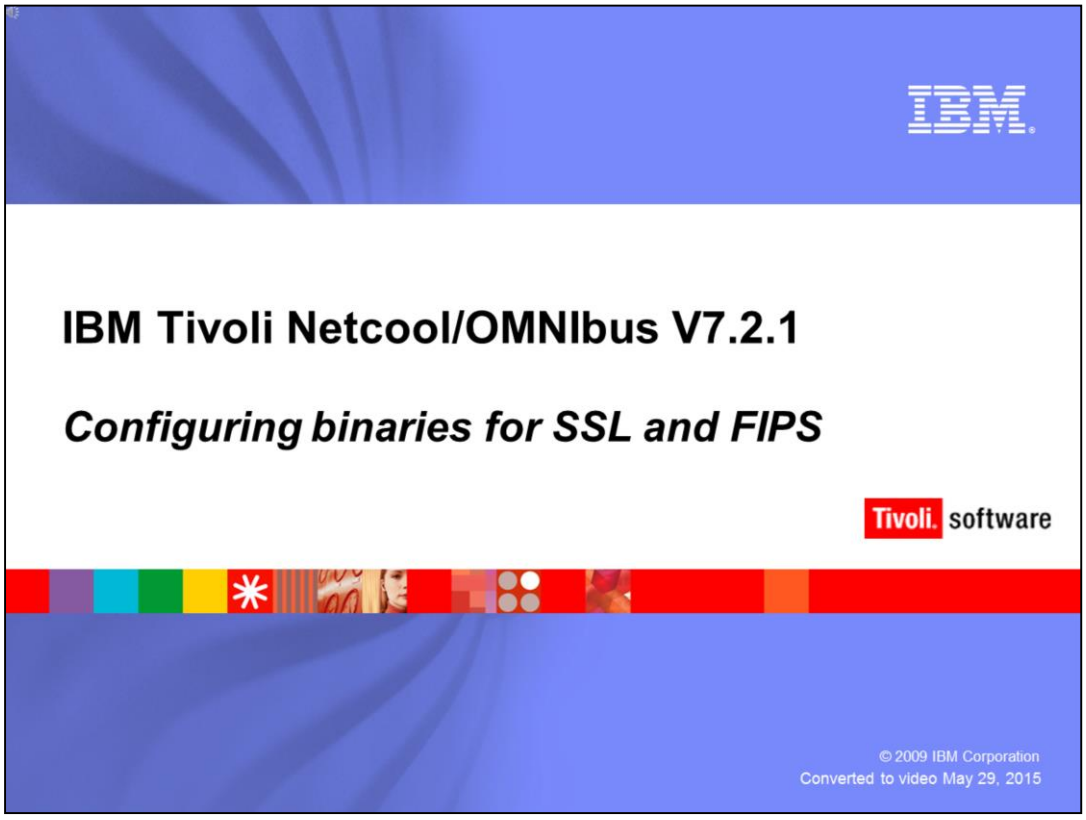
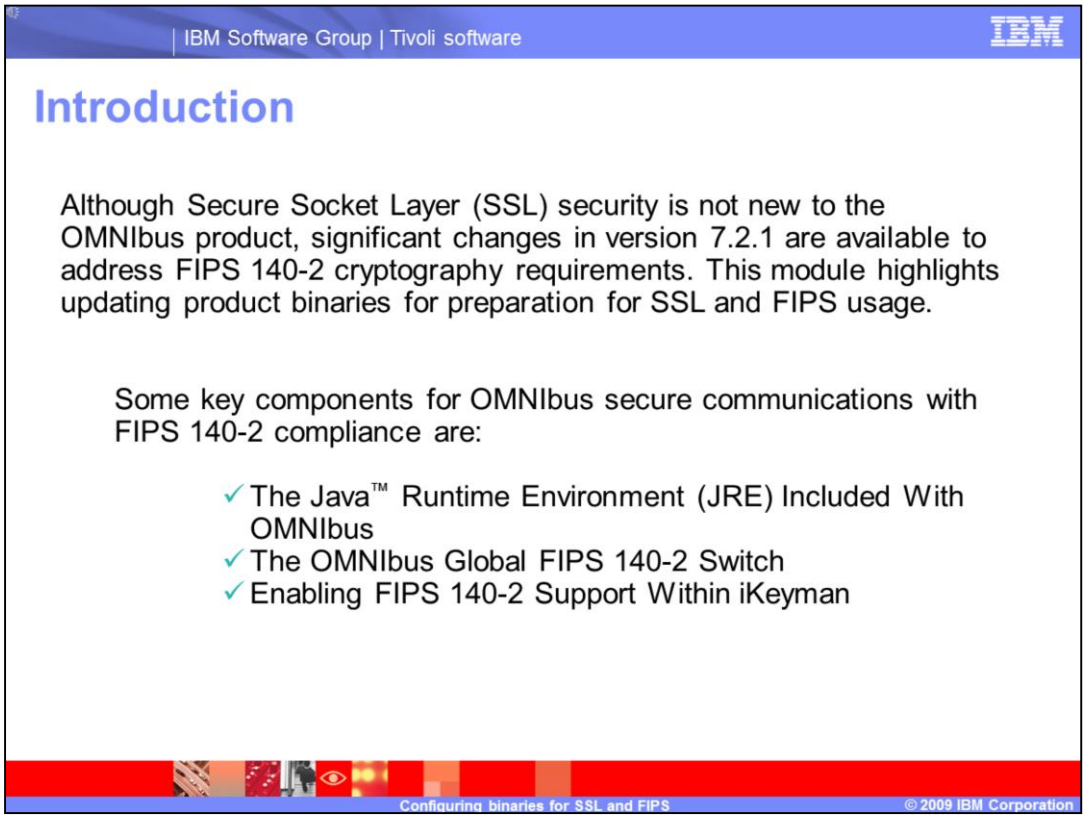


