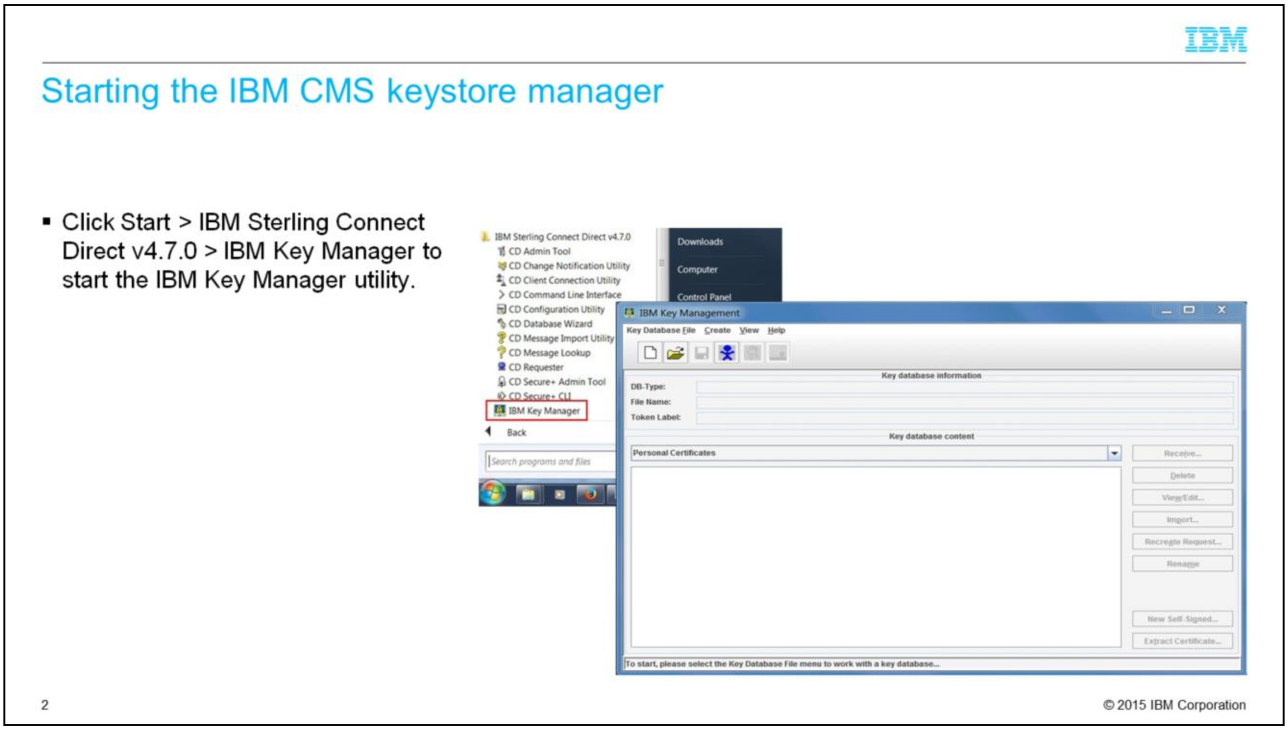
Sterling Connect:Direct for Microsoft Windows 4.7

Configuring the IBM CMS Keystore for Secure+ Part one

This presentation shows you how to configure the IBM CMS keystore for use with Secure plus. It shows you how to create self-signed certificates, and import partner trusted root certificates for Sterling Connect:Direct® for Microsoft® Windows® version 4.7 and later.



Starting the IBM CMS keystore manager

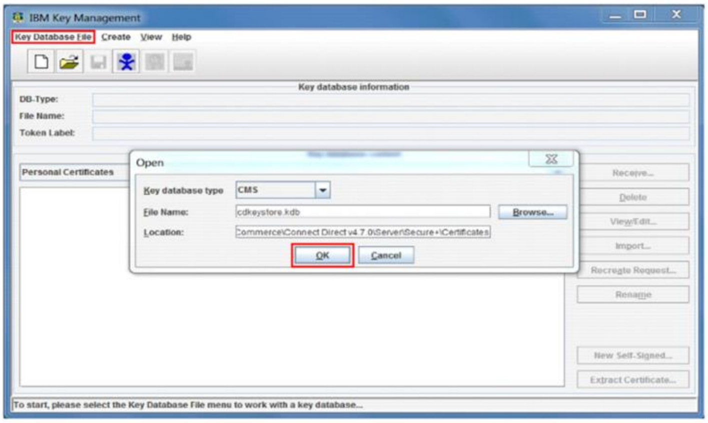
- Click Start > IBM Sterling Connect Direct v4.7.0 > IBM Key Manager to start the IBM Key Manager utility.

To start, please select the Key Database File menu to work with a key database...

