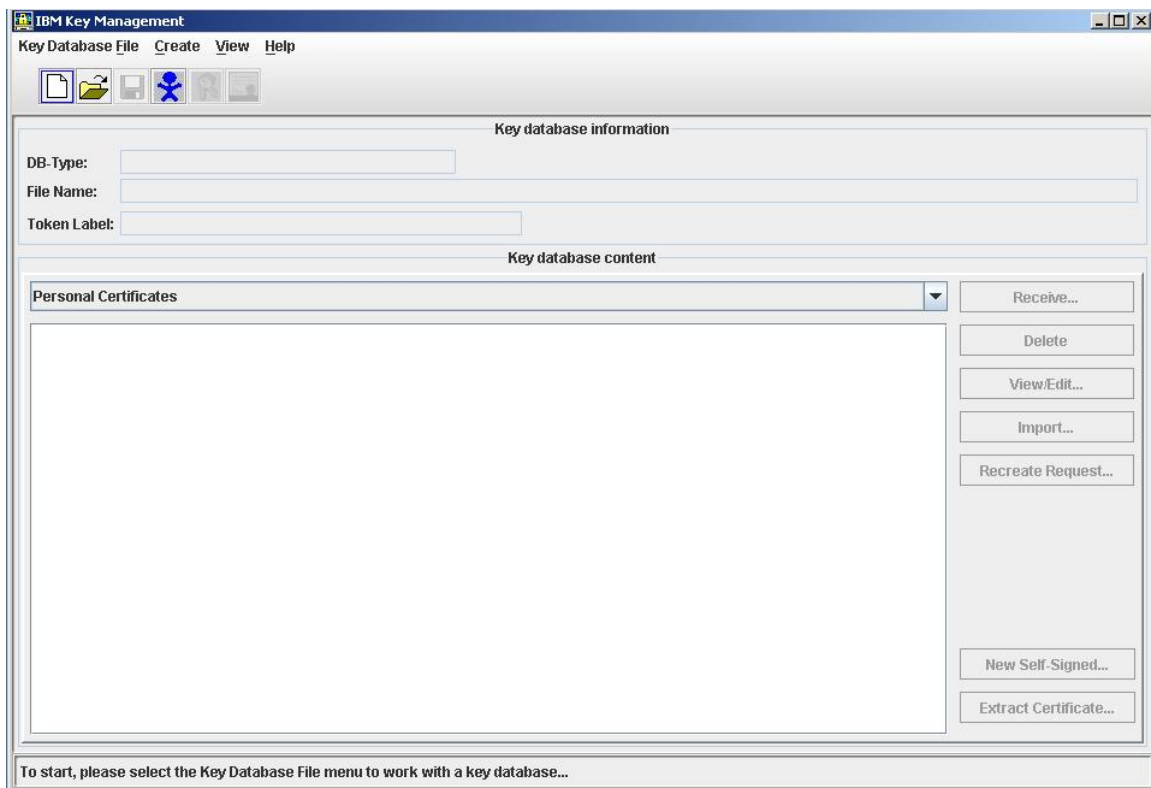


Configure IHS 6.1 with SSL and WebSphere Application Server 6.1

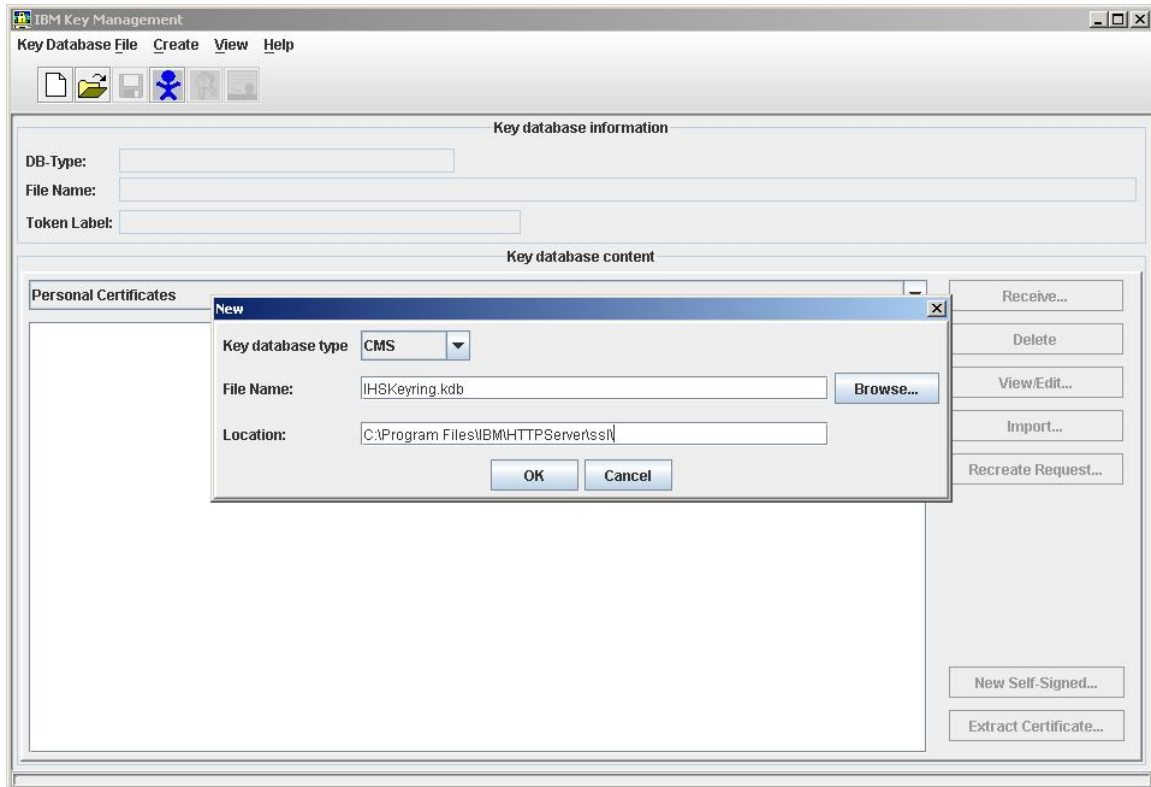
- 1) Create a new directory to hold the key ring.
 - a) Create the directory `<ihs_root>\ssl`.
- 2) Open iKeyman in `<ihs_root>\bin`
 - a) Bring up IHS's Ikeyman. This can be done through either a command-line window or using **Start —> Programs —> IBM HTTP Server 6.1 —> Start Key Management Utility**.
 - b) The command line can be executed from the `<ihs_root>\bin` directory:

ikeyman.bat

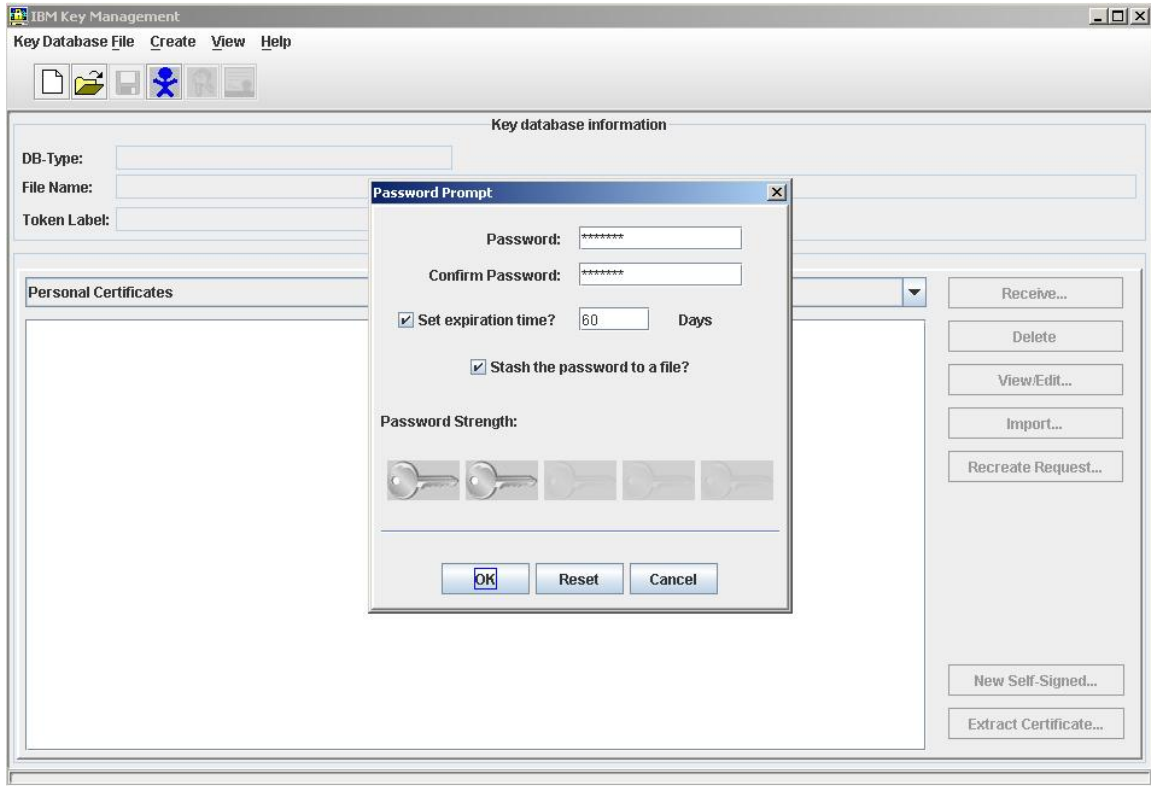


- 4) Create a key ring
 - a) Create a new key ring by selecting **Key Database File** —> **New**
 - b) Use type **CMS**, file name **ihSKeyring.kdb** and a location of **<ihS_root>\ssl**.

Click **OK**.

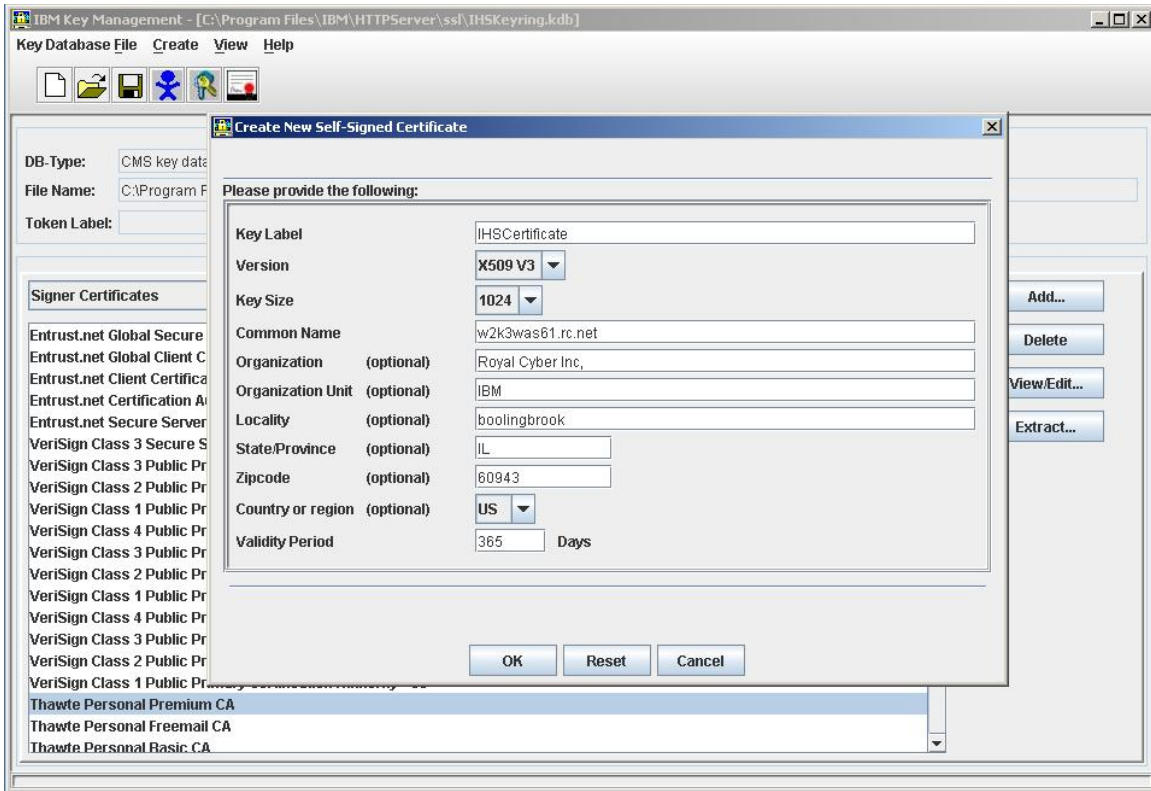


- 5) When prompted for a password for the key ring, enter and confirm was1edu as the password. If desired, modify the **expiration time**. Check the “**Stash the password to a file**” check box. Click OK and OK again for the informational box.

