IBM HTTP Server Jump Start Guide v6.1

by

Kevin Ackerman

01/03/09

Table of Contents

Installation....3
Installing IBM HTTP Server with a non-administrator user ID....3
Install GSKit. 3
Installing IBM HTTP Server silently....3
SSL Configurations and requirements....4
WebSphere Application Server Plugin configurations....4
Troubleshooting an IBM HTTP Server....5
Symptoms of poor server response time....5
I/O error messages....5
SSL initialization messages....6
Handshake messages....7
Configuration messages....15
Cache messages....16
SSL Key Management....17
Using the gsk7cmd command....17
gsk7cmd Syntax 17

Installation

Installing IBM HTTP Server with a non-administrator user ID

The common way to install IBM HTTP Server is to run the installation program using an administrator user ID. However, it is sometimes necessary to install IBM HTTP Server using a non-administrator (non-root) user ID.
Before you begin
You must run the setupadm command if you are installing IHS as a non-root user. The setupadm command is run in the <IHS_HOME>/bin directory so that you can properly use the administrative server with the WebSphere Application Server. The format for the command is as follows:

setupadm -usr <userName> -grp <groupName> -cfg <IHS Web server configuration file> -adm <IHS admistrative server configuration file> -plg <plug-in configuration file>

Install GSKit.

Complete this task separately, using the root user ID if SSL configuration is required and no version of GSKit is installed, or if the installed version is down-level. Launch the GSKit installation from the WebSphere Application Server CDROM as follows:

* [AIX] [HP-UX] [Linux] [Solaris] GSKit/gskit.sh
* [Windows] GSKit\setup.exe "IHS6.1"

If GSKit is not installed, the following configurations will not work:

* SSL between client (browser) and IBM HTTP Server.
* SSL between the IBM HTTP Server plug-in and WebSphere Application Server.
* SSL between IBM HTTP Server and LDAP server.

[Solaris] Note: The non-root installation of the IBM HTTP Server plug-in is not supported, because there is a dependency on the GSKit libraries which require full root authority to install. If you do not install GSKit, the IBM HTTP Server plug-in fails to load.

The way to handle this dependency is to first install the GSKit libraries with a root user ID. Then, you can install the IBM HTTP Server plug-in using a non-root user ID.

Installing IBM HTTP Server silently

Procedure

1. [AIX] [HP-UX] [Linux] [Solaris] Log on as root.
2. [Windows] Log on as a member of the administrator group. Considerations for Windows operating systems follow:
    * Some steps for installing silently require the administrator group user to have the following advanced user rights:
        - Act as part of the operating system
        - Log on as a service
    * The installation wizard grants your Windows user ID the advanced user rights, if the user ID belongs to the administrator group. The silent installation does not grant these rights. If you create a new user ID on a Windows platform to perform the silent installation, you must restart the system to activate the proper authorizations for the user ID, before you can perform a successful silent installation.
    * When installing IBM HTTP Server as a Windows service, do not use a user ID that contains spaces. A user ID with spaces cannot be validated. Such a user ID is not allowed to continue the installation. To work

around this problem, install with the service configured to run as LocalSystem, and then modify the user ID after install.

3. Copy the responsefile.txt file to your disk drive and rename it, for example myoptionsfile.txt. You can now customize it. Accept the IBM HTTP Server license by setting -OPT silentInstallLicenseAcceptance="true" in your response file.

4. Issue the proper command to use your custom response file. For example, issue one of the following commands:
    * [AIX] [HP-UX] [Linux] [Solaris] mnt_cdrom/IHS/install -options myoptionsfile.txt -silent
    * [Windows] "CD-ROM drive:\IHS\install" -options "myoptionsfile.txt" -silent

[AIX] [HP-UX] [Linux] [Solaris] To silently install IBM HTTP Server, the X Windows software must be installed on the system.

You can find the sample options response file in the IBM HTTP Server directory on the product CD.

Results

If the installation is successful, the IBM HTTP Server product is installed and the log file is located in the /logs/install/ directory. However, if the product installation fails, see the log.txt file in either the /logs/install/ directory or the $USER/ihslogs/ directory.

SSL Configurations and requirements

Confirm that the Global Security Kit is installed and meets the minimum requirements
Create a key database file and certificates needed to authenticate the Web server during an SSL handshake
Configure the httpd.conf configuration file

Verify that the SSL modules are uncommented
LoadModule ibm_ssl_module modules/mod_ibm_ssl.so

Add the following lines, replacing $IHSROOT with the location of the IHS installation
SSLEnable
Keyfile "$IHSROOT/keys/myhost1.myhost.kdb"

When possible you should reference the IBM support site for the latest modules available and apply.

WebSphere Application Server Plugin configurations

Add the following lines, replacing $IHSROOT with the location of the IHS installation
LoadModule was_ap20_module $IHSROOT/loadmodule/mod_was_ap20_http.so
WebSpherePluginConfig $IHSROOT/loadmodule/plugin-cfg.xml

Troubleshooting an IBM HTTP Server

The following was taken from
http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/index.jsp?topic=/com.ibm.websphere.ihs.doc/info/ihs/ihs/tihs_troubvwerrmsg.html

Symptoms of poor server response time

If you notice that server CPU utilization appears low, but client requests for static pages take a long time to service, your server may be running out of server threads to handle requests.
This situation results when you have more inbound requests than you have Apache threads to handle those requests. New connections queue in the TCP/IP stack listen queue wait for acceptance from an available thread. As a thread becomes available, it accepts and handles a connection off of the listen queue. Connections can take a long time to reach the top of the listen queue. When this condition occurs, the following error message will appear in the error log:

* [AIX] [HP-UX] [Linux] [Solaris] [z/OS] "Server reached MaxClients setting, consider raising the MaxClients setting"
* [Windows] "Server ran out of threads to serve requests. Consider raising the ThreadsPerChild setting"

I/O error messages

This topic contains error messages that might result due to I/O failures and provides solutions to help you troubleshoot these problems.
The following messages appear due to read failures:

* Message: SSL0400I: I/O failed, RC <code>.
    - Reason: The server received an error trying to read on the socket.
    - Solution: Some errors are expected during normal processing, especially a '406' error, which you can ignore. If you are unable to access the server and receive these errors, report this problem to Service.
* Message :SSL0401E: I/O failed with invalid handle <handle>.
    - Reason: An internal error has occurred.
    - Solution: Report this problem to Service.
* Message: SSL0402E: I/O failed, the GSKit library is not available.
    - Reason: A call to the GSKit function failed because the dynamic link library unloaded (Windows operating systems only).
    - Solution: Shut down the server and restart.
* Message: SSL0403E: I/O failed, internal error.
    - Reason: The communication between client and the server failed due to an error in the GSKit library.
    - Solution: Retry connection from the client. If the error continues, report the problem to Service.
* Message: SSL0404E: I/O failed, insufficient storage.
    - Reason: The server could not allocate memory needed to complete the operation.
    - Solution: Take action to free up some additional memory. Try reducing the number of threads or processes running, or increasing virtual memory.
* Message:SSL0405E: I/O failed, SSL handle <handle> is in an invalid state.
    - Reason: The SSL state for the connection is invalid.
    - Solution: Retry connection from the client. If the error continues, report the problem to Service.
* Message:SSL0406E: I/O failed, cryptography error.
    - Reason: A cryptography error occurred.
    - Solution: None. If the problem continues, report it to Service.