From the IBM Sterling Connect:Direct for Microsoft Windows Program directory, start the IBM key Manager utility.

Opening the keystore

- Select “Key Database File”.
- By default the Keystore is created in the Secure+ Certificates directory under the installation folder.



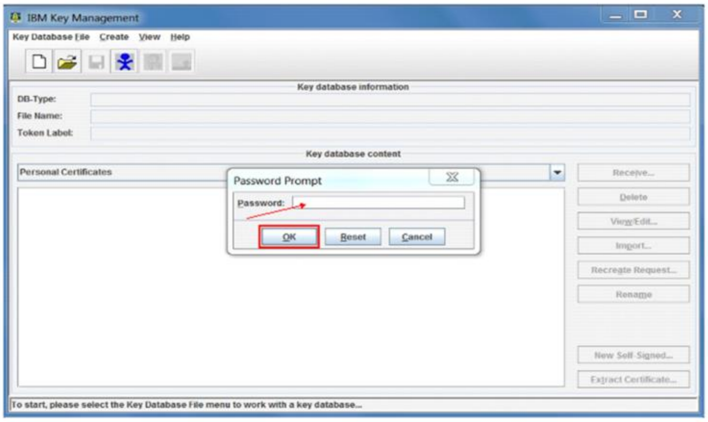
Key database type: CMS
File Name: cdkeystore.kdb
Location: Commerce\Connect Direct v4.7.0\Server\Secure+\Certificates

To start, please select the Key Database File menu to work with a key database...

During the installation of Sterling Connect:Direct for Microsoft Windows, you created a directory that contains the IBM CMS keystore. By default, the keystore is created in the secure plus certificates directory, under the installation folder. To open the keystore, select the Key Database file menu option, and browse to the directory.

Keystore passphrase

- Enter the Keystore password.
- Click “OK”.

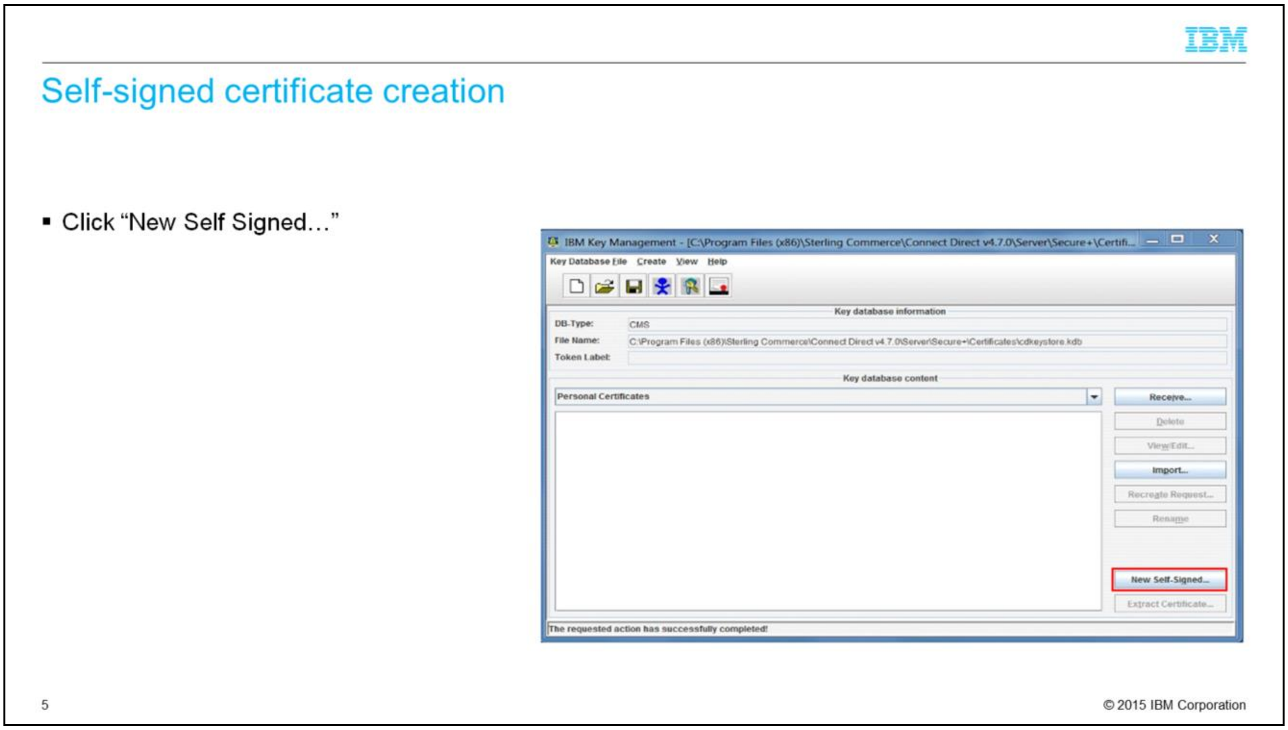


Personal Certificates

To start, please select the Key Database File menu to work with a key database...

