the service configuration.

You may add, modify and remove services.

Add
Enter the new service details in the entry fields and press '**Add**'

Modify
Select the service you wish to modify, make your changes, then press the '**Modify**' button.

Remove
Select the service you wish to remove, then press the '**Remove**' button.

When you have completed your alterations press the '**Submit**' button to commit all changes.

Services

Installed Services

```
IdentrusAuthErrorService:com.iplanet.trustbase.identrus.autherror.AuthErro
DeploymentService:com.iplanet.trustbase.service.deployment.DeploymentServi
LogonConfigService:uk.co.jcp.tbaseimpl.logon.configuration.LogonService
MessageLoggerManagerConfigurator:uk.co.jcp.tbaseimpl.log.raw.configuration
ErrorConfigService:uk.co.jcp.tbaseimpl.log.error.configuration.ErrorConfig
ServiceRegistryConfigService:uk.co.jcp.tbaseimpl.service.configuration.Ser
IdentrusCscService:com.iplanet.trustbase.identrus.csc.CscService
ScriptWriterService:uk.co.jcp.tbaseimpl.parse.message.http.configuration.S
```

Name

Class

Chapter 10

Templates

Templates allows you to deploy HTML based responses that are sent to the screen populated with data values that have been filled into the HTML page itself.

Under normal circumstances these should not need to be changed. However if you are deploying a new service that requires sending a message to the Trustbase screen you will need to deploy a template in this configuration screen.

Figure 66 Template Main Menu

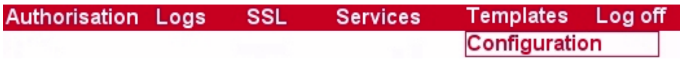
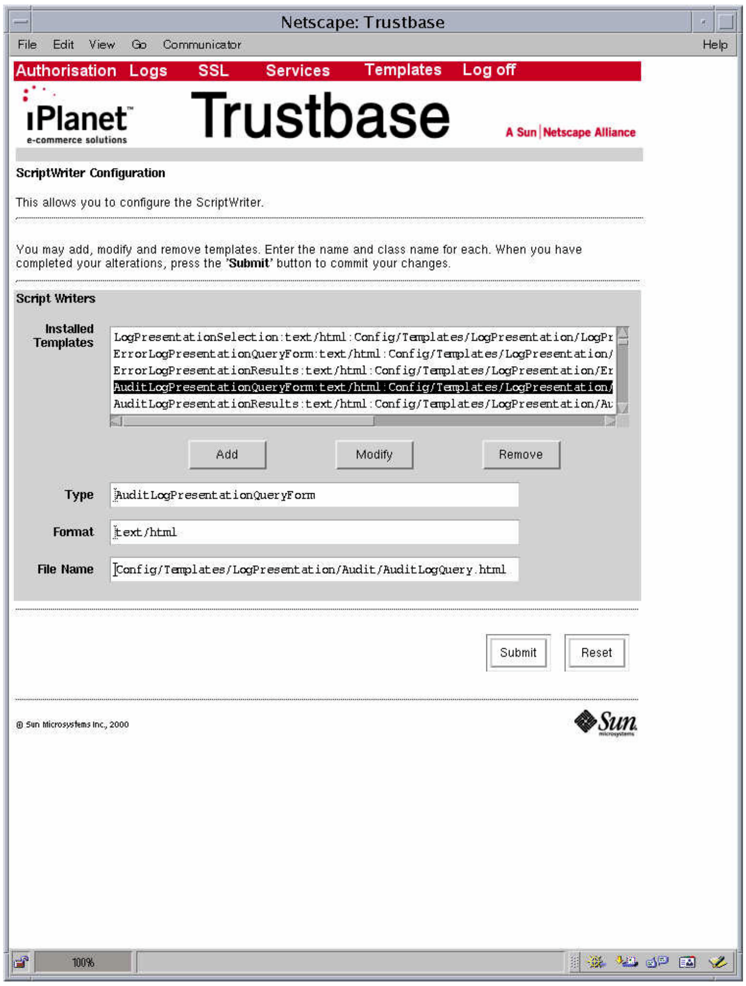


Figure 67 Template Configuration


Netscape: Trustbase
File Edit View Go Communicator Help
Authorisation Logs SSL Services Templates Log off
iPlanet e-commerce solutions
Trustbase
A Sun | Netscape Alliance

ScriptWriter Configuration

This allows you to configure the ScriptWriter.