* Message:SSL0407I: I/O failed, Error validating ASN fields in certificate.
    - Reason: The server was not able to validate one of the ASN fields in the certificate.
    - Solution: Try another certificate.
* Message:SSL0408E: I/O failed with invalid buffer size. Buffer <address>, size <length>.
    - Reason: The buffer size in the call to the read function is zero or negative.
    - Solution: None. Report this problem to Service.

* Message: SSL0409I: I/O error occurred
    - Reason: An unexpected network error occurred while reading or writing data over an SSL connection, likely a client disconnecting.
    - Solution: This is an informational message that does not indicate any failure in delivering a response, therefore no solution is provided.
* Message: SSL0410I: Socket was closed
    - Reason: An SSL client connection was closed by the client.
    - Solution: This is an informational message that does not indicate any failure in delivering a response, therefore a solution is not provided.

SSL initialization messages

This topic contains error messages that might result due to SSL initialization problems and provides solutions to help you troubleshoot these problems.
The following messages display as a result of initialization problems:

* Message: SSL0100S: GSK could not initialize, <errorCode>
    - Reason: Initialization failed when the SSL library returned an unknown error.
    - Solution: None. Report this problem to Service.
* Message: SSL0101S: GSK could not initialize, Neither the password nor the stash file name was specified. Could not open key file.
    - Reason: The stash file for the key database could not be found or is corrupted.
    - Solution: Use IKEYMAN to open the key database file and recreate the password stash file.
* Message: SSL0102E: GSK could not initialize, Could not open key file.
    - Reason: The server could not open the key database file.
    - Solution: Check that the Keyfile directive is correct and that the file permissions allow the Web server user ID to access the file.
* Message: SSL0103E: Internal error - GSK could not initialize, Unable to generate a temporary key pair.
    - Reason: GSK could not initialize; Unable to generate a temporary key pair.
    - Solution: Report this problem to Service.
* Message: SSL0104E: GSK could not initialize, Invalid password for key file.
    - Reason: The password retrieved from the stash file could not open the key database file.
    - Solution: Use IKEYMAN to open the key database file and recreate the password stash file. This problem could also result from a corrupted key database file. Creating a new key database file may resolve the problem.
* Message: SSL0105E: GSK could not initialize, Invalid label.
    - Reason: Specified key label is not present in key file.
    - Solution: Check that the SSLServerCert directive is correct, if coded, and that the label is valid for one of the keys in the key database.
* Message: SSL0106E: Initialization error, Internal error - Bad handle
    - Reason: An internal error has occurred.
    - Solution: Report this problem to Service.
* Message: SSL0107E: Initialization error, The GSK library unloaded.
    - Reason: A call to the GSKit function failed because the dynamic link library unloaded (Windows only).
    - Solution: Shut down the server and restart.
* Message: SSL0108E: Initialization error, GSK internal error.
    - Reason: The communication between client and the server failed due to an error in the GSKit library.
    - Solution: Retry connection from the client. If the error continues, report the problem to Service.
* Message: SSL0109E: GSK could not initialize, Internal memory allocation failure.

    o Reason: The server could not allocate memory needed to complete the operation.
    o Solution: Take action to free up some additional memory. Try reducing the number of threads or processes running, or increasing virtual memory.
  * Message :SSL0110E: Initialization error, GSK handle is in an invalid state for operation.
    o Reason: The SSL state for the connection is invalid.
    o Solution: Retry connection from the client. If the error continues, report the problem to Service.
  * Message: SSL0111E: Initialization error, Key file label not found.
    o Reason: Certificate or key label specified was not valid.
    o Solution: Verify that the certificate name specified with the SSLServerCert directive is correct or, if no SSLServerCert directive was coded, that a default certificate exists in the key database.
  * Message: SSL0112E: Initialization error, Certificate is not available.
    o Reason: The client did not send a certificate.
    o Solution: Set Client Authentication to optional if a client certificate is not required. Contact the client to determine why it is not sending an acceptable certificate.
  * Message: SSL0113E: Initialization error, Certificate validation error.
    o Reason: The received certificate failed one of the validation checks.
    o Solution: Use another certificate. Contact Service to determine why the certificate failed validation.
  * Message: SSL0114E: Initialization error, Error processing cryptography.
    o Reason: A cryptography error occurred.
    o Solution: None. If the problem continues, report it to Service.
  * Message: SSL0115E: Initialization error, Error validating ASN fields in certificate.
    o Reason: The server was not able to validate one of the ASN fields in the certificate.
    o Solution: Try another certificate.
  * Message: SSL0116E: Initialization error, Error connecting to LDAP server.
    o Reason: The Web server failed to connect to the CRL LDAP server.
    o Solution: Verify that the values entered for the SSLCRLHostname and SSLCRLPort directives are correct. If access to the CRL LDAP server requires authentication, is the SSLCRLUserID directive coded and was the password added to the stash file pointed to by the SSLStashfile directive.