Hello, and welcome to the OMNIBUS IBM Education assistance module, Configuring binaries for SSL and FIPS .

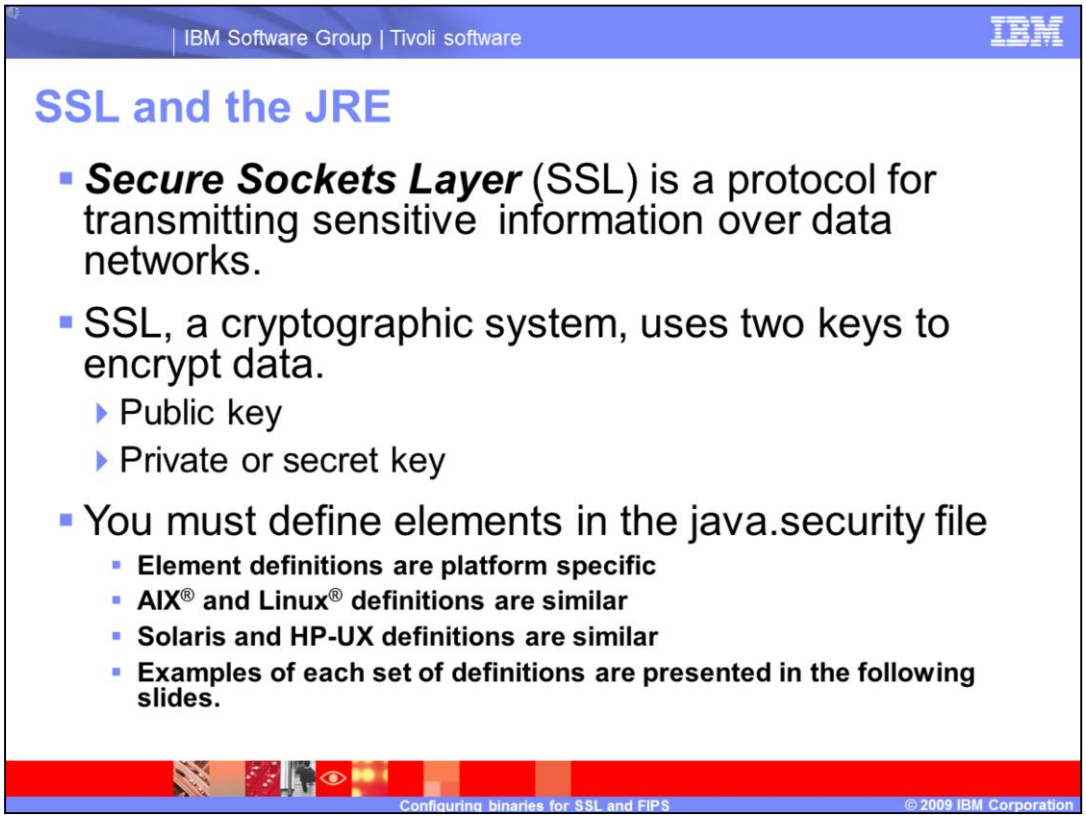


Although Secure Socket Layer (SSL) security is not new to the OMNIbus product, significant changes in version 7.2.1 are available to address FIPS 140-2 cryptography requirements. This module highlights updating product binaries for preparation for SSL and FIPS usage. Some key components for OMNIbus secure communications with FIPS 140-2 compliance are:

The Java Runtime Environment (JRE) Included With OMNIbus

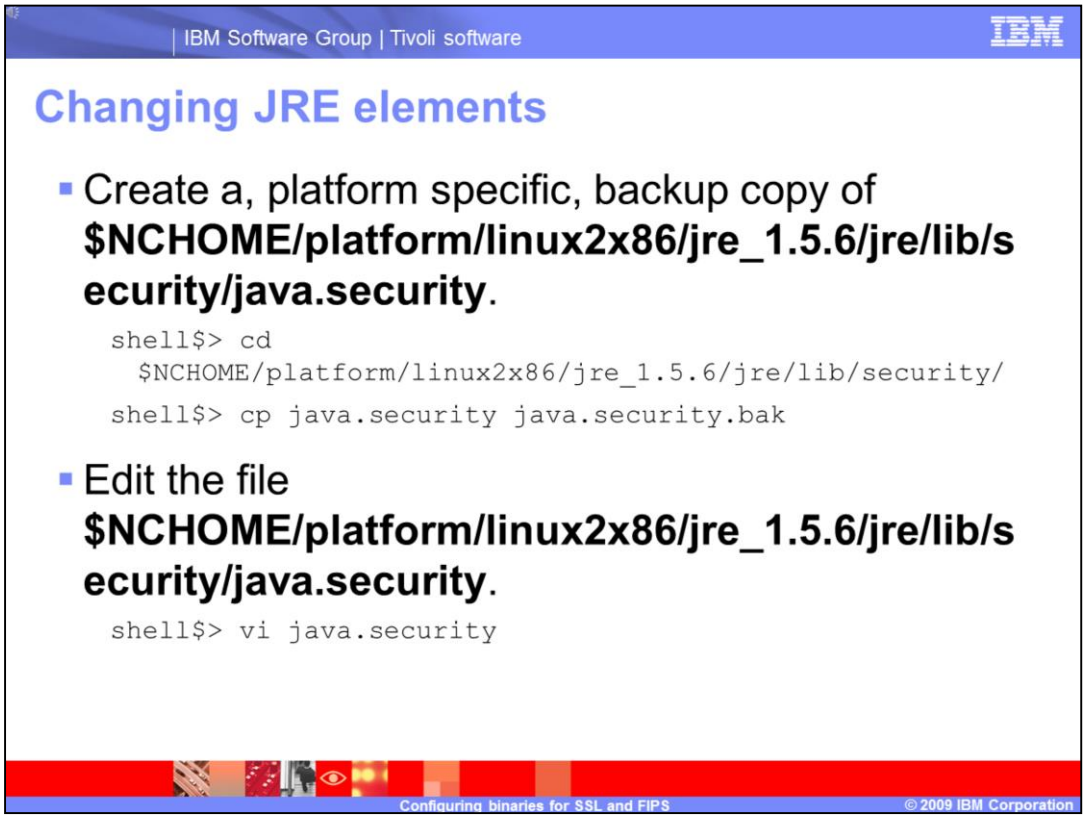
The OMNIbus Global FIPS 140-2 Switch

Enabling FIPS 140-2 Support Within iKeyman

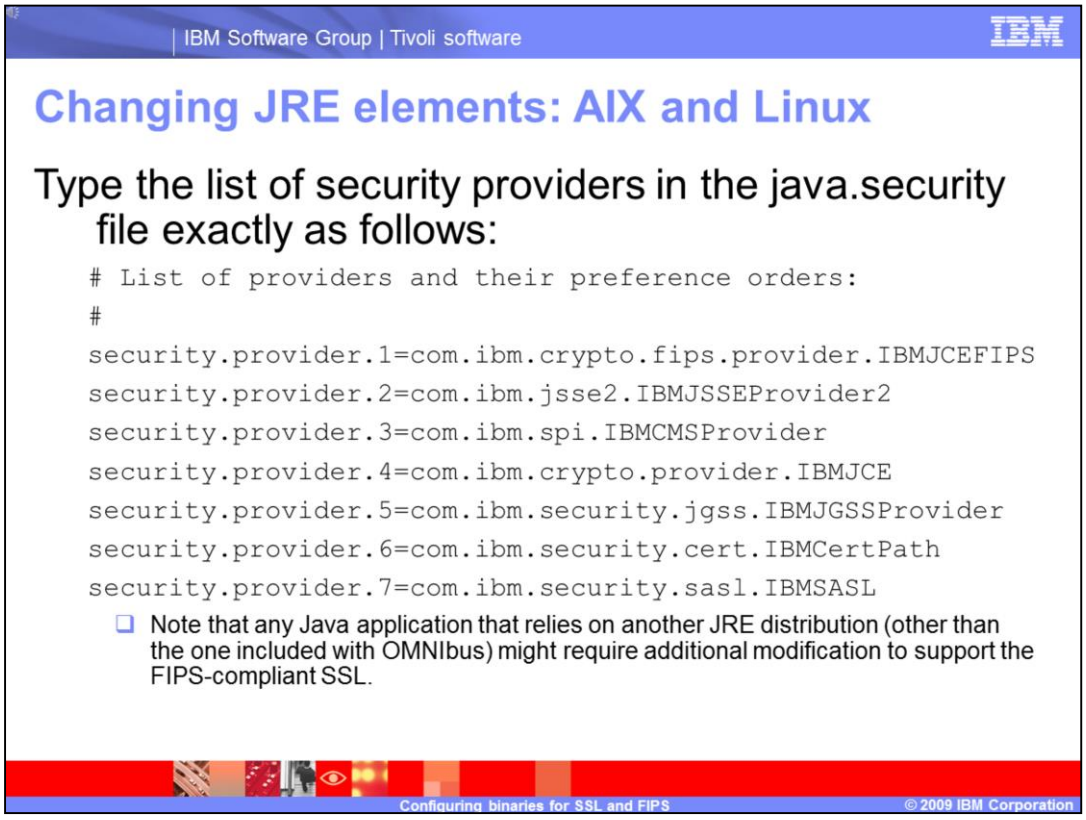


Secure Sockets Layer is a protocol for transmitting sensitive information over data networks.

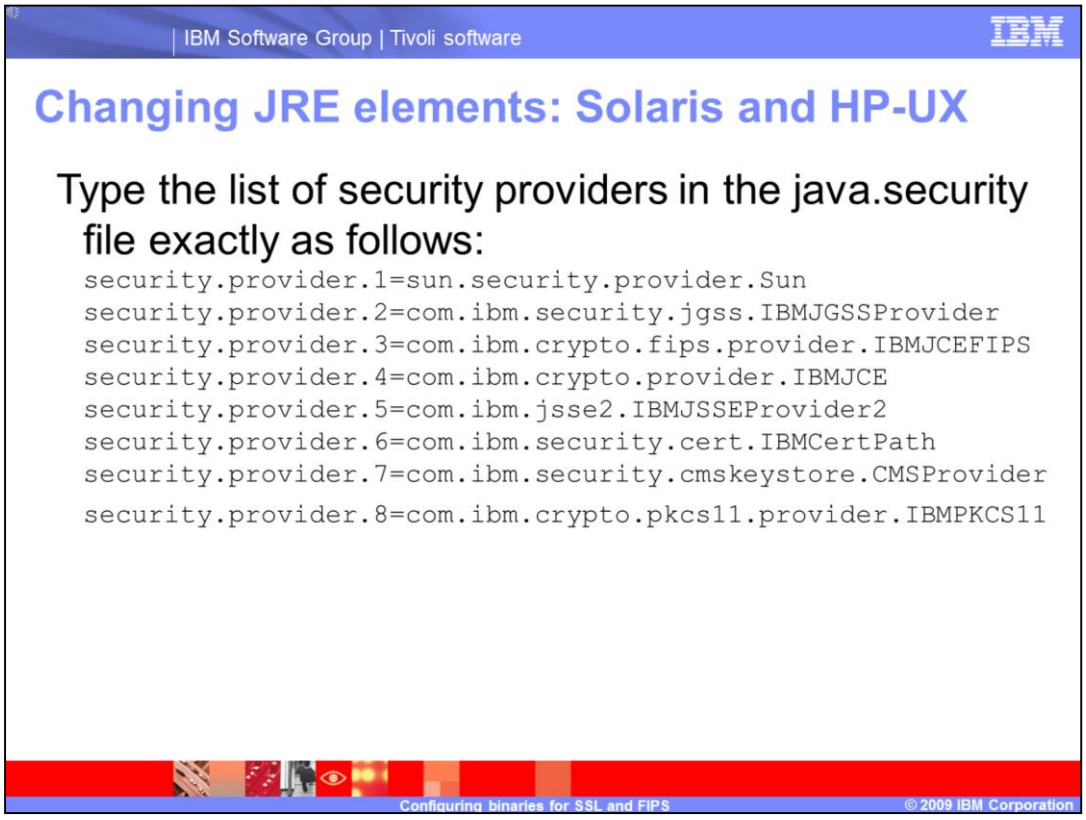
SSL, a cryptographic system, uses two keys to encrypt data. The first key is a public key the next a private or secret key. You must define different implementations of cryptographic elements in the java.security file. The java.security defines both SSL and FIPS compliance elements. Examples of each set of definitions are presented in the following slides.