You may add, modify and remove templates. Enter the name and class name for each. When you have completed your alterations, press the '**Submit**' button to commit your changes.

Script Writers

Installed Templates

```
LogPresentationSelection:text/html:Config/Templates/LogPresentation/LogPr
ErrorLogPresentationQueryForm:text/html:Config/Templates/LogPresentation/
ErrorLogPresentationResults:text/html:Config/Templates/LogPresentation/Er
AuditLogPresentationQueryForm:text/html:Config/Templates/LogPresentation/
AuditLogPresentationResults:text/html:Config/Templates/LogPresentation/Au
```

Type AuditLogPresentationQueryForm

Format text/html

File Name Config/Templates/LogPresentation/Audit/AuditLogQuery.html

Chapter 11

Backup

The objectives of this chapter are to cover

- What data needs backup?
- How do I recover disk space using archiving.
- How to do weekly and daily backups.
- What to do when certificates expire.
- How to recover from a System crash or disaster.

What data needs backup?

The database tables employed by the iPlanet™ Trustbase Transaction Manager fall into two groups:

- Those that are to all intents and purposes read-only (e.g. configuration information)
- Those that are used to store large volumes of frequently written data (e.g. raw log)

This next section describes the function and composition of the tables used, so that the database administrator may more accurately devise an archiving strategy.

What data is Read-Only?

The following tables are largely used for static read-only data. These tables are not expected to grow to large sizes, so archiving should not be required, and all data can be kept online. However these tables should be backed up initially after configuration and after any subsequent certificate or configuration changes for backup and disaster recovery purposes.

- Tables comprising the certificate store. All these tables are modified only when items are added to the store, which is an infrequent occurrence.
    - ATTRIBUTE_KEY_ATTRS. Used to store the attributes associated with key pairs.
    - ATTRIBUTE_NAME_ATTRS Used to store the attributes associated with certificates
    - CERT_TABLE Used to store X509 certificates
    - KEY_TABLE Used to store cryptographic key pairs
    - REVOCATION_ATTRS Used to store the attributes associated with Certificate Revocation Lists (CRLs)
    - REVOCATION_SERIAL_NUM Used to index the serial numbers of certificates revoked in CRLs
    - REVOCATION_TABLE Used to store encoded X509 CRLs.
    - SALT_TABLE Holds the salt value for the password-based authentication used in the database. This table never exceeds one entry.
- Identrus
    - CERT_DATA All unique certificates from Identrus Messaging
    - BILL_DATA Billing Records for processed Identrus Messaging

- Other tables

    - AUTHORISATION Maps role names to service names

    - CERTIFICATEAUTHENTICATION Maps certificate details to roles

    - CONFIG Used to store configuration data for the system. Each system element has one row in this table, so the table will only grow when new system elements are added.

    - ROLES Stores information about roles

    - USERNAMEPASSWORDAUTH Maps username / password combinations to roles

- The initialisation files *.properties and proxi.ini that can be found in /opt/Trustbase/TTM/<machine-name>

- When utilising an HSM such as nCipher, module keys. nCipher "Security World" allows module keys to be backed. Consult the KeySafe User Guide using the Administrator Card Set.

What Tables are used for frequently written data?

The following tables are written frequently and can be expected to grow rapidly. Therefore it will be necessary to archive data from these tables as storage limits are approached. These logs contain important information that mean it is imperative to avoid loss. A regular back-up process should be in force for the following tables:

- Frequently Written Data
  - AUDITDATA Stores audit log data
  - ERROR Stores error log data
  - RAW_DATA stores all the raw message data entering an leaving the system. This table is used for non-repudiation purposes, and is referenced by the INIT_TABLE described below. Due to this link, the archiving procedure for both these tables should follow that described above.

```
SQL> desc raw_data;
 Name                            Null?    Type
 ------------------------------- -------- ----
 SESSIONID                       NOT NULL NUMBER(38)
 LOGCONNECTIONID                 NOT NULL NUMBER(38)
 RECORDID                        NOT NULL NUMBER(38)
 MSGGRPID                                 VARCHAR2(120)
 MSGID                                    VARCHAR2(120)
 DOCTYPE                         NOT NULL VARCHAR2(120)
 RECORDMARKER                    NOT NULL VARCHAR2(240)
 CONNECTIONID                    NOT NULL VARCHAR2(100)
 PROTOCOLTYPE                    NOT NULL VARCHAR2(10)
 INPUT                           NOT NULL NUMBER(38)
 TIMESTAMP                       NOT NULL NUMBER(38)
 RAWDATA                         NOT NULL LONG
 DIGESTOFRECORD                           RAW(2000)
 SIGNEDDIGESTOFCALCULATION                RAW(2000)
```

  - INIT_TABLE Stores information relating to the integrity of the raw log tables.

```
SQL> desc init_table;
 Name                            Null?    Type
 ------------------------------- -------- ----
 SESSIONID                       NOT NULL NUMBER(38)
 TIMESTAMP                       NOT NULL NUMBER(38)
 N_CONNECTIONS                   NOT NULL NUMBER(38)
 SIGDATA                         NOT NULL RAW(2000)
 SERVERCERTISSUERDN                       VARCHAR2(2000)
 SERVERCERTSERIALNUMBER                   VARCHAR2(100)
```

Archiving for Raw Data and Init Table

For Identrus, the log init_table and raw_data table are inter linked. A raw_data record holds actual message data along with a time stamp that is digitally signed. An init_table record points to the beginning of a set of raw_data records. There are two circumstances under which archiving may take place:

1. **The TTM instance is not running**. In this case, the data in both raw_data and init_table tables may be archived using the prevailing archive strategy. Note that both tables should be archived in order to ensure that verification of the archived data operated correctly. When the system is re-started, a new initialisation record will be created in the init_table, and raw_data entries will be cryptographically chained from this.
2. **The TTM instance *is* running**. In this case, the raw log verification utility should be run, in order to provide a list of the log end-points. This will give output of the form:

The script can be run as follows:

```
$ cd <TrustbaseInstallDir>/TTM/Scripts
$ ./runcheckintegrity
```

the following output appears

```
Trustbase Raw Log Verification Utility
Checking all sessions
Checked chain 0 from session 4,160 with 82 records, ending at 26/02/01
19:41. Endpoint in chain is 81
Checked chain 1 from session 4,160 with 81 records, ending at 26/02/01
19:41. Endpoint in chain is 80
Checked chain 2 from session 4,160 with 81 records, ending at 26/02/01
19:41. Endpoint in chain is 80
Checked chain 3 from session 4,160 with 75 records, ending at 26/02/01
19:41. Endpoint in chain is 74
Checked chain 4 from session 4,160 with 87 records, ending at 26/02/01
19:41. Endpoint in chain is 86
Checked chain 5 from session 4,160 with 85 records, ending at 26/02/01
19:41. Endpoint in chain is 84
Checked chain 6 from session 4,160 with 81 records, ending at 26/02/01
19:41. Endpoint in chain is 80
Checked chain 7 from session 4,160 with 77 records, ending at 26/02/01
19:41. Endpoint in chain is 76
Checked chain 8 from session 4,160 with 82 records, ending at 26/02/01
19:41. Endpoint in chain is 81
Checked chain 9 from session 4,160 with 79 records, ending at 26/02/01
19:41. Endpoint in chain is 78
Checked session 4,160 with total 810 records over 10 connections.
Started at 26/02/01 19:39 Ended at 26/02/01 19:41
```

Note Before running the script you need to check the entries ([LogManager/MessageLoggerStore] and [LogManager/MessageLogger]) in tbase.properties. The database connection string, user, password and driver settings are read from this file. Also the signing certificate for the raw log records and signature algorithm are read from this file. The following is an example