Handshake messages

This topic contains error messages that might result due to Secure Sockets Layer (SSL) handshake failures and provides solutions to help you troubleshoot these problems.
The following messages display due to handshake failures:

  * Message: SSL0117E: Initialization error, Internal unknown error. Report problem to service.
    o Reason: Initialization error, Internal unknown error. Report problem to service.
    o Solution: Initialization error, Internal unknown error. Report problem to service.
  * Message: SSL0118E: Initialization error, Open failed due to cipher error.
    o Reason: Report problem to service.
    o Solution: Report problem to service.
  * Message: SSL0119E: Initialization error, I/O error reading keyfile.
    o Reason: I/O error trying to read SSL keyfile.
    o Solution: Check the file permissions for keyfile.
  * Message: SSL0120E: Initialization error, Keyfile has and invalid internal format. Recreate keyfile.
    o Reason: Initialization error, the keyfile has an invalid internal format. Recreate the keyfile.
    o Solution: Verify the keyfile is not corrupted.
  * Message: SSL0122E: Initialization error, Keyfile has two entries with the same label. Use Ikeyman to remove the duplicate label.
    o Reason: The keyfile has two entries with the same label. Use Ikeyman to remove the duplicate label.
    o Solution: Use Ikeyman to remove the duplicate label.
  * Message: SSL0123E: Initialization error, The keyfile password is used as an integrity check. Either the keyfile has become corrupted or the password is incorrect.
    o Reason: The keyfile password is used as an integrity check. Either the keyfile has become corrupted or the password is incorrect.
    o Solution: Use Ikeyman to verify that the keyfile is valid, check permissions on the stash file, verify

passwords.
* Message: SSL0124E: SSL Handshake Failed, Either the default key in the keyfile has an expired certificate or the keyfile password expired. Use iKeyman to renew or remove certificates that are expired or to set a new keyfile password.
    - Reason: Either the default key in the keyfile has an expired certificate or the keyfile password expired.
    - Solution: Use iKeyman to renew or remove certificates that are expired or to set a new keyfile password.
* Message: SSL0125E: Initialization error, There was an error loading one of the GSK dynamic link libraries. Be sure GSK is installed correctly.
    - Reason: There was an error loading one of the GSK dynamic link libraries. Be sure GSK is installed correctly.
    - Solution: Verify GSK is installed and appropriate level for release of IBM HTTP Server.
* Message: SSL0126S: Handshake Failed, Either the certificate has expired or the system clock is incorrect.
    - Reason: Either the certificate expired or the system clock is incorrect.
    - Solution: Use the key management utility (iKeyman) to recreate or renew your server certificate or change the system date to a valid date.
* Message: SSL0127S: Initialization error, No ciphers specified.
    - Reason: Initialization error, no ciphers specified.
    - Solution: Report problem to service.
* Message: SSL0128S: Initialization error, No certificate.
    - Reason: Initialization error, no certificate.
    - Solution: Report problem to service.
* Message: SSL0129S: Initialization error, The received certificate was formatted incorrectly.
    - Reason: The received certificate is formatted incorrectly.
    - Solution: Use Ikeyman to validate certificates used for connection.
* Message: SSL0130E: Initialization error, Unsupported certificate type.
    - Reason: Unsupported certificate type.
    - Solution: Check certificates that are used for this connection in Ikeyman.
* Message: SSL0131I: Initialization error, I/O error during handshake.
    - Reason: I/O error during handshake.
    - Solution: Check network connectivity.
* Message: SSL0132E: Initialization error, Invalid key length for export.
    - Reason: Invalid key length for export.
    - Solution: Report problem to service.
* Message: SSL0133W: Initialization error, An incorrectly formatted SSL message was received.
    - Reason: An incorrectly formatted SSL message was received.
    - Solution: Check client settings.
* Message: SSL0134W: Initialization error, Could not verify MAC.
    - Reason: Could not verify MAC.
    - Solution: Report problem to service.
* Message: SSL0135W: Initialization error, Unsupported SSL protocol or unsupported certificate type.
    - Reason: Unsupported SSL protocol or unsupported certificate type.
    - Solution: Check server ciphers and certificate settings.
* Message: SSL0136W: Initialization error, Invalid certificate signature.
    - Reason: Invalid certificate signature.
    - Solution: Check certificate in Ikeyman.
* Message: SSL0137W: Initialization error, Invalid certificate sent by partner.
    - Reason: Invalid certificate sent by partner.
    - Solution: If this occurs during an SSL Proxy connection, the remote SSL server sent a bad certificate to IBM HTTP Server. Check the certificate and certificate authority chain at the other end of the SSL connection.
* Message: SSL0138W: Initialization error, Invalid peer.
    - Reason: Invalid peer.
    - Solution: Report problem to service.
* Message: SSL0139W: Initialization error, Permission denied. [AIX Solaris HP-UX Linux Windows]
    - Reason: Permission denied.
    - Solution: Report problem to service.

  [z/OS]
    - Reason: If a System Authorization Facility (SAF) SSL keyring is in use, the current user ID is not authorized to read the keyring.
    - Solution: See the information about access to SAF keyrings in Performing required z/OS system

configurations

* Message: SSL0140W: Initialization error, The self-signed certificate is not valid.
  - Reason: The self-signed certificate is not valid.
  - Solution: Check the certificate in Ikeyman.
* Message: SSL0141E: Initialization error, Internal error - read failed.
  - Reason: Internal error - read failed.
  - Solution: Report to service.
* Message: SSL0142E: Initialization error, Internal error - write failed.
  - Reason: Internal error - write failed.
  - Solution: Report to service.
* Message: SSL0143I: Initialization error, Socket has been closed.
  - Reason: Socket has been closed unexpectedly.
  - Solution: Check the client and network. Report problem to service.
* Message: SSL0144E: Initialization error, Invalid SSLV2 Cipher Spec.
  - Reason: Invalid SSLV2 cipher spec.
  - Solution: Check the SSLCipherSpec directive.
* Message: SSL0145E: Initialization error, Invalid SSLV3 Cipher Spec.
  - Reason: Invalid SSLV3 Cipher Spec.
  - Solution: Check the SSLCipherSpec directive.
* Message: SSL0146E: Initialization error, Invalid security type.
  - Reason: Invalid security type.
  - Solution: Report to service.
* Message: SSL0147E: Initialization error, Invalid security type combination.
  - Reason: Invalid security type combination.
  - Solution: Report to service.
* Message: SSL0148E: Initialization error, Internal error - SSL Handle creation failure.
  - Reason: Internal error - SSL handle creation failure.
  - Solution: Report to service.
* Message: SSL0149E: Initialization error, Internal error - GSK initialization has failed.
  - Reason: Internal error - GSK initialization has failed.
  - Solution: Report to service.
* Message: SSL0150E: Initialization error, LDAP server not available.
  - Reason: LDAP server not available.
  - Solution: Check CRL directives.
* Message: SSL0151E: Initialization error, The specified key did not contain a private key.
  - Reason: The specified key did not contain a private key.
  - Solution: Check the certificate in use in Ikeyman.
* Message: SSL0152E: Initialization error, A failed attempt was made to load the specified PKCS#11 shared library.
  - Reason: A failed attempt was made to load the specified PKCS#11 shared library.
  - Solution: Check SSLPKCSDriver directive and file system.
* Message: SSL0153E: Initialization error, The PKCS#11 driver failed to find the token specified by the caller.
  - Reason: The PKCS#11 driver failed to find the token specified by the caller.
* Message: SSL0154E: Initialization error, A PKCS#11 token is not present for the slot.
  - Reason: A PKCS#11 token is not present for the slot.
  - Solution: Verify PKCS#11 directives.
* Message: SSL0155E: Initialization error, The password/pin to access the PKCS#11 token is invalid.
  - Reason: The password and pin to access the PKCS#11 token is invalid.
* Message: SSL0156E: Initialization error, The SSL header received was not a properly SSLV2 formatted header.
  - Reason: The SSL header received was not a properly SSLV2 formatted header.
* Message: SSL0157E: Initialization error, The function call, %s, has an invalid ID.
  - Reason: The function call, %s, has an invalid ID.
  - Solution: Report problem to service.
* Message: SSL0158E: Initialization error, Internal error - The attribute has a negative length: %s.
  - Reason: Internal error - The attribute has a negative length.
  - Solution: Report problem to service.
* Message: SSL0159E: Initialization error, The enumeration value is invalid for the specified enumeration type: %s.