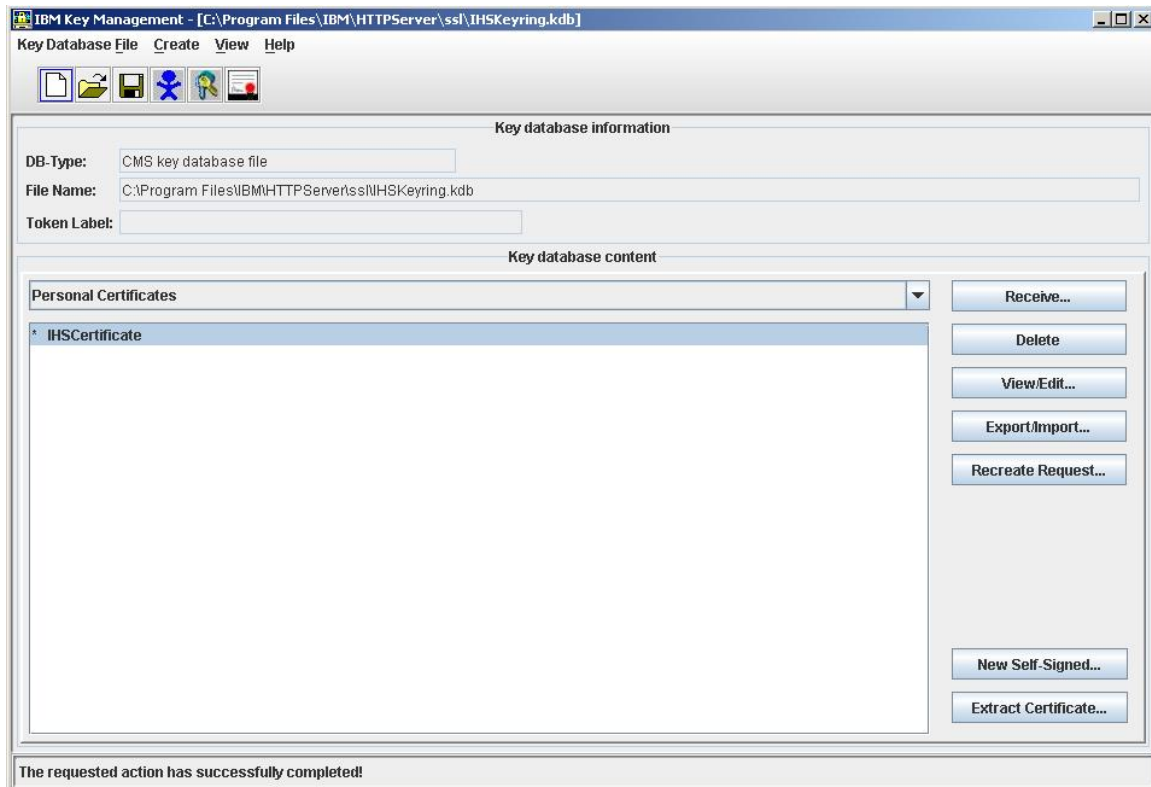


- 4) Create a new self-signed certificate.
 a) In Ikeyman, select **Create —> New Self-Signed Certificate** and enter

Example	Description
Key Label	IHSCertificate
Common Name	<domain_name>
Organization	Royal Cyber Inc.
Organization Unit	IBM WebSphere
Locality	bolingbrook
State/Province	IL
Zipcode	60563



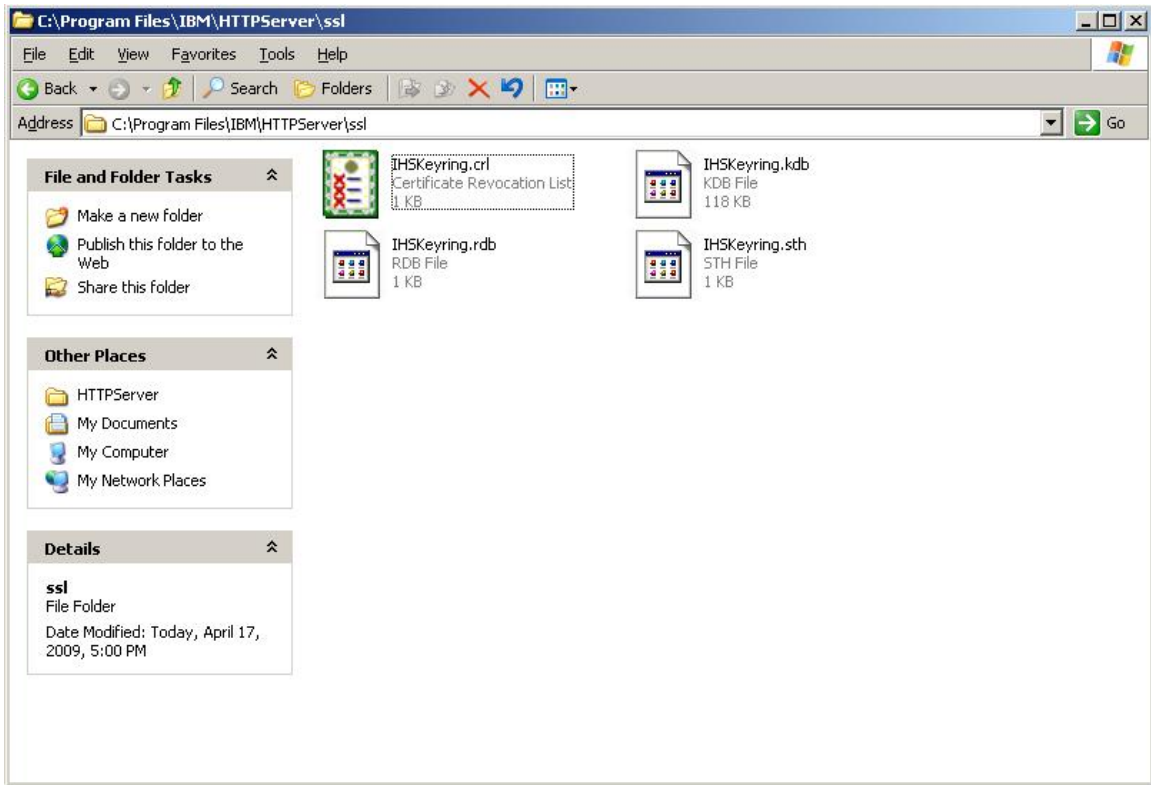
5) Click OK



6) Exit iKeyman

List the contents of the directory `<ihs_root>\ssl\` and verify that the following files were created:

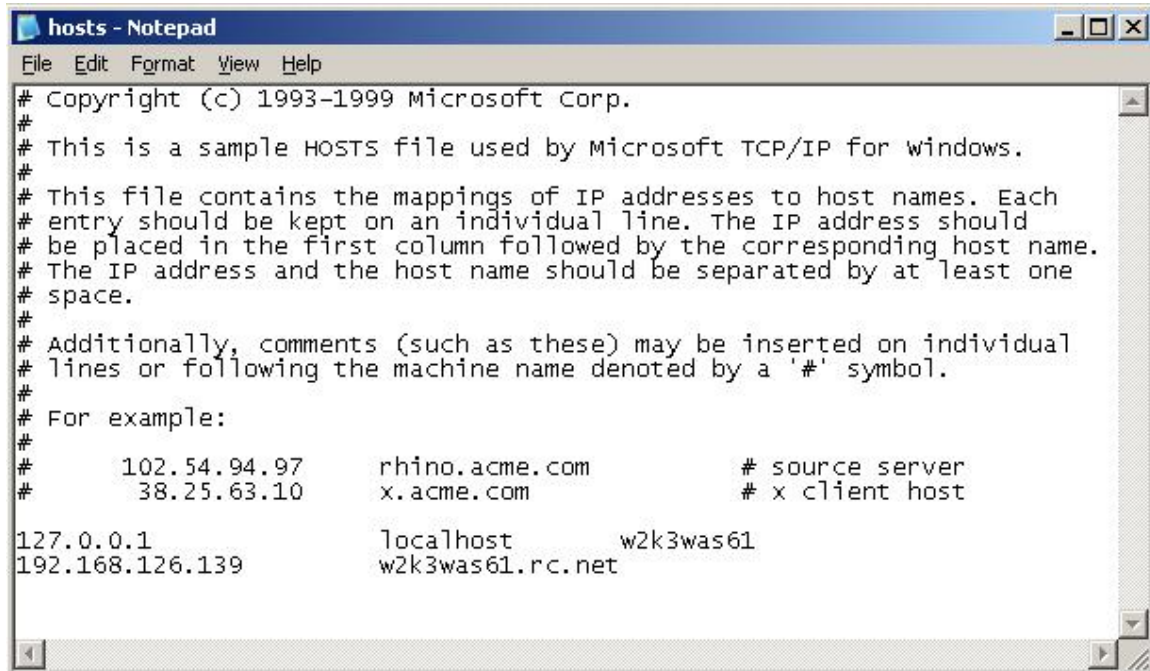
ihsKeyring.kdb
ihsKeyring.sth
ihsKeyring.crl
ihsKeyring.rdb



Configure a Virtual Host on IHS for HTTPS

This section of the document modifies the httpd.conf in order to define the required setting to enable SSL for IBM HTTP Server. This includes loading the SSL module, defining a listener port, defining a virtual host and enabling SSL.