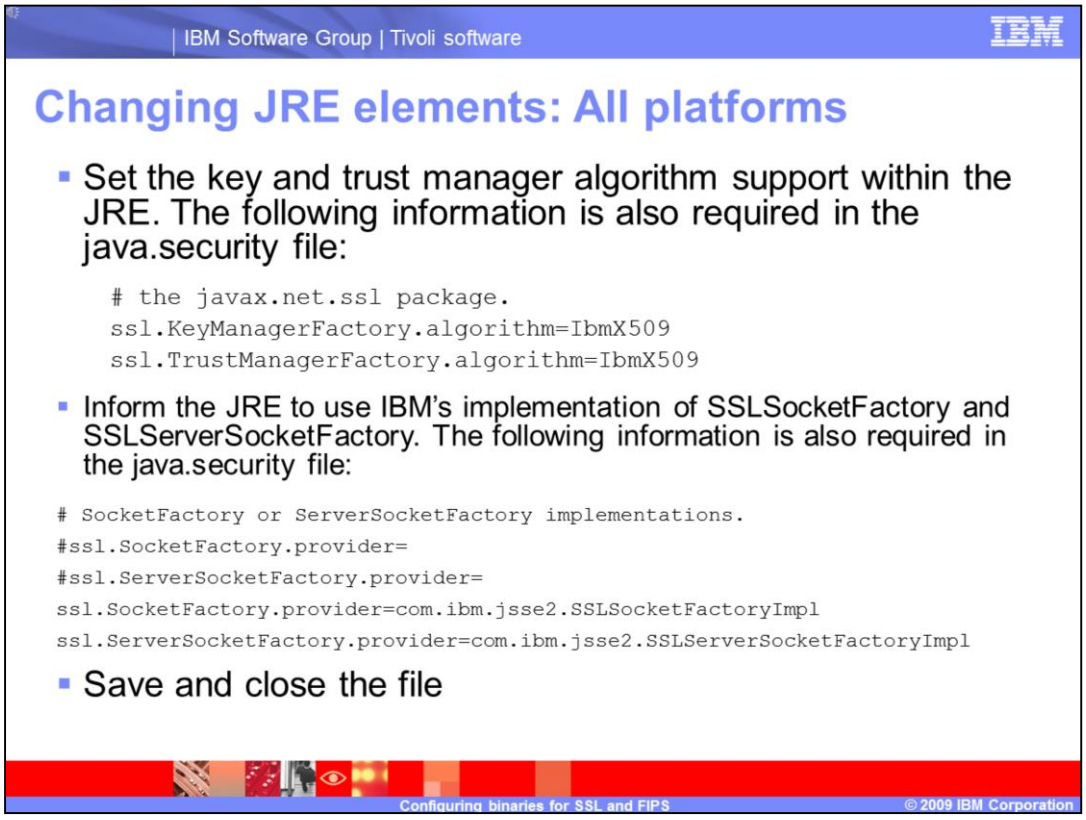
The first step is to create a backup copy of the java.security file. Next, open the java.security file for editing.



