How to create keystore and import certificate?

* Have the certificate downloaded from the Server like (LDAP server, Exchange Server, any other server with which any client connects).
* Export the client certificate with .cer extn.
* Copy the certificate to the AR Server where we want to create Keystore and import certificate.
* For Ex: C:\Certificates\xxx.cer
	+ Where xxx is the certificate name.
* Now check which java is being used by AR Server (C:\Program files\Java\jre\bin).
* Open command prompt and navigate to above java path.
* Use below command to create a keystore and import the certificate downloaded from server (xxx.cer)
* ***Keytool –import –noprompt –trustcacerts –keystore <path1> -storepass “<password>” –alias <aliasname> -file <path2>***
	+ Where
		- Path1: path where you want to create .jks (keystore) something like “C:\Cert\LDAP.jks
		- Password: any password with which keystore can be accessed something like remedy12
		- Aliasname: alias name to the keystore like AREALDAP
		- Path2: path where you have stored .cer file something like “c:\Cert\xxx.cer
* The above command will create a keystore and import the certificate in the keystore and now the keystore is available to use with AR server.

Screenshots:

1. Create a folder on the server with full permission.



1. Ensure the folder has full permission (RWX)



1. Copy the .cer file that is exported from LDAP Server or Exchange Server to Test Folder. (Note if the extn is different check with your LDAP team or try with changing the extn to .cer)



1. Change the extn from b64 to .cer



1. Now navigate to the java/jre/bin folder (java which ARServer is using)



1. Open command prompt and navigate to above location highlighted in Address bar or type **cmd** in address bar to open command prompt from the same location.



1. Use the keytool command to create keystore and import the certificate as below.

Command:

* ***Keytool –import –noprompt –trustcacerts –keystore <path1> -storepass “<password>” –alias <aliasname> -file <path2>***
	+ Where
		- Path1: path where you want to create .jks (keystore) something like “C:\Cert\LDAP.jks
		- Password: any password with which keystore can be accessed something like remedy12
		- Aliasname: alias name to the keystore like AREALDAP
		- Path2: path where you have stored .cer file something like “c:\Cert\xxx.cer

Screenshot:





1. To view the keystore details use below command:

Command:

***keytool -list -keystore C:\Test\ldap.jks -storepass remedy12***



We successfully created keystore and the certificate is imported successfully. Now this path can be used for configuring AREA LDAP or Email Configuration.