Using the ikeycmd CLI to add the key, intermediate, and root certificates to the CDWS Keystore databases – ssl-server.jks and trustedkeystore.jks.

I. The 'ikeycmd' information presented is condensed from the IBM Key Manager User's Guide available here.
IBM Key Manager User's Guide.

II. The ikeycmd executable is located here.
/<cdws_install_path>/MFTWebServices/jre/bin

III. You **MUST** know the password for the Keystore databases to use these commands. The default password for both Keystores is 'changeit'. The Keystore passwords are **not** recoverable.

1. **If you have lost or forgotten the Keystore password, you can create a new Keystore database.**
   ikeycmd -keydb -create -db */<cdws_install_path>/*MFTWebServices/mftws/BOOT-INF/classes/[ssl-server.jks|trustedkeystore.jks] -pw *<keystore_password>* -type jks

2. You can change the default Keystore passwords using the following command.
   ikeycmd -keydb -changepw -db */<cdws_install_path>/*MFTWebServices/mftws/BOOT-INF/classes/[ssl-server.jks|trustedkeystore.jks] -pw *<keystore_password>* -new_pw *<new_keystore_password>* -type jks

A. Create a Certificate Signing Request (CSR).

NOTE: The "-label" and "-file" name values used in the following commands are examples. It is highly suggested that the values you choose for labels and file names be very descriptive to explicitly identify the object you are creating.

Navigate to the folder containing ikeycmd.
/<cdws_install_path>/MFTWebServices/jre/bin

ikeycmd -certreq -create -db */<cdws_install_path>/*MFTWebServices/mftws/BOOT-INF/classes/ssl-server.jks -label *<new_keycert_yyyymmdd>* -file */<your_certificate_folder>/<new_certreq_yyyymmdd.pem>* -pw *<keystore_password>* -dn "CN=*<cdws_server_name.your_domain.com>*, OU=*<your_department>*, O=*<your_company>*, L=*<your_city>*, ST=*<your_state(2-char)>*, POSTALCODE=*<your_zipcode>*, C=*<your_country(2-char)>*" -size 2048 -sig_alg SHA256WithRSA

If you wish to use an ECDSA certificate, then you can use the following "-size" and "-sig_alg" combinations.

-size 256 -sig_alg SHA256WithECDSA
-size 384 -sig_alg SHA384WithECDSA
-size 521 -sig_alg SHA512WithECDSA

Ensure that you tell your CA that you are using ECDSA. The signing process is different for ECDSA.

Optional "Subject Alternative Names" can also be added and used with the CSR. Add to the end of the command string.

-san_dnsname *<dns_name_of_server>*
-san_emailaddr *<email_of_server_admin>*
-san_ipaddr *<ip_address_of_server>*

B. Send the 'new_certreq_yyyymmdd.pem' file to your Certificate Authority (CA). From the CA, request an Apache style, x509, base64 encoded, PEM format signed server (public) certificate. Also, get the Root and Intermediate certificates in PEM format from the CA.

C. Add the Root and Intermediate Certificates from the CA to the trustedkeystore.jks Keystore.

If the certificates are in separate files, you can specify your own labels.

ikeycmd -cert -add -db */<cdws_install_path>/*MFTWebServices/mftws/BOOT-INF/classes/trustedkeystore.jks -file *<trusted_cert_from_CA.pem>* -label *<your_choice_of_label>* -pw *<keystore_password>* -trust enable

If the certificates are bundled in a single file, the certificates' 'CN' value will be used for the labels.

ikeycmd -cert -add -db */<cdws_install_path>/* MFTWebServices/mftws/BOOT-INF/classes/trustedkeystore.jks -file *<trusted_cert_from_CA.pem>* -pw *<keystore_password>* -trust enable

D. Receive the Signed Server (Public) Certificate into the ssl-server.jks Keystore to create the Key Certificate.

ikeycmd -cert -receive -db */<cdws_install_path>/*MFTWebServices/mftws/BOOT-INF/classes/ssl-server.jks -file *<signed_cert_from_CA.pem>* -pw *<keystore_password>* -format ascii -default_cert yes

The label used for the Key Certificate will be the same as the label used for creating the CSR.

E. You will add the root and intermediate certificates to your Connect:Direct servers' Keystores.

F. You will now need to update CDWS to use the new certificates.
Follow the instructions given at this link to complete this step.
Do Option 1 – Change Keystore and Option 2 – Change Truststore.