    - Reason: The enumeration value is invalid for the specified enumeration type: %s.
    - Solution: Report problem to service.
* Message: SSL0160E: Initialization error, The SID cache is invalid: %s.
    - Reason: The SID cache is invalid.
    - Solution: Report problem to service.
* Message: SSL0161E: Initialization error, The attribute has an invalid numeric value: %s.
    - Reason: The attribute has an invalid numeric value: %s.
    - Solution: Check SSL directives.
* Message: SSL0162W: Setting the LD_LIBRARY_PATH or LIBPATH for GSK failed.
    - Reason: Could not update the environment for GSK libraries.
    - Solution: Report problem to service.
* Message: SSL0163W: Setting the LIBPATH for GSK failed, could not append /usr/opt/ibm/gskkm/lib.
    - Reason: Could not append to LD_LIBRARY_PATH or LIBPATH for GSK failed.
    - Solution: Report problem to service.
* Message: SSL0164W: Error accessing Registry, RegOpenKeyEx/RegQueryValueEx returned [%d].
    - Reason: Error accessing registry.
    - Solution: Check GSK installation and windows registry.
* Message: SSL0165W: Storage allocation failed.
    - Reason: Storage allocation failed.
    - Solution: Check memory usage, report problem to service.
* Message: SSL0166E: Failure attempting to load GSK library.
    - Reason: Failure while attempting to load GSK library.
    - Solution: Check the GSK installation.
* Message: SSL0167E: GSK function address undefined.
    - Reason: GSK function address is undefined.
    - Solution: Check the GSK installation and level.
* Message: SSL0168E: SSL initialization for server: %s, port: %u failed due to a configuration error.
    - Reason: Iinitialization for server: %s, port: %u failed due to a configuration error.
    - Solution: Check the SSL configuration.
* Message: SSL0169E: Keyfile does not exist: %s.
    - Reason: Keyfile does not exist.
    - Solution: Check to ensure the path that is provided to the KeyFile directive exists, and is readable by the user that IBM HTTP Server is running as.
* Message: SSL0170E: GSK could not initialize, no keyfile specified.
    - Reason: Keyfile is not specified.
    - Solution: Specify Keyfile directive.
* Message: SSL0171E: CRL cannot be specified as an option for the SSLClientAuth directive on HPUX because the IBM HTTP Server does not support CRL on HPUX.
    - Reason: CRL cannot be specified as an option for the SSLClientAuth directive on HPUX because IBM HTTP Server does not support CRL on HPUX.
    - Solution: Remove CRL directives.
* Message: SSL0172E: If CRL is turned on, you must specify an LDAP hostname for the SSLCRLHostname directive.
    - Reason: If CRL is turned on, you must specify an LDAP hostname for the SSLCRLHostname directive.
    - Solution: Specify SSLCRLHostname.
* Message: SSL0173E: Failure obtaining supported cipher specs from the GSK library.
    - Reason: Failure obtaining supported cipher specs from the GSK library.
    - Solution: Check the GSK installation, report problem to service.
* Message: SSL0174I: No CRL password found in the stash file: %s.
    - Reason: No CRL password is found in the stash file: %s.
    - Solution: Check the stash file permissions, regenerate stash file.
* Message: SSL0174I: No CRYPTO password found in the stash file: %s.
    - Reason: No CRYPTO password is found in the stash file: %s.
    - Solution: Check stash file permissions, regenerate stash file.
* Message: SSL0175E: fopen failed for stash file: %s.
    - Reason: fopen failed for stash file.
    - Solution: Check stash file permissions, regenerate stash file.
* Message: SSL0176E: fread failed for the stash file: %s.
    - Reason: fread failed for the stash file.