4

You will be prompted to enter the keystore password. You chose the password during the installation of Sterling Connect Direct for Microsoft Windows. Enter the password. Click OK.



Self-signed certificate creation

- Click “New Self Signed…”

IBM Key Management - [C:\Program Files (x86)\Sterling Commerce\Connect Direct v4.7.0\Server\Secure+\Certifi...

Key database information

DB-Type: CMS

File Name: C:\Program Files (x86)\Sterling Commerce\Connect Direct v4.7.0\Server\Secure+\Certificates\cdkeystore.kdb

Token Label:

Key database content

Personal Certificates

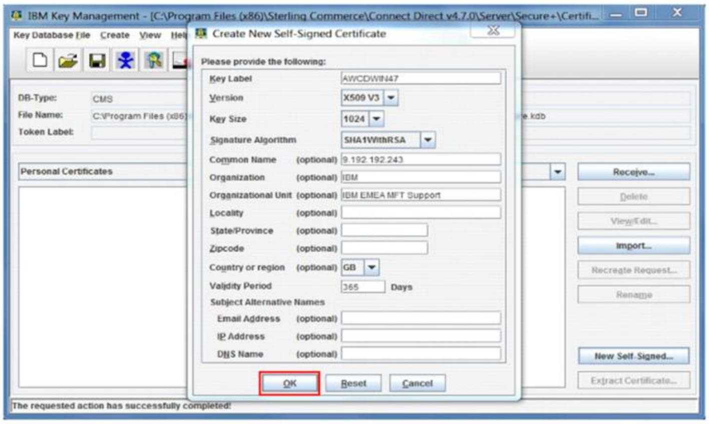
The requested action has successfully completed!

To create a new self-signed certificate, click the New Self Signed button on the IBM Key Management window.

IBM

Certificate details

- Enter your certificate details.
- Click “OK”



DB-Type: CMS
File Name: C:\Program Files (x86)... .kdb
Token Label:

Create New Self-Signed Certificate

Please provide the following:

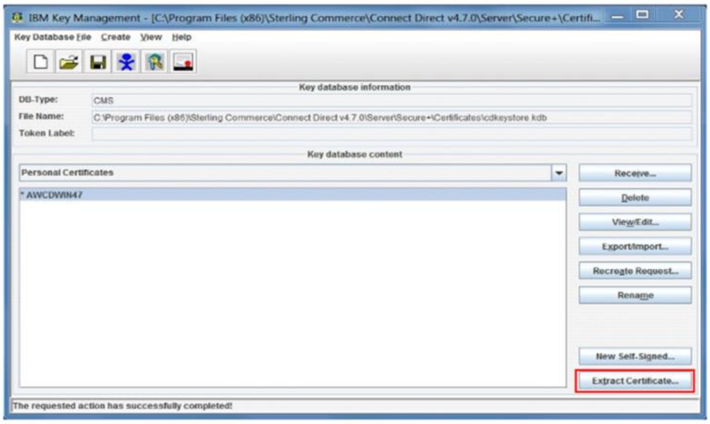
Key Label		AWCDWIN47
Version		X509 V3
Key Size		1024
Signature Algorithm		SHA1WithRSA
Common Name	(optional)	9.192.192.243
Organization	(optional)	IBM
Organizational Unit	(optional)	IBM EMEA MFT Support
Locality	(optional)	
State/Province	(optional)	
Zipcode	(optional)	
Country or region	(optional)	GB
Validity Period		365 Days
Subject Alternative Names		
Email Address	(optional)	
IP Address	(optional)	
DNS Name	(optional)	

The requested action has successfully completed!

Enter your certificate details in the “Create New Self-Signed Certificate” window and click OK.

Export certificate

- Select certificate to act as trusted root certificate.
- Click “Extract Certificate”.



IBM Key Management - [C:\Program Files (x86)\Sterling Commerce\Connect Direct v4.7.0\Server\Secure+\Certifi...

Key database information

DB-Type: CMS

File Name: C:\Program Files (x86)\Sterling Commerce\Connect Direct v4.7.0\Server\Secure+\Certificates\cdkeystore.kdb

Token Label:

Key database content

Personal Certificates

* AWCDWIN47

The requested action has successfully completed!