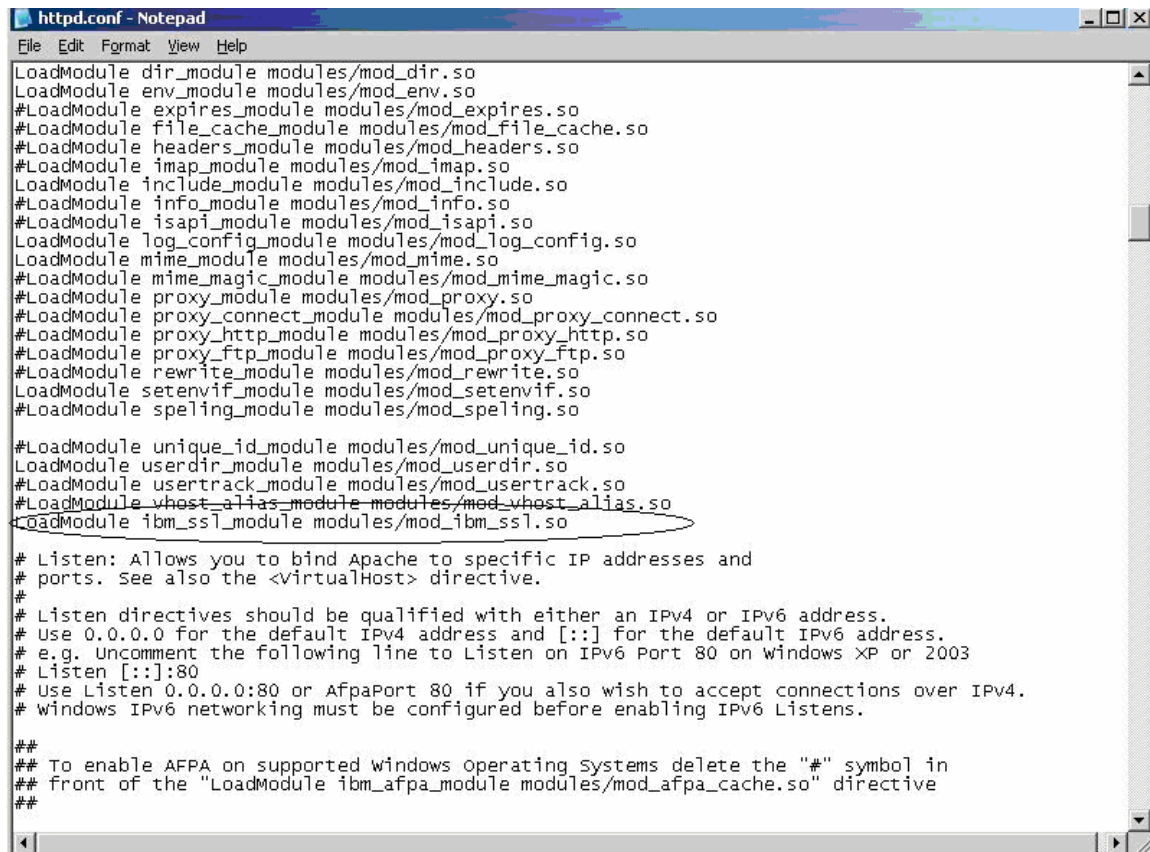
- 1) Add your domain name <domain_name> to hosts file.
 - a) Edit C:\Winnt\System32\Drivers\etc\hosts
 - b) Add a line at the bottom of the hosts file for <domain_name> in our case it w2k3was61.rc.net and use your system's IP address.



```
hosts - Notepad
File Edit Format View Help
# Copyright (c) 1993-1999 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#       102.54.94.97       rhino.acme.com           # source server
#       38.25.63.10      x.acme.com               # x client host
127.0.0.1                localhost                w2k3was61
192.168.126.139          w2k3was61.rc.net
```

- c) Save the file.
- 2) **Backup** the **httpd.conf**.
 - a) Since changes are about to be made to the httpd.conf, it would be a good idea to make a backup of it before starting. **Copy** the **httpd.conf** in **<ihs_root>\conf** to **httpd-backup.conf**.
- 3) Add Virtual Host definition for HTTPS. This allows for the definition of HTTPS on a separate virtual host from HTTP.
 - a) Edit the **httpd.conf** in **<ihs_root>\conf**.
 - b) Load the SSL module by adding the following line after where most of the other Load Modules are done:

LoadModule ibm_ssl_module modules/mod_ibm_ssl.so



```
httpd.conf - Notepad
File Edit Format View Help
LoadModule dir_module modules/mod_dir.so
LoadModule env_module modules/mod_env.so
#LoadModule expires_module modules/mod_expires.so
#LoadModule file_cache_module modules/mod_file_cache.so
#LoadModule headers_module modules/mod_headers.so
#LoadModule imap_module modules/mod_imap.so
LoadModule include_module modules/mod_include.so
#LoadModule info_module modules/mod_info.so
#LoadModule isapi_module modules/mod_isapi.so
LoadModule log_config_module modules/mod_log_config.so
LoadModule mime_module modules/mod_mime.so
#LoadModule mime_magic_module modules/mod_mime_magic.so
#LoadModule proxy_module modules/mod_proxy.so
#LoadModule proxy_connect_module modules/mod_proxy_connect.so
#LoadModule proxy_http_module modules/mod_proxy_http.so
#LoadModule proxy_ftp_module modules/mod_proxy_ftp.so
#LoadModule rewrite_module modules/mod_rewrite.so
LoadModule setenvif_module modules/mod_setenvif.so
#LoadModule spelling_module modules/mod_spelling.so

#LoadModule unique_id_module modules/mod_unique_id.so
LoadModule userdir_module modules/mod_userdir.so
#LoadModule usertrack_module modules/mod_usertrack.so
#LoadModule vhost_alias_module modules/mod_vhost_alias.so
LoadModule ibm_ssl_module modules/mod_ibm_ssl.so

# Listen: Allows you to bind Apache to specific IP addresses and
# ports. See also the <virtualHost> directive.
#
# Listen directives should be qualified with either an IPv4 or IPv6 address.
# Use 0.0.0.0 for the default IPv4 address and [::] for the default IPv6 address.
# e.g. Uncomment the following line to Listen on IPv6 Port 80 on Windows XP or 2003
# Listen [::]:80
# Use Listen 0.0.0.0:80 or Afpaport 80 if you also wish to accept connections over IPv4.
# windows IPv6 networking must be configured before enabling IPv6 Listens.

##
## To enable AFPA on supported windows operating systems delete the "#" symbol in
## front of the "LoadModule ibm_afpa_module modules/mod_afpa_cache.so" directive
##
```

c) Add the following lines to **httpd.conf** to configure the virtual host and SSL. Make sure to use the correct **ServerName** for your machine (was61hostXX) and the appropriate **DocumentRoot** and **Keyfile**. Place these lines near the very bottom of the httpd.conf, after the VirtualHost example and before the loading of the WebSphere plug-in module.