The following is an example <install_directory/TTM/Scripts/runcheckintegrity script:

```
. ./setcp
CLASSPATH=$TBASE_INSTALL:$CLASSPATH
cd $TBASE_INSTALL
exec java uk.co.jcp.tbaseimpl.log.raw.tools.VerUtil
```

Each Session holds a collection of chains, each containing a start point and an end point. All data up to these end points may now be archived. Future runs of the raw log verification utility, when an archive has taken place, will report data written subsequently as “orphan” data, but will verify and report on the data. Output will be similar to that below:

```
$ ./runcheckintegrity
```

the following output appears

```
Trustbase Raw Log Verification Utility
Checking all sessions
No init records were found
Orphan chain from session 4,160, Connection 0, startpoint 10, endpoint
81 is valid
Orphan chain from session 4,160, Connection 1, startpoint 10, endpoint
80 is valid
Orphan chain from session 4,160, Connection 2, startpoint 10, endpoint
80 is valid
Orphan chain from session 4,160, Connection 3, startpoint 10, endpoint
74 is valid
Orphan chain from session 4,160, Connection 4, startpoint 10, endpoint
86 is valid
Orphan chain from session 4,160, Connection 5, startpoint 10, endpoint
84 is valid
Orphan chain from session 4,160, Connection 6, startpoint 10, endpoint
80 is valid
Orphan chain from session 4,160, Connection 7, startpoint 10, endpoint
76 is valid
Orphan chain from session 4,160, Connection 8, startpoint 10, endpoint
81 is valid
Orphan chain from session 4,160, Connection 9, startpoint 10, endpoint
76 is valid
Checked ORPHAN session 4,160 with total 710 records over 10 connections.
Started at 26/02/01 19:40 Ended at 26/02/01 19:41
```

RecordIds are declared valid when the signature of this record matches with the certificates held in the local database. If the recorded end points tally with the start points of the orphan data, the integrity of the log may be inferred. Provided the RecordId of subsequent verifications is less (and stated as valid) than its predecessor then integrity can be assumed. If this is not the case then either the archiving procedure has been mismanaged or somebody has deleted or tampered with some records. Under such circumstances you will need to go back and check the integrity of the archives. The fact that the second verification illustrated above shows only 710 records compared with 810 records in the first verification means that 100 records were archived between the two verification checks. Indeed all records within chains whose startpoints were less than 10 were archived.

By default the tool will check the integrity of all records in the raw log. An individual session can be checked with the command line switch

```
-session <Session Id>
```

For Example:

```
./runcheckintegrity -session 12344
```

What happens when certificates expire?

In the event of any certificate expiring, a complete new set of Transaction Co-ordinator certificates will need to be generated. Before you do this it is a good idea to archive the contents of the logs as this ensures the archived logs are only signed by one set of certificates. This can be done as part of the general backup.

Note	Please refer to the chapter on Certificate Management. The procedure for obtaining new certificates is identical to the procedure that you used to obtain them the first time.

How to do Disaster Recovery?

In the event of hardware or disk failure it will be necessary to perform a disaster recovery. By ensuring the following contents are intact through restoration from backup, a iPlanet™ Trustbase Transaction Manager can continue its operation.

- nCipher Users only. nCipher "Security World" needs to be restored according to the KeySafe User Guide using the Administrator Card Set and the nCipher backup data.
- Reinstall iPlanet™ Trustbase Transaction Manager, Application Server and database.
- Reinstate *.properties and proxi.ini found in /opt/Trustbase/TTM/<machine-name>
- Reinstate database from the backup of tables created under the user specified in the SQL script in your Installation Guide. If necessary consult your Database Administrator.

Note Refer to the installation worksheet for information about the setup of iPlanet™ Trustbase Transaction Manager's application server and database.