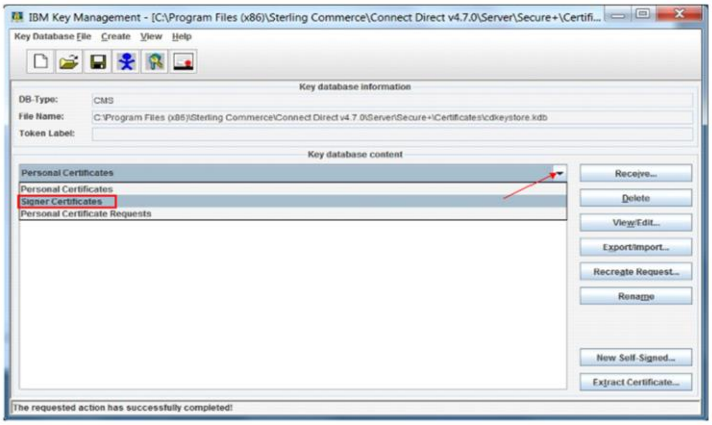
7

© 2015 IBM Corporation

To save a copy of the certificate, click the “Extract Certificate” button for sending to your remote partner to act as your trusted root certificate.

Import a trusted root certificate

- For each partner, add a trusted root certificate to the keystore.
- Select “Signer Certificates”.



IBM Key Management - [C:\Program Files (x86)\Sterling Commerce\Connect Direct v4.7.0\Server\Secure+\Certifi...
Key Database File
Create
View
Help
Key database information

DB-Type: CMS

File Name: C:\Program Files (x86)\Sterling Commerce\Connect Direct v4.7.0\Server\Secure+\Certificates\cdkeystore.kdb

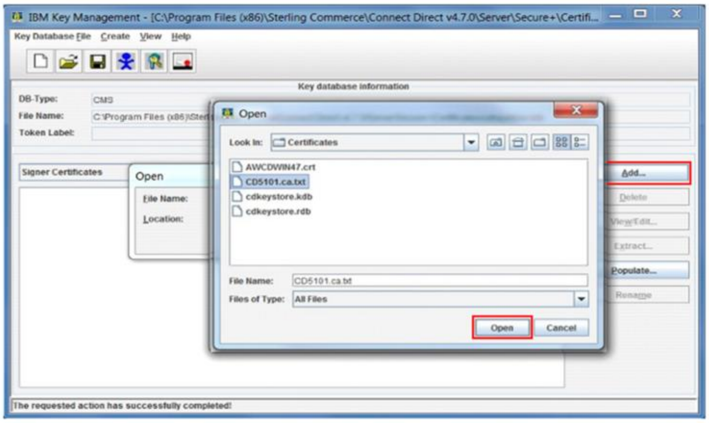
Token Label:

The requested action has successfully completed!

For each partner, you must receive a trusted root certificate. Add the trusted root certificate to the keystore. From the drop-down list under “Key database content”, select “Signer Certificates”.

Import a trusted root certificate II

- Select remote partner trusted root certificate.
- Click “Open”.



IBM Key Management - [C:\Program Files (x86)\Sterling Commerce\Connect Direct v4.7.0\Server\Secure+\Certifi...

Key database information

DB-Type: CMS

File Name: C:\Program Files (x86)\Sterl

Token Label:

Look In: Certificates

AWCDWIN47.crt

CD5101.ca.txt

cdkeystore.kdb

cdkeystore.rdb

File Name: CD5101.ca.txt

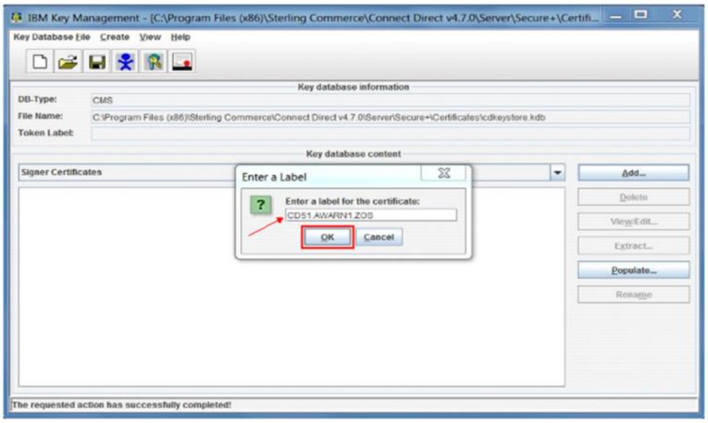
Files of Type: All Files

The requested action has successfully completed!

Click the “Add” button, and browse to the location where the remote partner trusted root certificate is located. Click “Open”.

Import a trusted root certificate III

- Enter a name for the trusted root certificate.
- Close the keystore.



IBM Key Management - [C:\Program Files (x86)\Sterling Commerce\Connect Direct v4.7.0\Server\Secure+\Certifi...