Update CDWS with new certificate information

1. **If you did not change the Keystore passwords or create new Keystores, then you only need to do Steps 3 and 4 from the instructions at this link.**

NOTE: The "-label" and "-file" name values used in the above commands are examples. It is highly suggested that the values you choose for labels and file names be very descriptive to explicitly identify the object you are creating.

Renew An Existing Key Certificate That Is About To Expire.

NOTE: This will not work if the Key Certificate is already expired. If the Key Certificate is already expired, you will need to start over with a new Certificate Signing Request.

A. View the details of the current default key certificate. Note the label of the key certificate.

ikeycmd -cert -getdefault -db */<cdws_install_path>*/MFTWebServices/mftws/BOOT-INF/classes/ssl-server.jks -pw *<keystore_password>*

B. Recreate the Certificate Signing Request from the existing key certificate.

ikeycmd -certreq -recreate -db */<cdws_install_path>*/MFTWebServices/mftws/BOOT-INF/classes/ssl-server.jks -label *<current_key_certificate_label>* -target */<your_certificate_folder>/<current_key_certificate_label.pem>* -pw *<keystore_password>*

C. Send the 'renew certificate request' file to your Certificate Authority (CA). From the CA, request an Apache style, x509, base64 encoded, PEM format signed server (public) certificate.
Also get the updated Root and Intermediate certificates from the CA if needed and add into the trustedkeystore.jks Keystore.
If you received updated Root and Intermediate certificates from your CA, you will need to add these to your Connect:Direct Servers' Keystores.

D. Receive the renewed Signed Server (Public) Certificate into the Keystore to update the Key Certificate.

ikeycmd -cert -receive -db */<cdws_install_path>/*MFTWebServices/mftws/BOOT-INF/classes/ssl-server.jks -file *<renewed_signed_cert_from_CA.pem>* -pw *<keystore_password>* -format ascii -default_cert yes

E. Verify the new validity date of the key certificate.

ikeycmd -cert -getdefault -db */<cdws_install_path>/*MFTWebServices/mftws/BOOT-INF/classes/ssl-server.jks -pw *<keystore_password>*

Look for the **"Valid: From:"** line in the output. Verify the validity date.

Viewing Certificates in the Keystore.

A. View all certificates in the Keystore.

./ikeycmd -cert -list -db */<cdws_install_path>/*MFTWebServices/mftws/BOOT-INF/classes/[ssl-server.jks|trustedkeystore.jks] -pw *<keystore_password>*

B. View details of the default key certificate.

./ikeycmd -cert -getdefault -db */<cdws_install_path>/*MFTWebServices/mftws/BOOT-INF/classes/ssl-server.jks -pw *<keystore_password>*

C. View details of any certificate in the Keystore.

./ikeycmd -cert -details -db */<cdws_install_path>/*MFTWebServices/mftws/BOOT-INF/classes/[ssl-server.jks|trustedkeystore.jks] -label *<certificate_label>* -pw *<keystore_password>*

D. Validate a key certificate.

./ikeycmd -cert -validate -db */<cdws_install_path>/*MFTWebServices/mftws/BOOT-INF/classes/ssl-server.jks -label *<certificate_label>* -pw *<keystore_password>*

PEM Certificate Format.

1. When a PEM format key certificate is opened in Notepad, it looks like this.

```
-----BEGIN ENCRYPTED PRIVATE KEY-----
MIIFHzBJBgkqhkiG9w0BBQ0wPDAbBgkqhkiG9w0BBQwwDgQIms5GmoGpBfgCAggA
.
.
6xEr6w1nfXKZaVWouj+Yn7PZNQ==
-----END ENCRYPTED PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIIF1TCCA72gAwIBAgICEA0wDQYJKoZIhvcNAQELBQAwazELMAkGA1UEBhMCVVMx
.
.
XnkM8DrNyV7p
-----END CERTIFICATE-----
```

2. When a PEM format root or intermediate certificate is opened in Notepad, it looks like this.

```
-----BEGIN CERTIFICATE-----
MIIF1zCCA7+gAwIBAgICEA4wDQYJKoZIhvcNAQELBQAwazELMAkGA1UEBhMCVVMx
.
.
+u0BTWnw8KhQPhyBqxhbzfc9mK2dO0ChYIUjsCC445py4904HKJmRXNdZ
JJsf06EfgsZir+Q=
-----END CERTIFICATE-----
```