    o Solution: Make sure the stash file is readable by user IBM HTTP Server is running as.
  * Message: SSL0179E: Unknown return code from stash_recover(), %d.
    o Reason: Unknown return code from stash_recover(), %d.
    o Solution: Check the stash file.
  * Message: SSL0181S: Unable to fork for startup of session ID cache.
    o Reason: Unable to fork for startup of session ID cache.
    o Solution: Check the location of sidd daemon, file permissions.
  * Message: SSL0182E: Error creating file mapped memory for SSL passwords.
    o Reason: Error creating file mapped memory for SSL passwords.
    o Solution: Report problem to service.
  * Message: SSL0183E: Exceeded map memory limits.
    o Reason: Exceeded map memory limits.
    o Solution: Report problem to service.
  * Message: SSL0184E: Could not find a password for the resource: %s.
    o Reason: SSL0184E: Could not find a password for the resource: %s.
    o Solution: Report problem to service, disable password prompting.
  * Message: SSL0185E: ssl_getpwd() failed, unable to obtain memory.
    o Reason: ssl_getpwd() failed, unable to obtain memory.
    o Solution: Report problem to service, disable password prompting.
  * Message: SSL0186E: Linked list mismatch.
    o Reason: SSL0186E: Linked list mismatch.
    o Solution: Report problem to service, disable password prompting.
  * Message: SSL0186E: ssl_getpwd() failed, password exceeded maximum size of 4095.
    o Reason: ssl_getpwd() failed, password exceeded the maximum size of 4095.
    o Solution: The password must be smaller than 4K.
  * Message: SSL0187E: It is invalid to enable password prompting for the SSLServerCert directive without specifying a Crypto Card Token.
    o Reason: It is invalid to enable password prompting for the SSLServerCert directive without specifying a crypto card token.
    o Solution: Specify a crypto card token or disable password prompting for the SSLServerCert directive.
  * Message: SSL0200E: Handshake Failed, <code>.
    o Reason: The handshake failed when the SSL library returned an unknown error.
    o Solution: None. Report this problem to Service.
  * Message: SSL0201E: Handshake Failed, Internal error - Bad handle.
    o Reason: An internal error has occurred.
    o Solution: Report this problem to Service.
  * Message: SSL0202E: Handshake Failed, The GSK library unloaded.
    o Reason: A call to the GSKit function failed because the dynamic link library unloaded (Windows operating systems only).
    o Solution: Shut down the server and restart.
  * Message: SSL0203E: Handshake Failed, GSK internal error.
    o Reason: The communication between client and the server failed due to an error in the GSKit library.
    o Solution: Retry connection from the client. If the error continues, report the problem to Service.
  * Message: SSL0204E: Handshake Failed, Internal memory allocation failure.
    o Reason: The server could not allocate memory needed to complete the operation.
    o Solution: Take action to free up some additional memory. Try reducing the number of threads or processes running, or increasing virtual memory.
  * Message: SSL0205E: Handshake Failed, GSK handle is in an invalid state for operation.
    o Reason: The SSL state for the connection is invalid.
    o Solution: Retry connection from the client. If the error continues, report the problem to Service.
  * Message: SSL0206E: Handshake Failed, Key-file label not found
    o Reason: The label specified for the SSLServerCert directive was not found in the key database (KDB) file specified for the KeyFile directive.
    o Solution: Specify a value for the SSLServerCert directive that corresponds to a personal certificate available in the KDB file specified for the KeyFile directive
  * Message: SSL0207E: Handshake Failed, Certificate is not available.
    o Reason: The client did not send a certificate.
    o Solution: Set client authentication to optional if a client certificate is not required. Contact the client to determine why it is not sending an acceptable certificate.

* Message: SSL0208E: Handshake Failed, Certificate validation error.
    - Reason: The received certificate failed one of the validation checks.
    - Solution: Use another certificate. Contact Service to determine why the certificate failed validation.
* Message: SSL0209E: Handshake Failed, ERROR processing cryptography.
    - Reason: A cryptography error occurred.
    - Solution: None. If the problem continues, report it to Service.
* Message: SSL0210E: Handshake Failed, ERROR validating ASN fields in certificate.
    - Reason: The server was not able to validate one of the ASN fields in the certificate.
    - Solution: Try another certificate.
* Message: SSL0211E: Handshake Failed, ERROR connecting to LDAP server.
    - Reason: The Web server failed to connect to the CRL LDAP server.
    - Solution: Verify that the values entered for the SSLCRLHostname and SSLCRLPort directives are correct. If access to the CRL LDAP server requires authentication, is the SSLCRLUserID directive coded and was the password added to the stash file pointed to by the SSLStashfile directive.
* Message: SSL0212E: Handshake Failed, Internal unknown error.
    - Report problem to Service. Reason: An unknown error has occurred in the SSL library.
    - Solution: Report the problem to Service.
* Message: SSL0213E: Handshake Failed, Open failed due to cipher error.
    - Reason: An unknown error has occurred in the SSL library.
    - Solution: Report the problem to Service.
* Message: SSL0214E: Handshake Failed, I/O error reading key file.
    - Reason: The server could not read the key database file.
    - Solution: Check file access permissions and verify the Web server user ID is allowed access.
* Message: SSL0215E: Handshake Failed, Key file has an invalid internal format. Recreate key file.
    - Reason: Key file has an invalid format.
    - Solution: Recreate key file.
* Message: SSL0216E: Handshake Failed, Key file has two entries with the same key. Use IKEYMAN to remove the duplicate key.
    - Reason: Two identical keys exist in key file.
    - Solution: Use IKEYMAN to remove duplicate key.
* Message: SSL0217E: Handshake Failed, Key file has two entries with the same label. Use IKEYMAN to remove the duplicate label.
    - Reason: A second certificate with the same label was placed in the key database file.
    - Solution: Use IKEYMAN to remove duplicate label.
* Message: SSL0218E: Handshake failed, Either the key file has become corrupted or the password is incorrect.
    - Reason: The key file password is used as an integrity check and the test failed. Either the key database file is corrupted, or the password is incorrect.
    - Solution: Use IKEYMAN to stash the key database file password again. If that fails, recreate the key database.
* Message: SSL0219E: SSL Handshake Failed, Either the default key in the keyfile has an expired certificate or the keyfile password expired. Use iKeyman to renew or remove certificates that are expired or to set a new keyfile password.
    - Reason: Either the default key in the keyfile has an expired certificate or the keyfile password expired.
    - Solution: Use iKeyman to renew or remove certificates that are expired or to set a new keyfile password.
* Message: SSL0220E: Handshake Failed, There was an error loading one of the GSKdynamic link libraries. Be sure GSK was installed correctly.
    - Reason: Opening the SSL environment resulted in an error because one of the GSKdynamic link libraries could not load.
    - Solution: Contact Support to make sure the GSKit is installed correctly.
* Message: SSL0221E: Handshake Failed. Either the certificate has expired or the system clock is incorrect.
    - Reason: Either the certificate expired or the system clock is incorrect.
    - Solution: Use the key management utility (iKeyman) to recreate or renew your server certificate or change the system date to a valid date.
* Message: SSL0222W: Handshake failed, no ciphers specified.
    - Reason: SSLV2 and SSLV3 are disabled.
    - Solution: None. Report this problem to Service.
* Message: SSL0223E: Handshake Failed, No certificate.
    - Reason: The client did not send a certificate.