Key database information

DB-Type: CMS

File Name: C:\Program Files (x86)\Sterling Commerce\Connect Direct v4.7.0\Server\Secure+\Certificates\cdkeystore.kdb

Token Label:

Key database content

Signer Certificates

Enter a Label

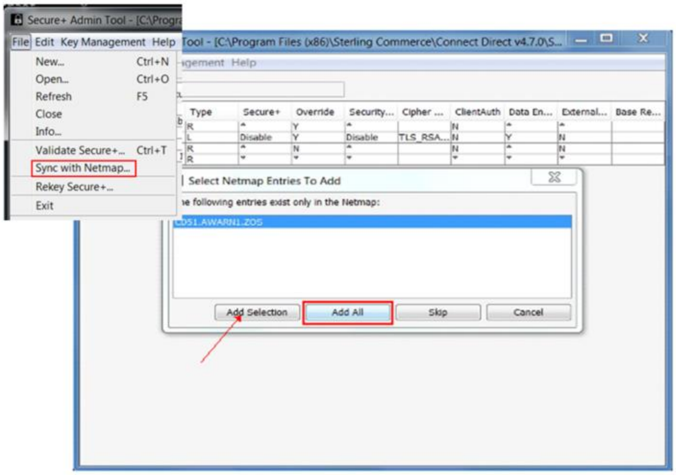
Enter a label for the certificate: CD51.AWARN1.ZOS

The requested action has successfully completed!

Enter a name for the trusted root certificate, and click “OK” to add it to the keystore. You can now close the keystore.

Configuring Secure+

- Open the Sterling Secure+ Admin Tool, click Start > IBM Sterling Connect Direct v4.7.0. > CD Secure+ Admin Tool.
- Sync with Netmap.
- Add nodes to Secure+.


Secure+ Admin Tool - [C:\Progra
File Edit Key Management Help
New... Ctrl+N
Open... Ctrl+O
Refresh F5
Close
Info...
Validate Secure+... Ctrl+T
Sync with Netmap...
Rekey Secure+...
Exit
Tool - [C:\Program Files (x86)\Sterling Commerce\Connect Direct v4.7.0\S...
agement Help
Add Selection
Add All
Skip
Cancel

Type	Secure+	Override	Security...	Cipher ...	ClientAuth	Data En...	External...	Base Re...
R	▴	Y	▴		N	▴	▴	
L	Disable	Y	Disable	TLS_RSA...	N	Y	N	
R	▴	N	▴		N	▴	N	
R	▾	▾	▾		▾	▾	▾	

Select Netmap Entries To Add

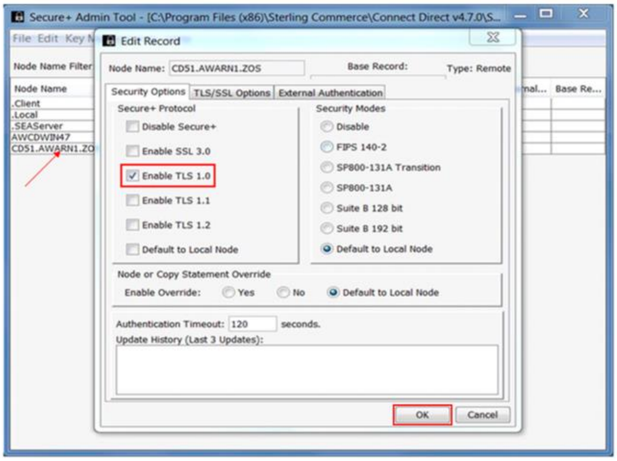
he following entries exist only in the Netmap:

CD51.AWARN1.ZOS

Open the Sterling Secure plus Admin tool, and select File > Sync with Netmap to ensure that all node entries are available. Click “Add All” or select the required node and click “Add Selection” to add a node to the Secure plus configuration.

Configure a Secure+ remote node entry

- Open remote node entry.
- Select the Secure+ protocol.
- Click “OK” to continue.



Secure+ Admin Tool - [C:\Program Files (x86)\Sterling Commerce\Connect Direct v4.7.0\S...

Edit Record

Node Name: CD51.AWARN1.ZOS

Base Record:

Type: Remote

Security Options | TLS/SSL Options | External Authentication

Secure+ Protocol

□ Disable Secure+
□ Enable SSL 3.0
☑ Enable TLS 1.0
□ Enable TLS 1.1
□ Enable TLS 1.2
□ Default to Local Node

Security Modes

○ Disable
○ FIPS 140-2
○ SP800-131A Transition
○ SP800-131A
○ Suite B 128 bit
○ Suite B 192 bit
● Default to Local Node