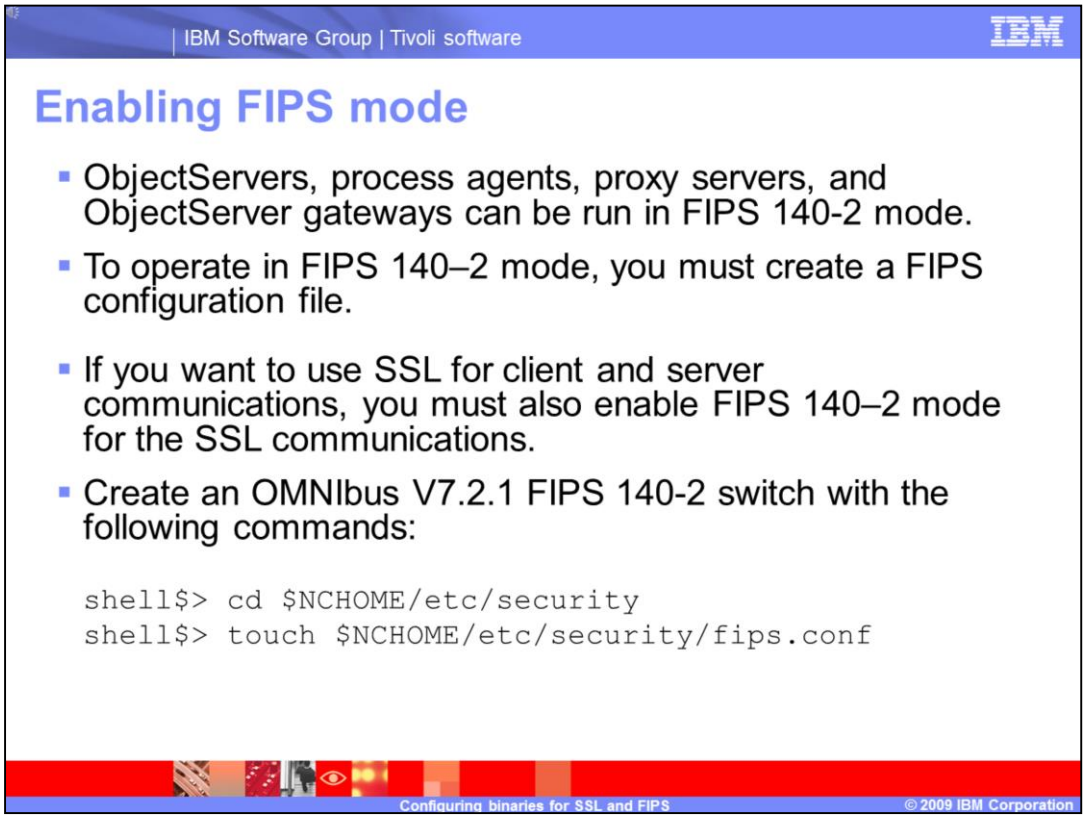
Next, for AIX and Linux platforms, modify the java.security file to include the list of cryptographic providers in exactly the order shown. Any other JRE distributions not included with the OMNIbus product distribution might require modifications.



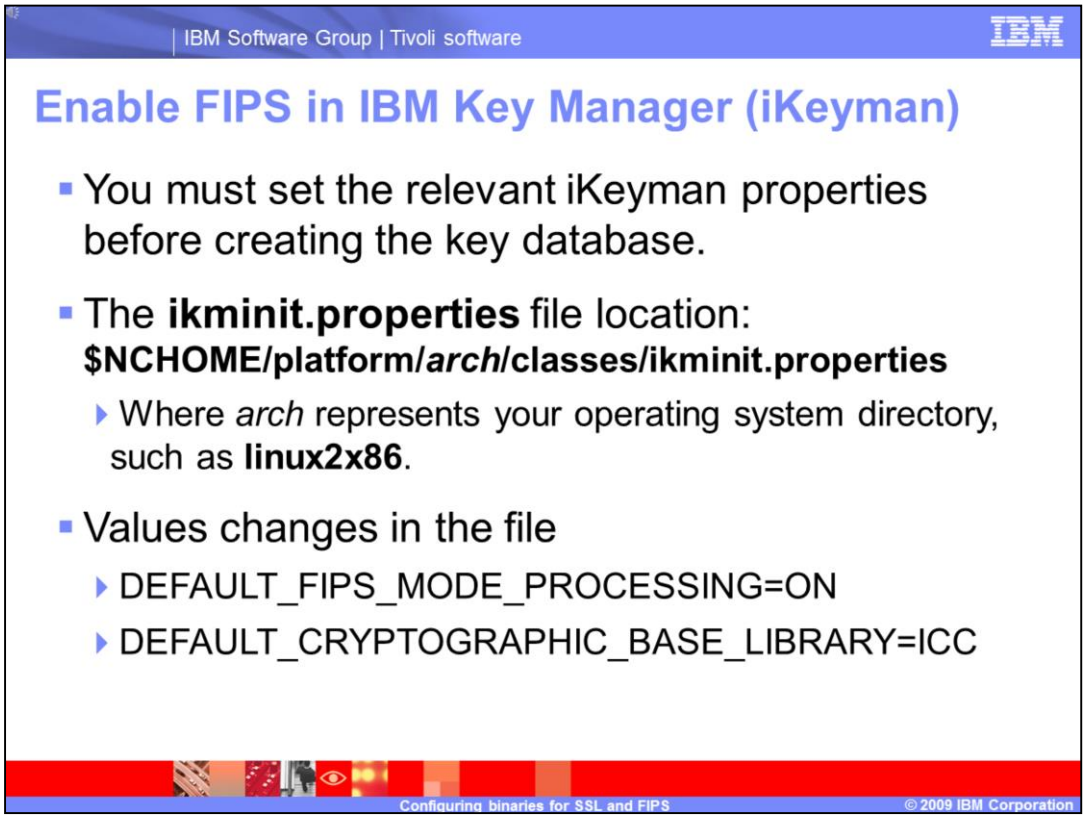
If you are configuring a Solaris or HP-UX platform, modify the java.security file to include the list of cryptographic providers in exactly the order shown.