Listen 443

```
<VirtualHost w2k3was61.rc.net:443>
```

```
ServerName w2k3was61
```

```
DocumentRoot "C:/Program Files/IBM/HTTPServer/htdocs/en_US"
```

```
SSLEnable
```

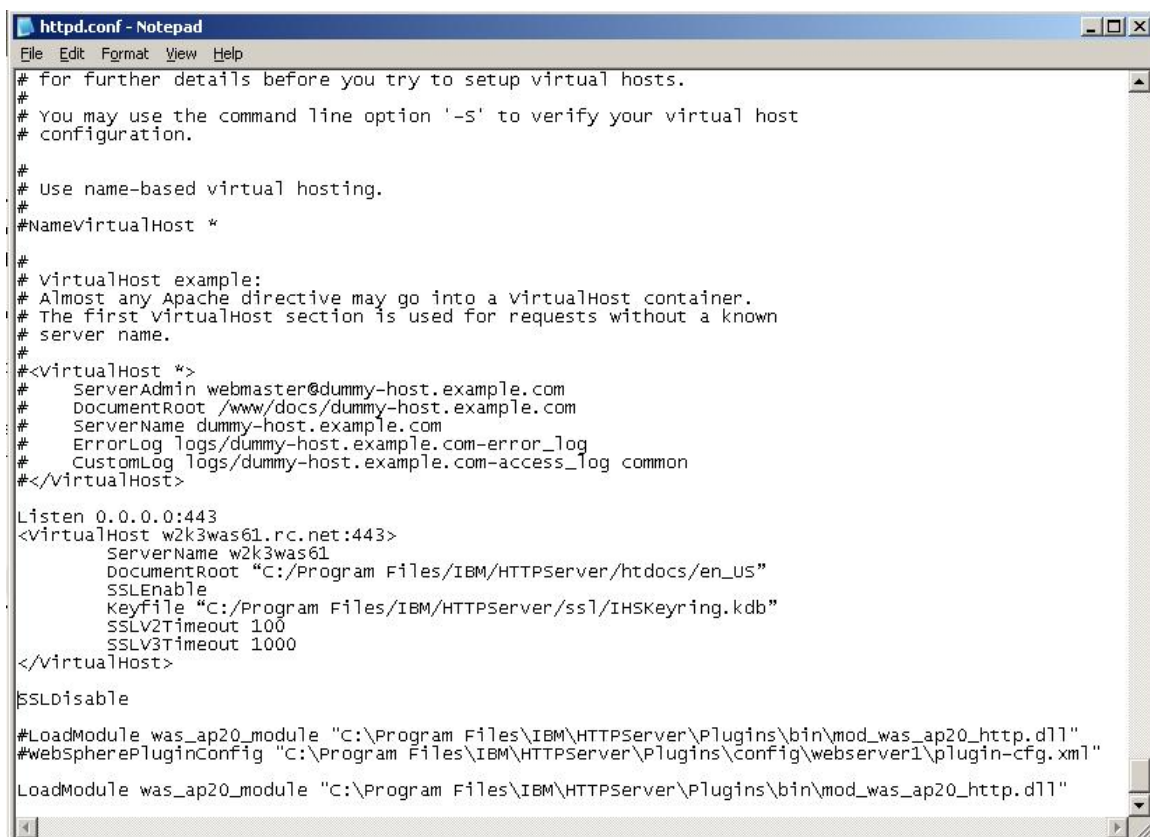
```
Keyfile "C:/Program Files/IBM/HTTPServer/ssl/ihsKeyring.kdb"
```

```
SSLV2Timeout 100
```

```
SSLV3Timeout 1000
```

```
</VirtualHost>
```

```
SSLDisable
```



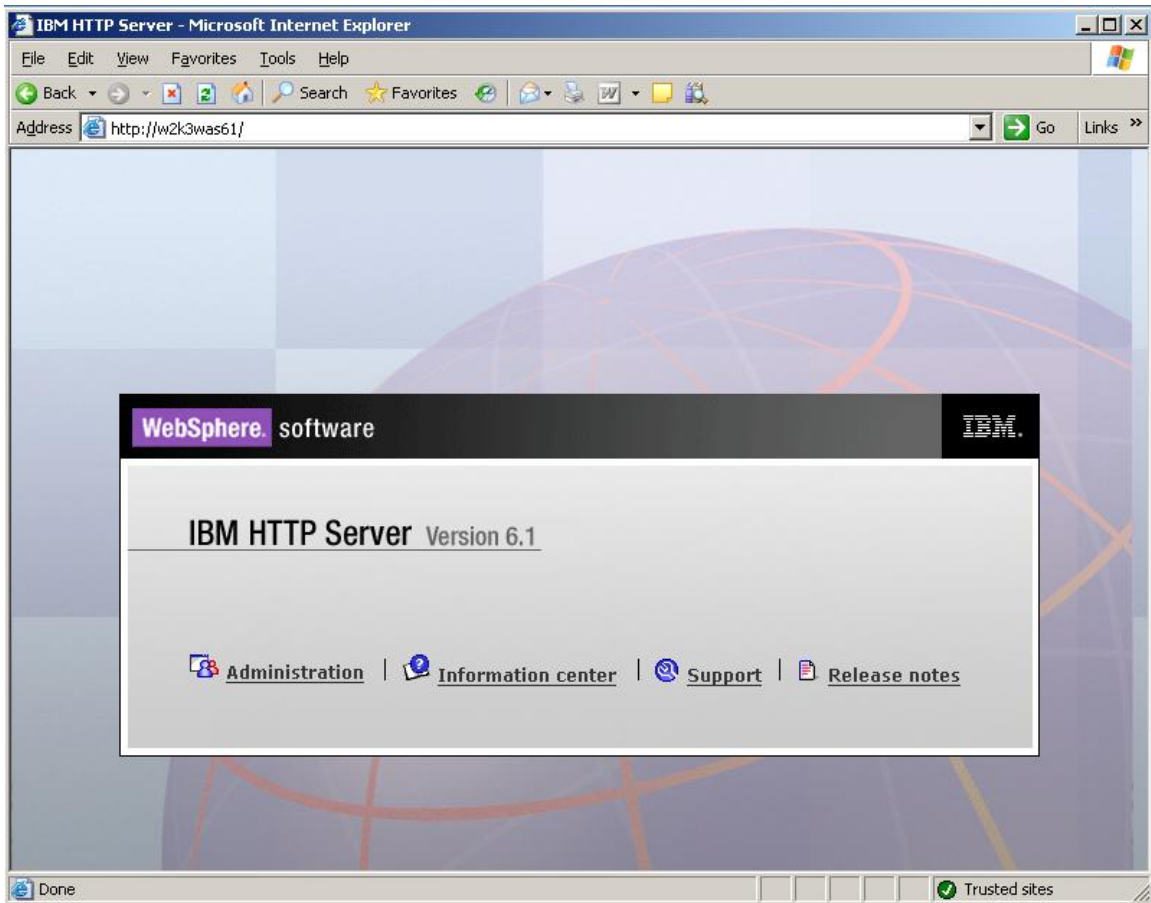
```
httpd.conf - Notepad
File Edit Format View Help
# for further details before you try to setup virtual hosts.
#
# You may use the command line option '-s' to verify your virtual host
# configuration.
#
# Use name-based virtual hosting.
#
#NameVirtualHost *
#
# virtualHost example:
# Almost any Apache directive may go into a virtualHost container.
# The first virtualHost section is used for requests without a known
# server name.
#
#<VirtualHost *>
#   ServerAdmin webmaster@dummy-host.example.com
#   DocumentRoot /www/docs/dummy-host.example.com
#   ServerName dummy-host.example.com
#   ErrorLog logs/dummy-host.example.com-error_log
#   CustomLog logs/dummy-host.example.com-access_log common
#</VirtualHost>
Listen 0.0.0.0:443
<VirtualHost w2k3was61.rc.net:443>
    ServerName w2k3was61
    DocumentRoot "C:/Program Files/IBM/HTTPServer/htdocs/en_US"
    SSLEnable
    Keyfile "C:/Program Files/IBM/HTTPServer/ssl/ihsKeyring.kdb"
    SSLV2Timeout 100
    SSLV3Timeout 1000
</VirtualHost>
SSLDisable
#LoadModule was_ap20_module "C:/Program Files/IBM/HTTPServer/Plugins/bin/mod_was_ap20_http.dll"
#WebSpherePluginConfig "C:/Program Files/IBM/HTTPServer/Plugins/config/webserver1/plugin-cfg.xml"
LoadModule was_ap20_module "C:/Program Files/IBM/HTTPServer/Plugins/bin/mod_was_ap20_http.dll"
```