Chapter 12

Glossary and References

The objectives of this chapter are to cover

- Software Platform
- Protocol
- Glossary

Software Platform

Solaris 8 and JDK

http://www.sun.com/software/solaris/cover/sol8.html

Java

http://www.javasoft.com

iPlanet Application Server 4.1

http://www.iplanet.com/products/infrastructure/app_servers/index.html

iPlanet Web Server 6.0

http://www.iplanet.com/products/infrastructure/web_servers/index.html

Oracle 8i

http://www.oracle.com

Hardware Security nCipher KeySafe 1.0 and CAFast

http://www.ncipher.com

Transport Protocols

HTTP

HTTP/1.0 or 1.1 protocol:

http://www.w3.org/Protocols/rfc1945/rfc1945.txt

http://www.ietf.org/rfc/rfc1945.txt

SMTP RFC821

ftp://ftp.isi.edu/in-notes/rfc821.txt http://www.imc.org/ietf-smtp/

Security Related Protocols

S/MIME Version 2 Message Specification

ftp://ftp.isi.edu/in-notes/rfc2311.txt

http://www.imc.org/ietf-smime

http://www.ietf.org/rfc/rfc2311.txt

DOMHASH

http://www.ietf.org/rfc/rfc2803.txt

OCSP

http://www.ietf.org/rfc/rfc2560.txt

Certificate requests and responses

PKCS10 requests RFC2314 can be found in http://www.ietf.org/rfc.html

PKCS7 responses RFC2315 can be found in http://www.ietf.org/rfc.html

Trading Protocols

Identrus

http://www.identrus.com

Transaction Coordinator requirements (IT-TCFUNC)

Core messaging specification (IT-TCMPD)

Certificate Status Check Messaging specification (IT-TCCSC)

Message Protocols

DOM

http://www.w3.org/TR/REC-DOM-Level-1/

DTD

http://www.w3.org/XML/1998/06/xmlspec-v20.dtd

XML

http://www.w3.org/TR/REC-xml

XML Syntax Processing specification

http://www.w3.org/TR/xmldsig-core

HTML

HTML 3.2 as specified in http://www.w3.org/TR/REC-html32.html

Glossary

AIA Authority Information Access

Application protocol. An application protocol is a protocol that normally layers directly on top of the transport layer (e.g., TCP/IP). Examples include HTTP, TELNET, FTP, and SMTP.

ASN.1. Abstract Syntax Notation One.

Authentication. Authentication is the ability of one entity to determine the identity of another entity. i.e. in the case of NetMail Lite, you know who your email message came from.

base64. A representation of characters in digital format using a 65 character subset of U.S. ASCII.

BBS. A random number generating algorithm.

BER. Basic encoding Rules used with X509.

Block cipher. A block cipher is an algorithm that operates on plaintext in groups of bits, called blocks. 64 bits is a typical block size.

Bulk cipher. A symmetric encryption algorithm used to encrypt large quantities of data.

CA Certificate Authority

Cipher Block Chaining Mode (CBC). CBC is a mode in which every plaintext block encrypted with the block cipher is first eXclusive-OR-ed with the previous ciphertext block (or, in the case of the first block, with the initialisation vector).

Certificate. As part of the X.509 protocol (a.k.a. ISO Authentication framework), certificates are assigned by a trusted Certificate Authority and provide verification of a party's identity and may also supply its public key.

Certificate Authority. An organisation authorised to issue certificates (as in CA).

Client. The application entity that initiates a connection to a server.

CN Common Name See for instance http://www.itu.int/itudoc/itu-t/rec/x/x500up/x500.html for definition or http://docs.iplanet.com/docs/manuals/directory/schema/contents.htm

Connection. A connection is a transport (in the OSI layering model definition) that provides a suitable type of service. For SSL, such connections are peer to peer relationships. The connections are transient. Every connection is associated with one session.

CRL Certificate Revocation List. A list of certificates that have been declared invalid by their issuing CA before their expiry dates

CSC Certificate Status Check

Data Encryption Standard (DES). DES is a very widely used symmetric encryption algorithm. DES is a block cipher.

3DES. Similar to DES.

DER. Distinguished Encoding rules used in X509.

DH. A public-key cryptographic algorithm for encrypting and decrypting data.

Digital Signature Standard (DSS). A standard for digital signing, including the Digital Signing Algorithm, approved by the National Institute of Standards and Technology, defined in NIST FIPS PUB 186, "Digital Signature Standard," published May, 1994 by the U.S. Dept. of Commerce.

Digital signatures. Digital signatures utilise public key cryptography and one-way hash functions to produce a signature of the data that can be authenticated, and is difficult to forge or repudiate.