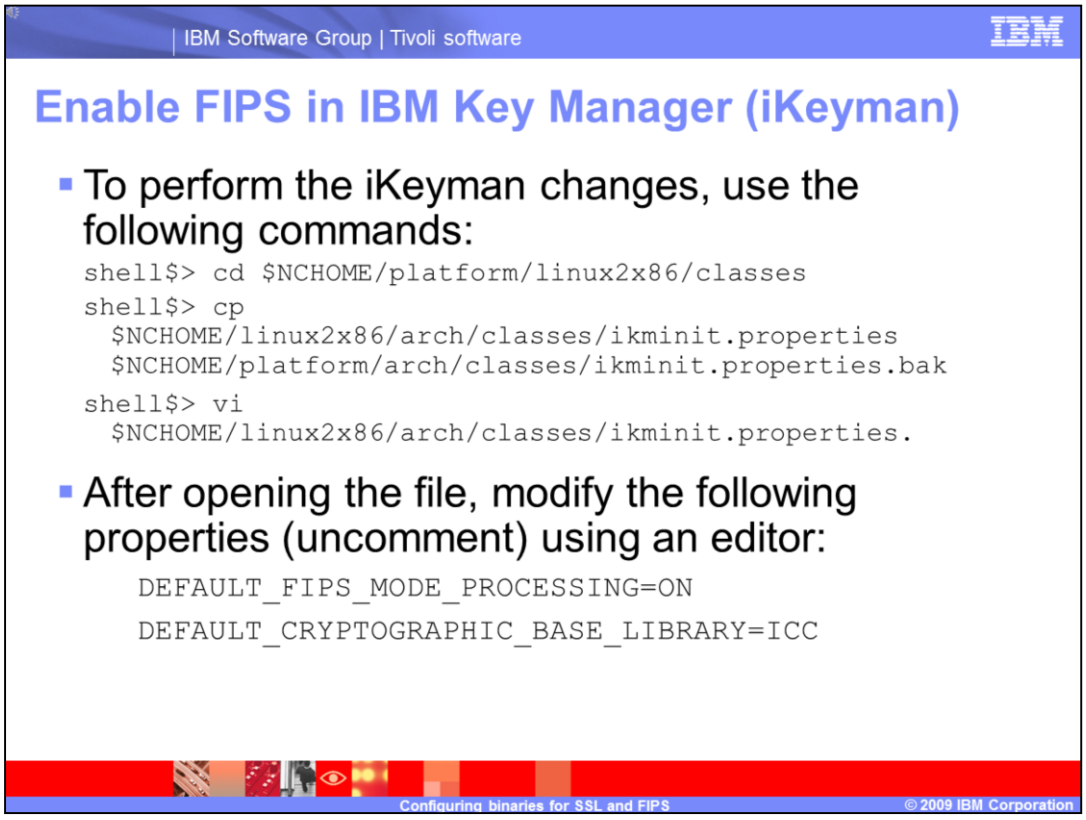
Continue to edit the java.security file in the section under **java.net.ssl**. Type the lines for the key and trust factories. In the Socket and ServerSocket sections, add the two additional lines. After you complete those last two entries, save and close the file.



ObjectServers, process agents, proxy servers, and ObjectServer gateways can be run in FIPS 140-2 mode. To operate in FIPS 140 2 mode, you must create a FIPS configuration file. If you want to use SSL for client and server communications, you must also enable FIPS 140 2 mode for the SSL communications. You create an OMNIbus 7.2.1 FIPS 140-2 Switch by performing the following command: **touch $NCHOME/etc/security/fips.conf .** This command is all that is required to enable FIPS within OMNIbus.