d. **Save** your updates and **exit** the editor

Testing the SSL Connection

- 1) Restart the IBM HTTP Server process so that the new httpd.conf settings take effect
 - a) Using the Window Services, select the IBM HTTP Server 6.1 service from its context menu select **Restart**
 - b) Verify that the IBM HTTP Server process is running by checking the system process list. If IBM HTTP Server failed to start, check the <ihs_root>\logs\error.log and <profile_root>\logs\<webserver>\http_plugin.log for the cause.
- 2) Connect to IBM HTTP Server using HTTPS
 - a) First, verify that the Web server is actually running. Connect to the following site:

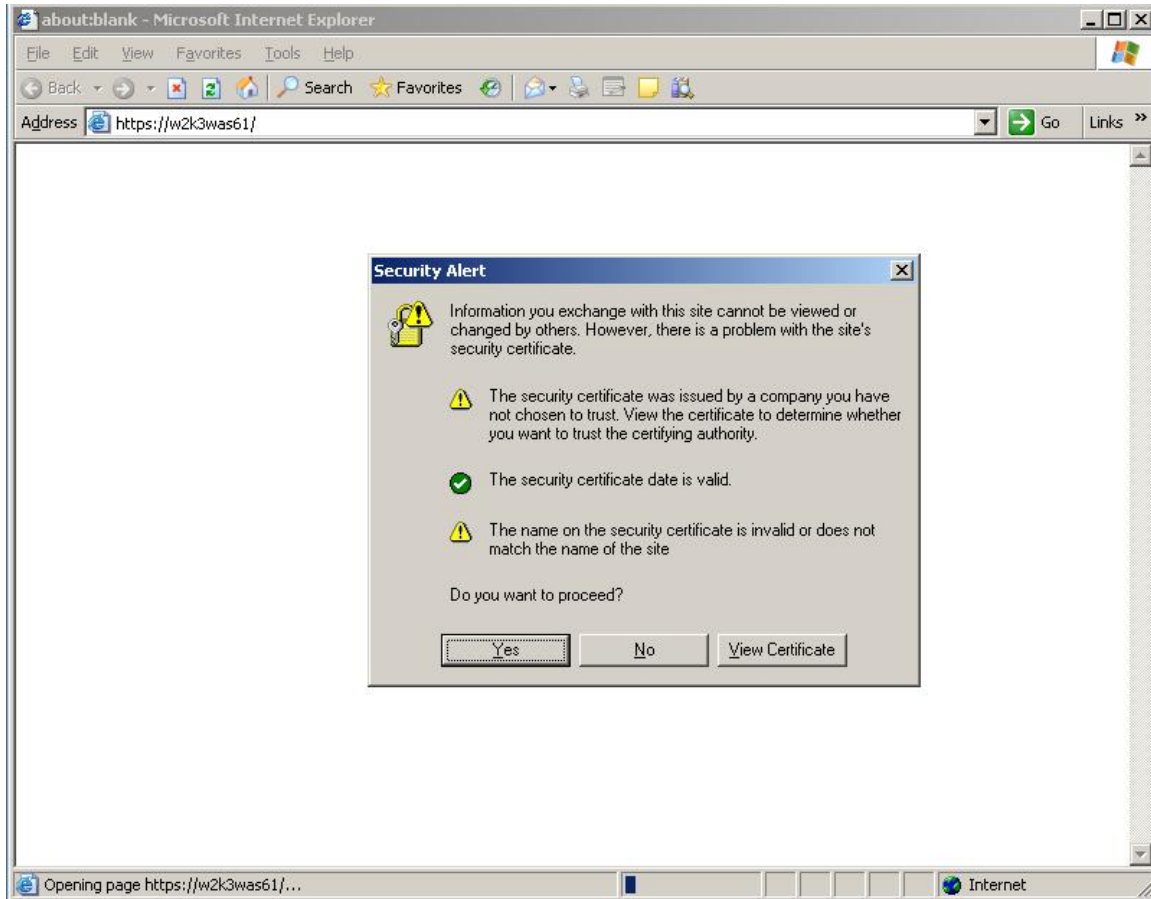
<http://w2k3was61/>



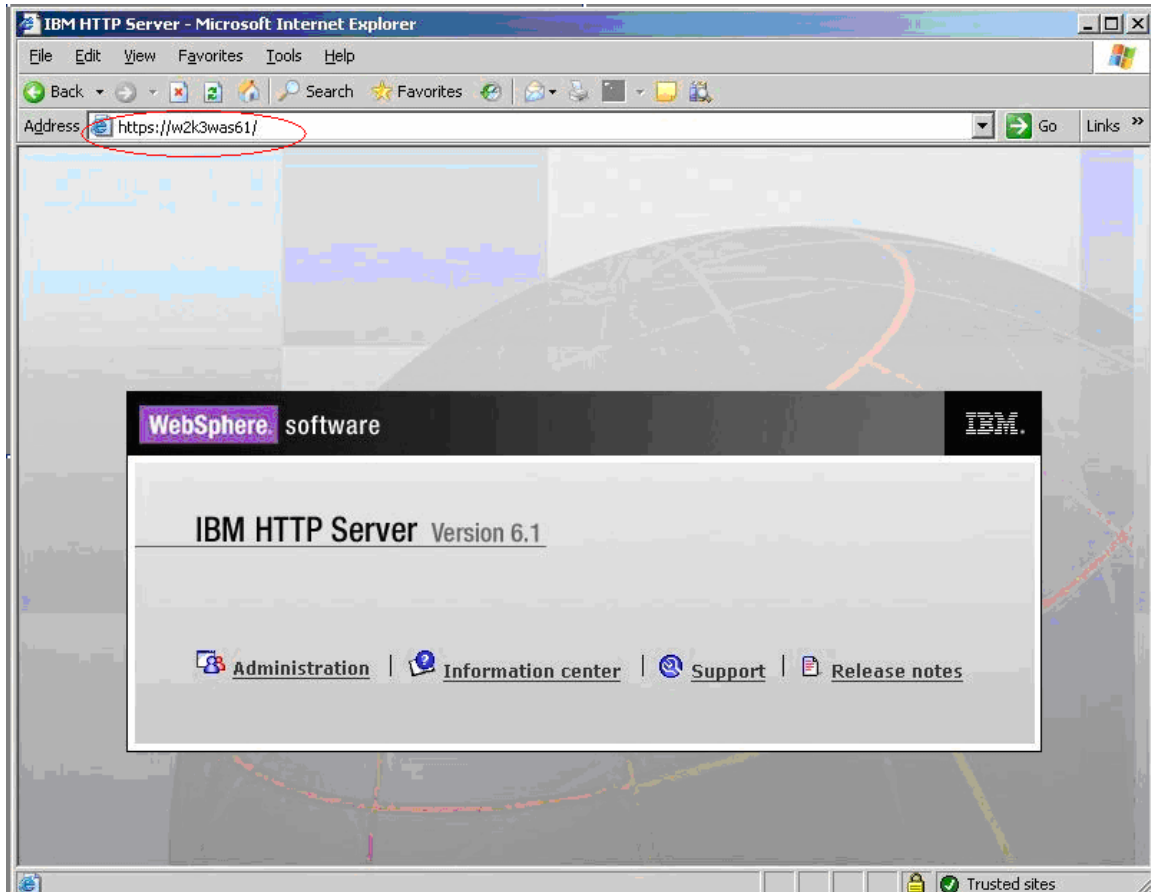
b) Now that the Web server is known to be running, enter the following URL to verify that **HTTPS** is working (notice, the only different is that the HTTP protocol was replaced with HTTPS):

https://w2k3was61/

c) There should be a challenge regarding the certificate since it is self signed



e) The front page for IBM HTTP Server should now be displayed having used HTTPS.