You can also see this message when your keyfile does not have a default certificate specified and you have not specified an SSLServerCert directive. It will pass initialization but fail at connection (handshake) time.
    - Solution: Set client authentication to optional if a client certificate is not required. Contact the client to determine why it is not sending a certificate.
* Message: SSL0224E: Handshake failed, Invalid or improperly formatted certificate.
    - Reason: The client did not specify a valid certificate.
    - Solution: Client problem.
* Message: SSL0225E: Handshake Failed, Unsupported certificate type.
    - Reason: The certificate type received from the client is not supported by this version of IBM HTTP Server SSL.
    - Solution: The client must use a different certificate type.
* Message: SSL0226I: Handshake Failed, I/O error during handshake.
    - Reason: The communication between the client and the server failed. This is a common error when the client closes the connection before the handshake has completed.
    - Solution: Retry the connection from the client.
* Message: SSL0227E: Handshake Failed, Specified label could not be found in the key file.
    - Reason: Specified key label is not present in key file.
    - Solution: Check that the SSLServerCert directive is correct, if coded, and that the label is valid for one of the keys in the key database.
* Message: SSL0228E: Handshake Failed, Invalid password for key file.
    - Reason: The password retrieved from the stash file could not open the key database file.
    - Solution: Use IKEYMAN to open the key database file and recreate the password stash file. This problem can also result from a corrupted key database file. Creating a new key database file may resolve the problem.
* Message: SSL0229E: Handshake Failed, Invalid key length for export.
    - Reason: In a restricted cryptography environment, the key size is too long to be supported.
    - Solution: Select a certificate with a shorter key.
* Message: SSL0230I: Handshake Failed, An incorrectly formatted SSL message was received.
* Message: SSL0231W: Handshake Failed, Could not verify MAC.
    - Reason: The communication between the client and the server failed.
    - Solution: Retry the connection from the client.
* Message: SSL0232W: Handshake Failed, Unsupported SSL protocol or unsupported certificate type.
    - Reason: The communication between the client and the server failed because the client is trying to use a protocol or certificate which the IBM HTTP Server does not support.
    - Solution: Retry the connection from the client using an SSL Version 2 or 3, or TLS 1 protocol. Try another certificate.
* Message: SSL0233W: Handshake Failed, Invalid certificate signature.
* Message: SSL0234W: Handshake Failed, Invalid certificate sent by partner.
    - Reason: The partner did not specify a valid certificate. The server is acting as a reverse proxy to an SSL URL and the _server_ cert could not be validated.
    - Solution: Partner problem. If this occurs during an SSL Proxy connection, the remote SSL server sent a bad certificate to IBM HTTP Server. Check the certificate and certificate authority chain at the other end of the SSL connection. For more information, see Securing with SSL communications.
* Message: SSL0235W: Handshake Failed, Invalid peer.
* Message: SSL0236W: Handshake Failed, Permission denied.
* Message: SSL0237W: Handshake Failed, The self-signed certificate is not valid.
* Message: SSL0238E: Handshake Failed, Internal error - read failed.
    - Reason: The read failed.
    - Solution: None. Report this error to Service.
* Message: SSL0239E: Handshake Failed, Internal error - write failed.
    - Reason: The write failed.
    - Solution: None. Report this error to Service.
* Message: SSL0240I: Handshake Failed, Socket has been closed.
    - Reason: The client closed the socket before the protocol completed.
    - Solution: Retry connection between client and server.
* Message: SSL0241E: Handshake Failed, Invalid SSLV2 Cipher Spec.
    - Reason: The SSL Version 2 cipher specifications passed into the handshake were invalid.
    - Solution: Change the specified Version 2 cipher specs.

* Message: SSL0242E: Handshake Failed, Invalid SSLV3 Cipher Spec.
    - Reason: The SSL Version 3 cipher specifications passed into the handshake were invalid.
    - Solution: Change the specified Version 3 cipher specs.
* Message: SSL0243E: Handshake Failed, Invalid security type.
    - Reason: There was an internal error in the SSL library.
    - Solution: Retry the connection from the client. If the error continues, report the problem to Service.
* Message: SSL0245E: Handshake Failed, Internal error - SSL Handle creation failure.
    - Reason: There was an internal error in the security libraries.
    - Solution: None. Report this problem to Service.
* Message: SSL0246E: Handshake Failed, Internal error - GSK initialization has failed.
    - Reason: An error in the security library has caused SSL initialization to fail.
    - Solution: None. Report this problem to Service.
* Message: SSL0247E: Handshake Failed, LDAP server not available.
    - Reason: Unable to access the specified LDAP directory when validating a certificate.
    - Solution: Check that the SSLCRLHostname and SSLCRLPort directives are correct. Make sure the LDAP server is available.
* Message: SSL0248E: Handshake Failed, The specified key did not contain a private key.
    - Reason: The key does not contain a private key.
    - Solution: Create a new key. If this was an imported key, include the private key when doing the export.
* Message: SSL0249E: Handshake Failed, A failed attempt was made to load the specified PKCS#11 shared library.
    - Reason: An error occurred while loading the PKCS#11 shared library.
    - Solution: Verify that the PKCS#11 shared library specified in the SSLPKCSDriver directive is valid.
* Message: SSL0250E: Handshake Failed, The PKCS#11 driver failed to find the token label specified by the caller.
    - Reason: The specified token was not found on the PKCS#11 device.
    - Solution: Check that the token label specified on the SSLServerCert directive is valid for your device.
* Message: SSL0251E: Handshake Failed, A PKCS#11 token is not present for the slot.
    - Reason: The PKCS#11 device has not been initialized correctly.
    - Solution: Specify a valid slot for the PKCS#11 token or initialize the device.
* Message: SSL0252E: Handshake Failed, The password/pin to access the PKCS#11 token is either not present, or invalid.
    - Reason: Specified user password and pin for PKCS#11 token is not present or invalid.
    - Solution: Check that the correct password was stashed using the SSLStash utility and that the SSLStashfile directive is correct.
* Message: SSL0253E: Handshake Failed, The SSL header received was not a properly SSLV2 formatted header.
    - Reason: The data received during the handshake does not conform to the SSLV2 protocol.
    - Solution: Retry connection between client and server. Verify that the client is using HTTPS.
* Message: SSL0254E: Internal error - I/O failed, buffer size invalid.
    - Reason: The buffer size in the call to the I/O function is zero or negative.
    - Solution: None. Report this problem to Service.
* Message: SSL0255E: Handshake Failed, Operation would block.
    - Reason: The I/O failed because the socket is in non-blocking mode.
    - Solution: None. Report this problem to Service.
* Message: SSL0256E: Internal error - SSLV3 is required for reset_cipher, and the connection uses SSLV2.
    - Reason: A reset_cipher function was attempted on an SSLV2 connection.
    - Solution: None. Report this problem to Service.
* Message: SSL0257E: Internal error - An invalid ID was specified for the gsk_secure_soc_misc function call.
    - Reason: An invalid value was passed to the gsk_secure_soc_misc function.
    - Solution: None. Report this problem to Service.
* Message: SSL0258E: Handshake Failed, The function call, <function>, has an invalid ID.
    - Reason: An invalid function ID was passed to the specified function.
    - Solution: None. Report this problem to Service.
* Message: SSL0259E: Handshake Failed, Internal error - The attribute has a negative length in: <function>.
    - Reason: The length value passed to the function is negative, which is invalid.
    - Solution: None. Report this problem to Service.
* Message: SSL0260E: Handshake Failed, The enumeration value is invalid for the specified enumeration type in: <function>.