Node or Copy Statement Override

Enable Override: ○ Yes ○ No ● Default to Local Node

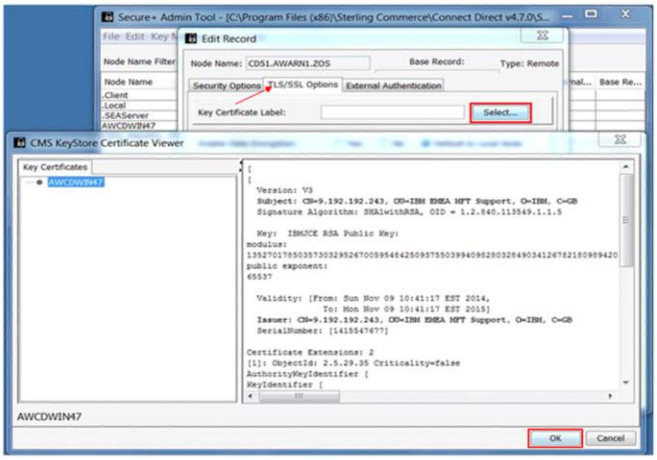
Authentication Timeout: 120 seconds.

Update History (Last 3 Updates):

To open the remote node entry, double-click the entry in the Secure plus Admin tool. Then, from the “Security Options” tab, select the Secure plus protocol to be used for this remote partner.

Selecting a key certificate

- Select the “TLS/SSL” Options tab.
- Choose the key certificate label.
- Click “OK’ to continue.



Node Name: CD51.AWARN1.ZOS

Base Record:

Type: Remote

Key Certificate Label:

AWCDWIN47

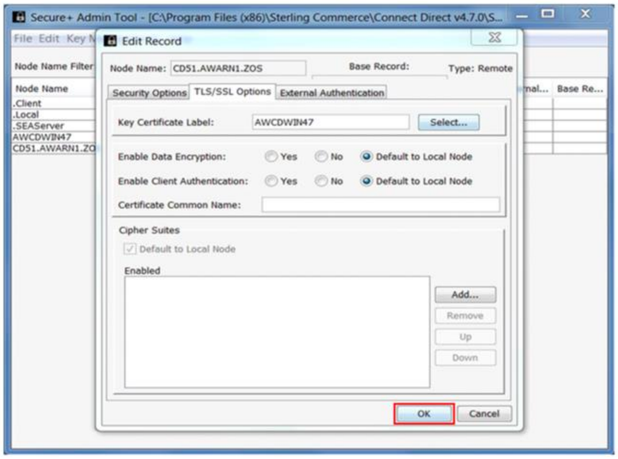
```
[
[
  Version: V3
  Subject: CN=9.192.192.243, OU=IBM EMEA MFT Support, O=IBM, C=GB
  Signature Algorithm: SHA1withRSA, OID = 1.2.840.113549.1.1.5

  Key:  IBMJCE RSA Public Key:
modulus:
13527017850357303295267005954842509375503994098280328490341267821809894 20
public exponent:
65537

  Validity: [From: Sun Nov 09 10:41:17 EST 2014,
               To: Mon Nov 09 10:41:17 EST 2015]
  Issuer: CN=9.192.192.243, OU=IBM EMEA MFT Support, O=IBM, C=GB
  SerialNumber: [1415547677]

Certificate Extensions: 2
[1]: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
KeyIdentifier [
```

AWCDWIN47

From the “TLS or SSL Options” tab, click the select button, and choose the key certificate label for the self-signed certificate that you created earlier.

Saving the Secure+ remote node entry

- Update the Secure+ remote node entry.
- Click “OK’ to continue.



Node Name: CD51.AWARN1.ZOS

Base Record:

Type: Remote

Key Certificate Label: AWCDWIN47

Enable Data Encryption: ○ Yes ○ No ● Default to Local Node

Enable Client Authentication: ○ Yes ○ No ● Default to Local Node

Certificate Common Name:

Cipher Suites

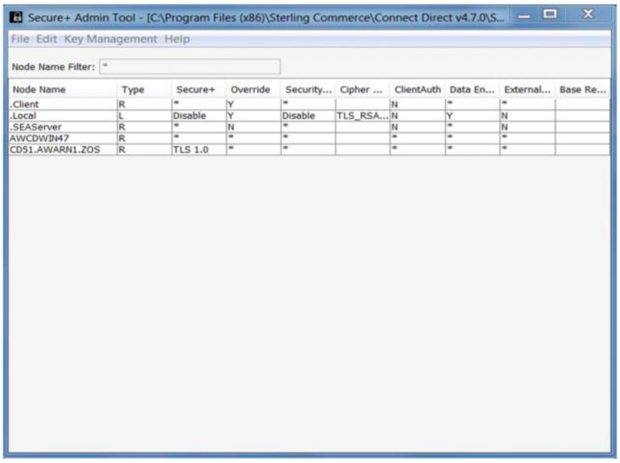
☑ Default to Local Node

Enabled

Click the OK button on the CMS Keystore Certificate Viewer window to update the Secure plus remote node entry.