That takes care of talking to the Web server with HTTPS. But, in order for the HTTPS connections to be able to reach the application server, port 443 needs to be enabled on the application server's virtual host. WebSphere Application Server V6.1 automatically adds port 443 to the default virtual host, but it would be a good idea to verify that it is there.

- 1) Using the administrative console, select **Environment** —> **Virtual Hosts**.
- 2) Click **default_host**.
- 3) On the right, under **Additional Properties**, click **Host Aliases**
- 4) Verify that port **443** is one of the ports listed. If it is not, you should add it.

Integrated Solutions Console - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address http://localhost:9060/ibm/console/login.do

Integrated Solutions Console Welcome wasadmin Help Logout

View: All tasks

- Welcome
- Guided Activities
- Servers
 - Application servers
 - Generic servers
 - Proxy Servers
 - Version 5 JMS servers
 - Web servers
 - Clusters
 - Cluster topology
 - Generic Server Clusters
 - WebSphere MQ servers
- Core groups
- Applications
 - Enterprise Applications
 - Install New Application
- Resources
- Security
- Environment
 - Virtual Hosts
 - Update global Web server plug-in configuration
 - WebSphere Variables
 - Shared Libraries
 - Replication domains
 - URI Groups
- Naming
- System administration
- Users and Groups
- Monitoring and Tuning
- Troubleshooting
- Service integration
- UDDI

Virtual Hosts

Virtual Hosts > default_host > Host Aliases

Use this page to edit, create, or delete a domain name system (DNS) alias by which the virtual host is known.

Preferences

New Delete

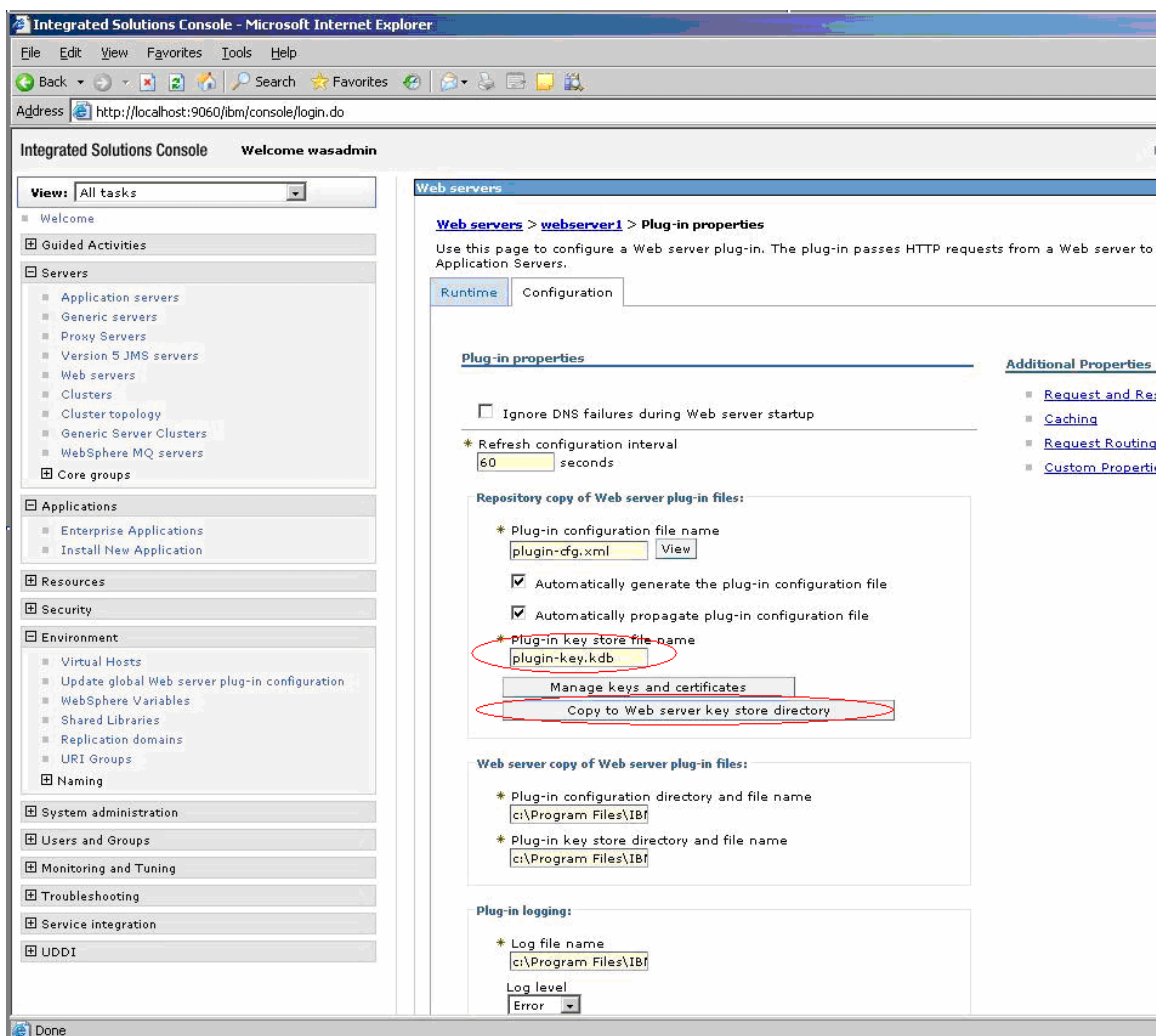
Select	Host Name	Port
<input type="checkbox"/>	*	9080
<input type="checkbox"/>	*	80
<input type="checkbox"/>	*	9443
<input type="checkbox"/>	*	5060
<input type="checkbox"/>	*	5061
<input type="checkbox"/>	*	443
Total		6

Field help
For field help information, select a field label or list marker when the help cursor appears.