DN Distinguished Name. See for instance http://www.itu.int/itudoc/itu-t/rec/x/x500up/x500.html or http://search.ietf.org/internet-drafts/draft-zeilenga-ldapv3bis-rfc2253-00.txt for definition. Also http://docs.iplanet.com/docs/manuals/directory/schema/contents.htm

DSA. Digital Signature Algorithm.

EE. End Entities are customers. i.e. the last person in the certificate chain.

Handshake. An initial negotiation between client and server that establishes the parameters of their transactions.

HSM Hardware Security Module.

HTML HyperText Markup Language.

IDEA. A 64-bit block cipher designed by Xuejia Lai and James Massey.

IRCA is the certificate for the Identrus root

Integrity i.e. You know your email message has not changed.

IP Issuing Participant Bank (or other financial institution) issuing smart cards containing private keys and certificates to Subscribing Customers.

IR Identrus Root

key. The key used to encrypt data written by the client.

LDAP Lightweight Directory Access Protocol

L1CA is the purpose ID or attribute for CA certificates

L1IPSC. The purpose ID or attribute of Certificate used for interbank message signing

L1EESSL. The purpose ID or attribute of Certificate used for bank/RC or bank/SC SSL connections - as server

L1EESC. The purpose ID or attribute of Certificate used for bank/RC or bank/SC message signing

Message Authentication Code (MAC). A Message Authentication Code is a one-way hash computed from a message and some secret data. Its purpose is to detect if the message has been altered.

MD5. MD5 is a secure hashing function that converts an arbitrarily long data stream into a digest of fixed size.

MIME. MultiPURPOSE Internet Mail Extension

Non-repudiation A process set up to ensure that the sender cannot disavow a message

OCSP Online Certificate Status Protocol

OU Organisation Unit See for instance http://www.itu.int/itudoc/itu-t/rec/x/x500up/x500.html or http://search.ietf.org/internet-drafts/draft-zeilenga-ldapv3bis-rfc2253-00.txt for definition or http://docs.iplanet.com/docs/manuals/directory/schema/contents.htm

PBE. Password based encryption

PEM. Privacy enhanced mail

Public Key Infrastructure (PKI). Defines protocols to support online interaction.

Public key cryptography. A class of cryptographic techniques employing two-key ciphers. Messages encrypted with the public key can only be decrypted with the associated private key. Conversely, messages signed with the private key can be verified with the public key.

OSI. Open Systems Inter-Connection.

RC2, RC4. Proprietary ciphers from RSA Data Security, Inc. RC2 is block cipher and RC4 is a stream cipher.

RC Relying Customer Party with whom the Subscribing Customer initiates a signed transaction.

RC Host Server software that performs the role of the RC in the Identrus certificate status check scheme. In the case of this document this is the portal server.

RC NetMail Lite or RC Mail. The client software interface that a customer uses to send and receive messages. In the case of this document this is NetMail Lite.

RP Relying Participant Bank with which the Relying Customer communicates to obtain some level of trust in the signed data received from the Subscribing Customer.

RSA. A very widely used public-key algorithm that can be used for either encryption or digital signing.

Server. The server is the application entity that responds to requests for connections from clients. The server is passive, waiting for requests from clients.

SC Subscribing Customer. Member of the Issuing Participant bank authorised to participate in Identrus activities.

Session. A SSL session is an association between a client and a server. Sessions are created by the handshake protocol. Sessions define a set of cryptographic security parameters, which can be shared among multiple connections. Sessions are used to avoid the expensive negotiation of new security parameters for each connection.

SmartCard A hardware token that incorporates one or more integrated circuit (IC) chips to implement cryptographic functions and that possesses some inherent resistance to tampering.

SHA. The Secure Hash Algorithm is defined in FIPS PUB 180-1. It produces a 20-byte output.

SSL. Secure sockets layer

Stub The java interface to support communication with the CAFast hard server

TC Transaction Co-ordinator

UTF8 A multi-byte character encoding format. See http://www.utf-8.org/

X509. An authentication framework based on ASN.1 BER and DER and base64.

Index