Completed Secure+ configuration

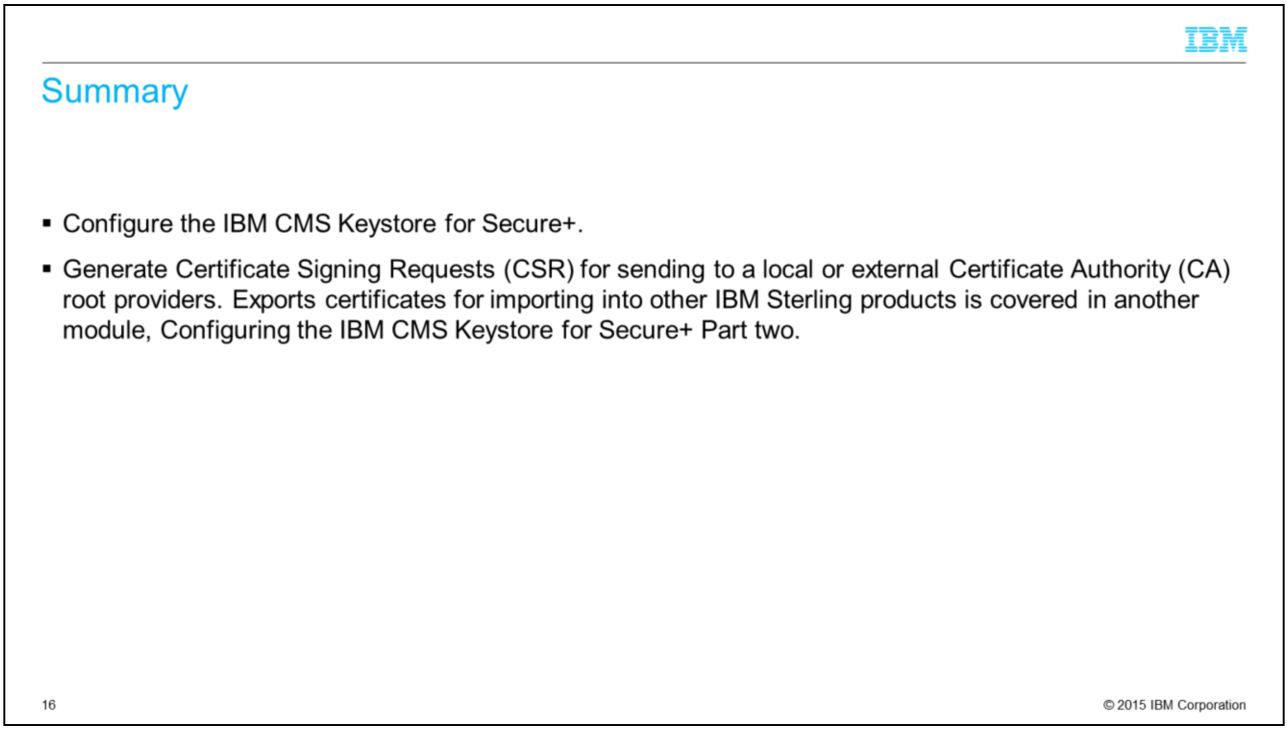
- Check settings correctly.
- Close the Secure+ Admin Tool.


Secure+ Admin Tool - [C:\Program Files (x86)\Sterling Commerce\Connect Direct v4.7.0\S...
File Edit Key Management Help

Node Name Filter: *

Node Name	Type	Secure+	Override	Security...	Cipher ...	ClientAuth	Data En...	External...	Base Re...
.Client	R	*	Y	*		N	*	*	
.Local	L	Disable	Y	Disable	TLS_RSA...	N	Y	N	
.SEAServer	R	*	N	*		N	*	N	
AWCDWIN47	R	*	*	*		*	*	*	
CD51.AWARN1.ZOS	R	TLS 1.0	*	*		*	*	*	