Page help
More information about this page

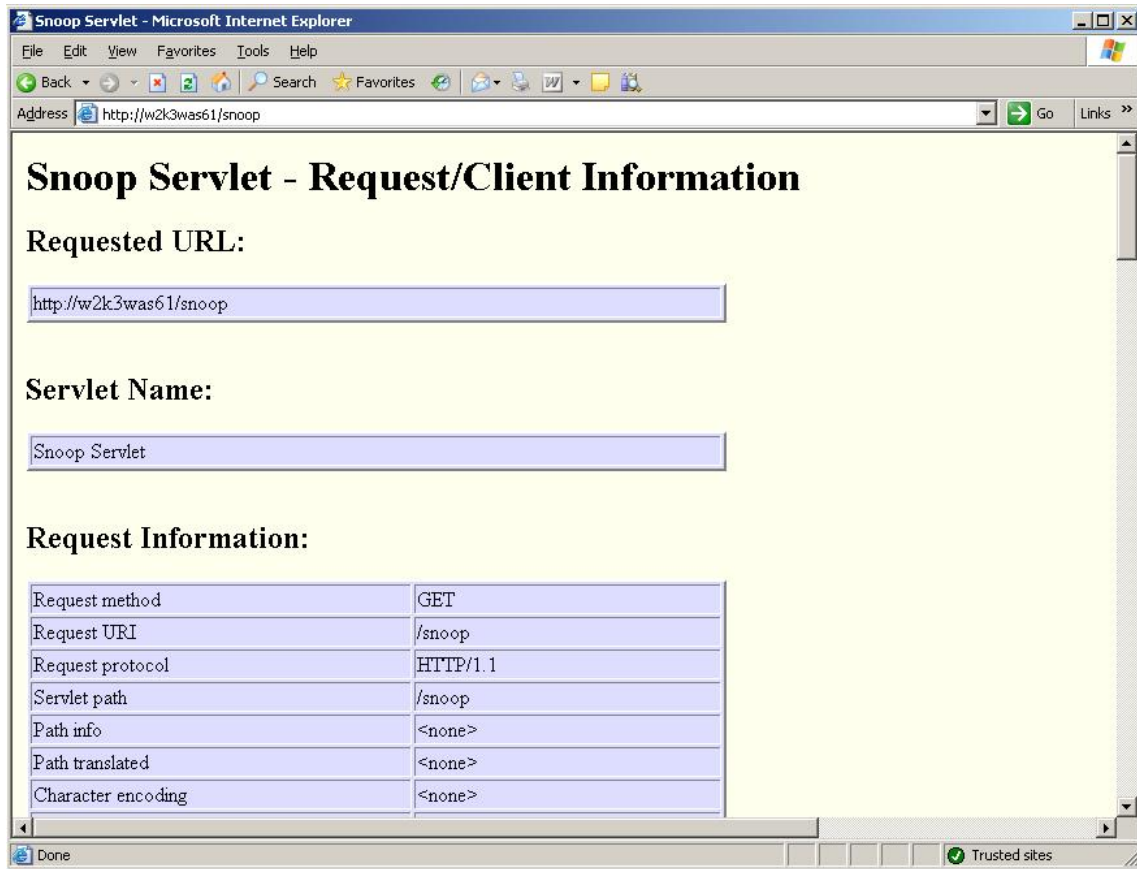
Local intranet

- 5) Since this document has configured the IBM HTTP Server to be a managed server, it is possible to propagate the correct version of the keyfile through the console. Using the administrative console, navigate to **Servers** → **Web servers**. Click your Web server, and then under the **Additional Properties** click **Plug-in properties**.
- 6) In the **Plug-in key store file name**, accept the default of **plugin-key.kdb** and click **Copy to Web server key store directory**. By checking the new date and time stamps of the directory entries, it is possible to verify that the key rings were in fact updated.



- 7) Test the HTTPS connection from the browser, through IBM HTTP Server, and back to WebSphere Application Server using snoop.
- a) Ensure that the WebSphere Application Server profile1 is running.
 - b) Restart the IBM HTTP Server.
 - c) Using a browser, verify that snoop is reachable with the following address:

<http://w2k3was61/snoop>



Snoop Servlet - Request/Client Information

Requested URL:

http://w2k3was61/snoop

Servlet Name:

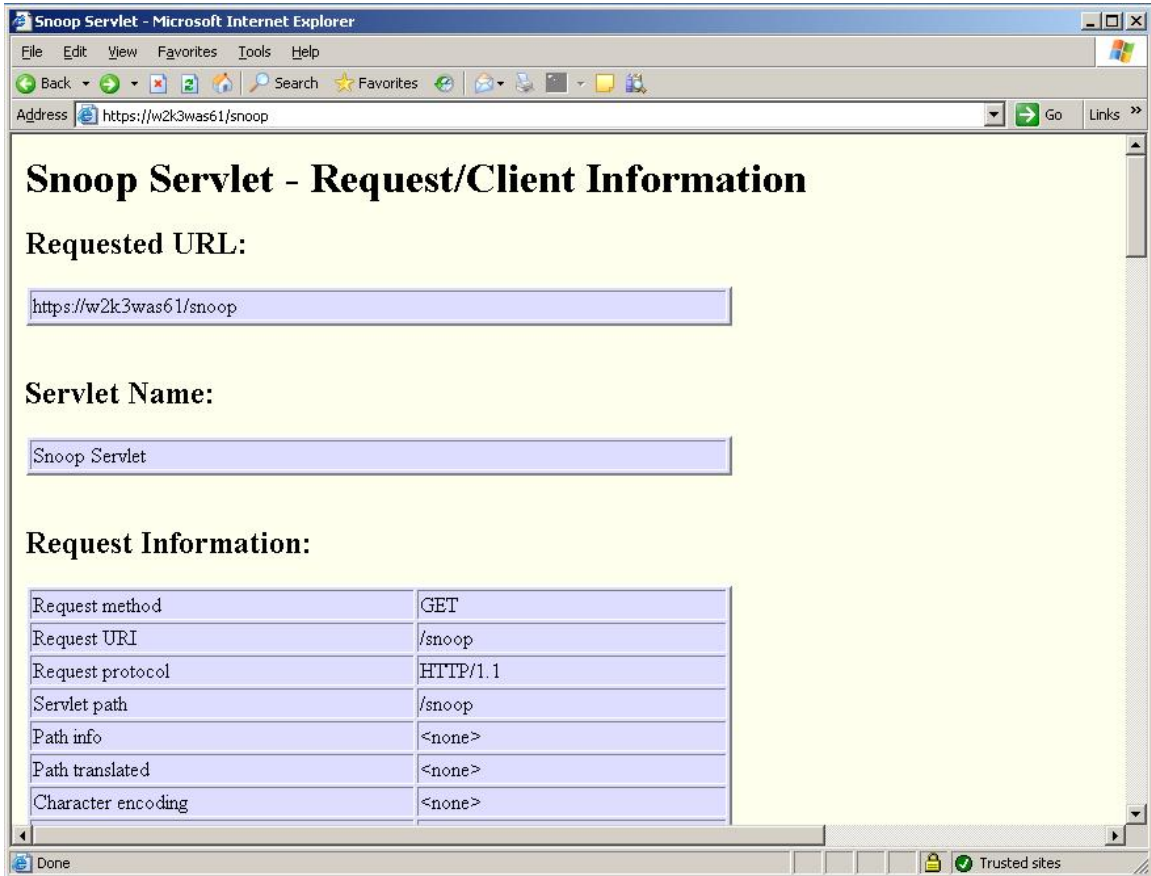
Snoop Servlet

Request Information:

Request method	GET
Request URI	/snoop
Request protocol	HTTP/1.1
Servlet path	/snoop
Path info	<none>
Path translated	<none>
Character encoding	<none>

Done Trusted sites

- d) Now try snoop using HTTPS, using the following URL (make sure to use HTTPS):
[https:// w2k3was61/snoop](https://w2k3was61/snoop)
- e) Accept the certificate if prompted.



Notice that the snoop servlet is showing that the connection was made via HTTPS.