    o Reason: The function call contains an invalid function ID.
    o Solution: None. Report this problem to Service.
  * Message: SSL0261E: Handshake Failed, The SID cache is invalid: <function>.
    o Reason: The function call contains an invalid parameter list for replacing the SID cache routines.
    o Solution: None. Report this problem to Service.
  * Message: SSL0262E: Handshake Failed, The attribute has an invalid numeric value: <function>.
    o Reason: The function call contains an invalid value for the attribute being set.
    o Solution: None. Report this problem to Service.
  * Message: SSL0263W: SSL Connection attempted when SSL did not initialize.
    o Reason: A connection was received on an SSL-enabled virtual host but it could not be completed because there was an error during SSL initialization.
    o Solution: Check for an error message during startup and correct that problem.
  * Message: SSL0264E: Failure obtaining Cert data for label <certificate>.
    o Reason: A GSKit error prevented the server certificate information from being retrieved.
    o Solution: Check for a previous error message with additional information.
  * Message: SSL0265W: Client did not supply a certificate.
    o Reason: A client who connected failed to send a client certificate and the server is configured to require a certificate.
    o Solution: Nothing on the server side.
  * Message: SSL0266E: Handshake failed.
    o Reason: Could not establish SSL proxy connection.
    o Solution: IBM HTTP Server could not establish a proxy connection to a remote server using SSL.
  * Message: SSL0267E: SSL Handshake failed.
    o Reason: Timeout on network operation during handshake.
    o Solution: Check client connectivity, adjust TimeOuts.

Configuration messages

This topic contains error messages that might result due to configuration problems and provides solutions to help you troubleshoot these problems.
The following messages appear due to configuration problems:

  * Message: SSL0300E: Unable to allocate terminal node.
  * Message: SSL0301E: Unable to allocate string value in node.
  * Message: SSL0302E: Unable to allocate non terminal node.
  * Message: SSL0303E: Syntax Error in SSLClientAuthGroup directive.
  * Message: SSL0304E: Syntax Error in SSLClientAuthRequire directive.
  * Message: SSL0307E: Invalid token preceding NOT or !
  * Message: SSL0308E: A group is specified in SSLClientAuthRequire but no groups are specified.
  * Message: SSL0309E: The group <group> is specified in SSLClientAuthRequire is not defined.
  * Message: SSL0310I: Access denied to object due to invalid SSL version <version>, expected <version>.
  * Message: SSL0311E: Unable to get cipher in checkBanCipher.
  * Message: SSL0312I: Cipher <cipher> is in ban list and client is forbidden to access object.
  * Message: SSL0313E: Fell through to default return in checkCipherBan.
  * Message: SSL0314E: Cipher is NULL in checkRequireCipher.
  * Message: SSL0315E: Cipher <cipher> used is not in the list of required ciphers to access this object.
  * Message: SSL0316E: Fell through to default return in checkCipherRequire.
  * Message: SSL0317E: Unable to allocate memory for fake basic authentication username.
  * Message: SSL0318E: Limit exceeded for specified cipher specs, only 64 total allowed.
    o Reason: The number of ciphers configured using the SSLCipherSpec directive exceeds the maximum allowed of 64.
    o Solution: Check for duplicate SSLCipherSpec directives.
  * Message: SSL0319E: Cipher Spec <cipher> is not supported by this GSK library.
    o Reason: The cipher is not a valid cipher for use with the installed SSL libraries.
    o Solution: Check that a valid cipher value was entered with the SSLCipherSpec directive.
  * Message: SSL0320I: Using Version 2|3 Cipher: <cipher>.

    - Reason: This is an informational message listing the ciphers used for connections to this virtual host.
    - Solution: None.
* Message: SSL0321E: Invalid cipher spec <cipher>.
    - Reason: The cipher is not a valid cipher.
    - Solution: Check the documentation for a list of valid cipher specs.
* Message: SSL0322E: Cipher Spec <cipher> is not valid.
    - Reason: The cipher is not a valid cipher.
    - Solution: Check the documentation for a list of valid cipher specs.
* Message: SSL0323E: Cipher Spec <cipher> has already been added.
    - Reason: A duplicate SSLCipherSpec directive has been encountered.
    - Solution: This instance of the directive is ignored and should be removed from the configuration file.
* Message: SSL0324E: Unable to allocate storage for cipher specs.
    - Reason: The server could not allocate memory needed to complete the operation.
    - Solution: Take action to free up some additional memory. Try reducing the number of threads or processes running, or increasing virtual memory.
* Message: SSL0325E: Cipher Spec <cipher> has already been added to the v2|v3 ban|require list.
    - Reason: A duplicate cipher was specified on the SSLCipherBan directive.
    - Solution: This instance of the directive is ignored and should be removed from the configuration file.
* Message: SSL0326E: Invalid cipher spec <cipher> set for SSLCipherBan|SSLCipherRequire.
    - Reason: The cipher is not a valid cipher.
    - Solution: Check the documentation for a list of valid cipher specs.
* Message: SSL0327E: Invalid value for sslv2timeout|sslv3timeout, using default value of nn seconds.
    - Reason: The timeout value specified is not in the valid range.
    - Solution: Check the documentation for the proper range of values.
* Message: SSL0328W: Invalid argument for SSLClientAuth: <args>. CRL can not be turned on unless Client Authentication is on.
* Message: SSL0329W: Invalid argument for SSLClientAuth: <args>. If a second argument is entered it must be CRL. CRL cannot be turned on unless client authentication is on.
* Message: SSL0330W: Invalid argument for SSLClientAuth: <args>. If a second value is entered it must be crl.
* Message: SSL0331W: Invalid argument for SSLClientAuth: <args>. The first value must be 0, 1, 2 none, optional, or required.
* Message: SSL0332E: Not enough arguments specified for SSLClientAuthGroup.
* Message: SSL0333E: No parse tree created for <parm>.
    - Reason: An error occurred processing the SSLClientAuthRequire directive.
    - Solution: Check for other error messages. Enable tracing of Client Authentication by adding the directive SSLClientAuthRequireTraceOn to the configuration file.
* Message: SSL0334E: Function ap_make_table failed processing label <certificate>.
* Message: SSL0337E: OCSP is not supported with this level of GSKit
    - Reason: OCSP support requires GSKit 7.0.4.14 or higher
    - Solution: Upgrade the level of GSKit on the system to 7.0.4.14 or higher

Cache messages

This topic contains error messages that might result due to caching problems and provides a solution to help you troubleshoot the problem.
The following messages are displayed due to caching problems:

* Message: SSL0600S: Unable to connect to session ID cache
    - Reason: The server cannot connect to the Session ID caching daemon.
    - Solution: Verify that the daemon successfully started.
* Message: SSL0601E: Session ID cache daemon process <process-id> exited with exit code <exit-code>; restarting
    - Reason: If the value of <exit-code> is 0, the session ID cache daemon (sidd) received the SIGTERM signal. Other exit codes are not expected. Sidd automatically restarted.
    - Solution: If the value of <exit-code> is 0 and IBM HTTP Server did not stop or restart, verify that locally

installed CGI scripts, scheduled operating system tasks, or other monitoring software cannot send SIGTERM to sidd.