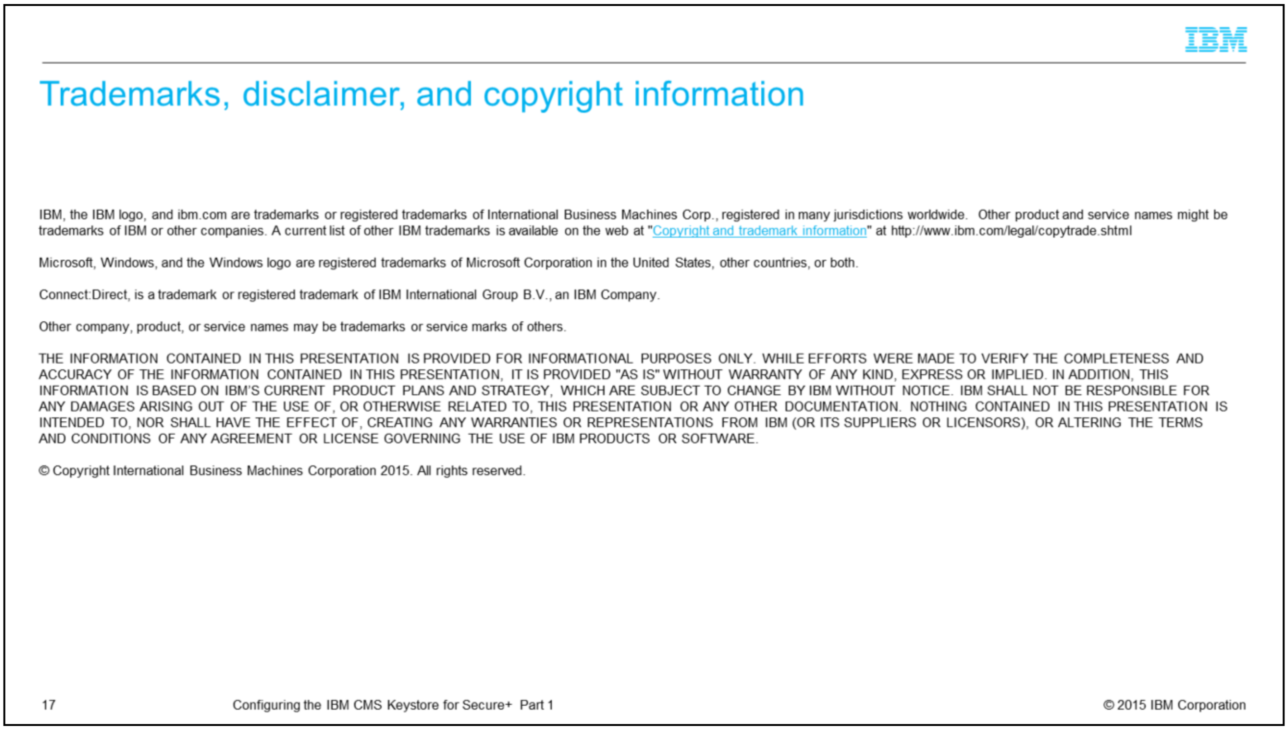
Check that you updated the settings correctly. You can now close the Secure plus Admin tool.



Summary

- Configure the IBM CMS Keystore for Secure+.
- Generate Certificate Signing Requests (CSR) for sending to a local or external Certificate Authority (CA) root providers. Exports certificates for importing into other IBM Sterling products is covered in another module, Configuring the IBM CMS Keystore for Secure+ Part two.

In the first part of this presentation, you learned about Configuring the IBM CMS keystore for Secure plus. In part two, you will look at generating Certificate signing requests for sending to local or external CA root providers. You will also learn how to export key certificates for importing into other IBM Sterling products.



Trademarks, disclaimer, and copyright information

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of other IBM trademarks is available on the web at "Copyright and trademark information" at http://www.ibm.com/legal/copytrade.shtml

Microsoft, Windows, and the Windows logo are registered trademarks of Microsoft Corporation in the United States, other countries, or both.

Connect:Direct, is a trademark or registered trademark of IBM International Group B.V., an IBM Company.

Other company, product, or service names may be trademarks or service marks of others.

THE INFORMATION CONTAINED IN THIS PRESENTATION IS PROVIDED FOR INFORMATIONAL PURPOSES ONLY. WHILE EFFORTS WERE MADE TO VERIFY THE COMPLETENESS AND ACCURACY OF THE INFORMATION CONTAINED IN THIS PRESENTATION, IT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. IN ADDITION, THIS INFORMATION IS BASED ON IBM'S CURRENT PRODUCT PLANS AND STRATEGY, WHICH ARE SUBJECT TO CHANGE BY IBM WITHOUT NOTICE. IBM SHALL NOT BE RESPONSIBLE FOR ANY DAMAGES ARISING OUT OF THE USE OF, OR OTHERWISE RELATED TO, THIS PRESENTATION OR ANY OTHER DOCUMENTATION. NOTHING CONTAINED IN THIS PRESENTATION IS INTENDED TO, NOR SHALL HAVE THE EFFECT OF, CREATING ANY WARRANTIES OR REPRESENTATIONS FROM IBM (OR ITS SUPPLIERS OR LICENSORS), OR ALTERING THE TERMS AND CONDITIONS OF ANY AGREEMENT OR LICENSE GOVERNING THE USE OF IBM PRODUCTS OR SOFTWARE.