To enable FIPS in iKeyman you must set iKeyman properties before creating the key database. The iKeyman.properties file is located under the operating system specific directory. There are two values you must change.



To perform the iKeyman changes, use the following commands:

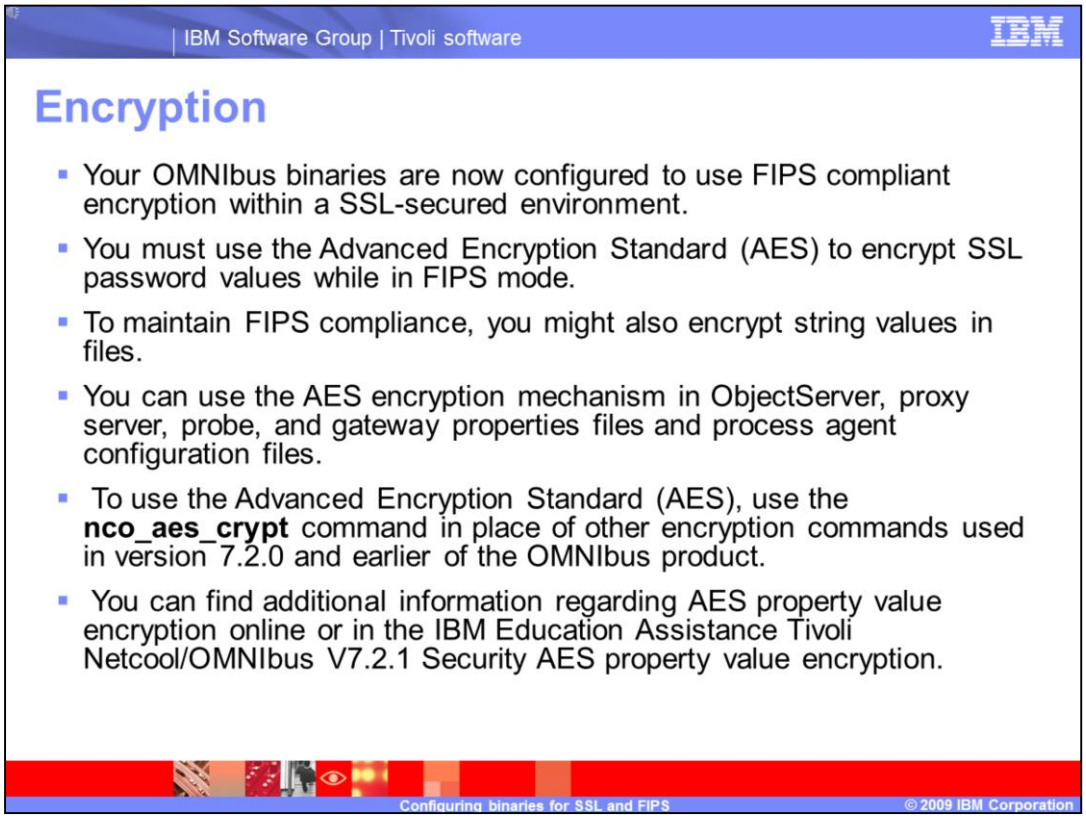
first, change directories to **`$NCHOME/platform/linux2x86/classes`**.

Next, copy **`ikminit.properties`** to **`ikminit.properties.bak`**

then use vi **`ikminit.properties`**.

After opening the file, modify the following properties by uncomment them using the editor:

```
DEFAULT_FIPS_MODE_PROCESSING and
DEFAULT_CRYPTOGRAPHIC_BASE_LIBRARY.
```



Your OMNIbus binaries are now configured to use FIPS compliant encryption within a SSL-secured environment.

You must use the Advanced Encryption Standard (AES) to encrypt SSL password values while in FIPS mode.

To maintain FIPS compliance, you might also encrypt string values in files.

You can use the AES encryption mechanism in ObjectServer, proxy server, probe, and gateway properties files and process agent configuration files.

To use the Advanced Encryption Standard (AES), use the **nco_aes_crypt** command in place of other encryption commands used in version 7.2.0 and earlier of the OMNIbus product.

Additional information regarding AES property value encryption can be referenced on-line or in the IBM Education Assistance Tivoli Netcool/OMNIbus V7.2.1 Security AES property value encryption.

For further training, refer to the link, http://www.ibm.com/software/tivoli/education/edu_prd.html.

This concludes this module.