* Message: SSL0602E: Session ID cache daemon process <process-id> exited with terminating signal <signal-number>; restarting
    - Reason: The session ID cache daemon (sidd) received a signal other than SIGTERM was received by the session ID cache daemon (sidd), which caused it to exit. Sidd automatically restarted.
    - Solution: If the value of <exit-code> is 0 and IBM HTTP Server did not stop or restart, verify that locally installed CGI scripts, scheduled operating system tasks, or other monitoring software cannot send the signal to sidd.

* Message: SSL0603E: Session ID cache daemon process <process-id> exited with exit code<exit-code>; not restarting; check sidd configuration or enable sidd error log with SSLCacheErrorLog
    - Reason: The session ID cache daemon (sidd) did not initialize. The following possible exit code values might be displayed:

Value	Reason
2	Log files could not be opened. The SSLCacheTraceLog or the SSLCacheErrorLog directive is not valid.
3	The AF_UNIX socket cannot be initialized. Use the SSLCachePortFilename directive to specify a different socket for the session ID cache daemon.
4	Sidd cannot switch to the configured user and group. Verify the values for the user and group directives.

    - Solution: Provide a valid value for the directives and restart IBM HTTP Server.

SSL Key Management

Using the gsk7cmd command

To run IKEYCMD using the gsk7cmd command, set up environmental variables. Set your PATH to the location of your Java or JRE executable as follows:

```
export PATH=/opt/IBMJava/bin:/usr/local/ibm/gsk7/bin:$PATH
```

The gsk7cmd command should run from any directory using the following syntax:

gsk7cmd command - where command is the required command name.

gsk7cmd Syntax

To run IKEYCMD using the gsk7cmd command you must set the PATH environmental variable to the location of your Java or JRE executable as follows. For more information, see Using the gsk7cmd command.

The syntax of the Java command line interface follows.

java [-Dikeycmd.properties=<*properties_file*>] com.ibm.gsk.ikeyman.ikeycmd <*object*> <*action*> *[options]*

Where:

- -Dikeycmd.properties specifies the name of an optional properties file to use for this Java invocation. A default properties file, ikeycmd.properties, exists as a sample file that you can modify and use with any Java application.
- object includes one of the following:
    - -keydb: Actions taken on the key database (either a CMS key database file, a WebDB key ring file, or SSLight class)
    - -cert: Actions taken on a certificate
    - -certreq: Actions taken on a certificate request
    - -help: Displays help for the IKEYCMD invocations
    - -version: Displays version information for IKEYCMD

The action represents the specific action to take on the object, and options represents the options, both required and optional, specified for the object and action pair.

The object and action keywords are positional and you must specify them in the selected order. However, options are not positional and you can specify them in any order, as an option and operand pair.

The following table describes each action **possible on a specified** object **that you can use with the gsk7cmd command** .

Object	Actions	Description
-keydb	-changepw	Change the password for a key database
	-convert	Convert a key database from one format to another
	-create	Create a key database
	-delete	Delete the key database
	-stashpw	Stash the password of a key database into a file
-cert	-add	Add a CA certificate from a file into a key database
	-create	Create a self-signed certificate
	-delete	Delete a CA certificate
	-export	Export a personal certificate and its associated private key from a key database into a PKCS#12 file, or to another key database
	-extract	Extract a certificate from a key database
	-getdefault	Get the default personal certificate
	-import	Import a certificate from a key database or PKCS#12 file
	-list	List all certificates
	-modify	Modify a certificate. (Currently the only field you can modify is the **Certificate trust** field)
	-receive	Receive a certificate from a file into a key database
	-setdefault	Set the default personal certificate
	-sign	Sign a certificate stored in a file with a certificate stored in a key database and store the resulting signed certificate in a file
-certreq	-create	Create a certificate request
	-delete	Delete a certificate request from a certificate request database
	-details	List the detailed information of a specific certificate request
	-extract	Extract a certificate request from a certificate request database into a file
	-list	List all certificate requests in the certificate request database
	-recreate	Recreate a certificate request
-help		Display help information for the IKEYCMD command
-version		Display IKEYCMD version informatoin

The following table describes the options **that you can use with the gsk7cmd command**.

Option	Description
dB	Fully qualified path name of a key database
-default_cert	Sets a certificate to use as the default certificate for client authentication (yes or no). Default is no.

-dn	X.500 distinguished name. Input as a quoted string of the following format (only CN, O, and C are required): "CN=Jane Doe,O=IBM,OU=Java Development,L=Endicott, ST=NY,ZIP=13760,C=country"
encryption	Strength of encryption used in certificate export command (strong or weak). Default is strong.
-expire	Expiration time of either a certificate or a database password (in days). Defaults are: 365 days for a certificate and 60 days for a database password.
-file	File name of a certificate or certificate request (depending on specified object).
-format	Format of a certificate (either ASCII for Base64_encoded ASCII or binary for Binary DER data). Default is ASCII.
-label	Label attached to a certificate or certificate request
-new_format	New format of key database
-new_pw	New database password
-old_format	Old format of key database
-pw	Password for the key database or PKCS#12 file. See Creating a new key database.
-size	Key size (512 or 1024). Default is 1024.
-stash	Indicator to stash the key database password to a file. If specified, the password will be stashed in a file.
-target	Destination file or database
-target_pw	Password for the key database if -target specifies a key database. See Creating a new key database.
-target_type	Type of database specified by -target operand (see -type)
-trust	Trust status of a CA certificate (enable or disable). Default is enable.
-type	Type of database. Allowable values are CMS (indicates a CMS key database), webdb (indicates a keyring), sslight (indicates an SSLight .class), or pkcs12 (indicates a PKCS#12 file).
-x509version	Version of X.509 certificate to create (1, 2 or 3). Default is 3.