

End-to-End HOWTO guide for silently and transparently provisioning and installing Java extensions to Notes 8.5.1+ clients using policies

Table of Contents

Table of Contents	1
Prerequisites	2
Create databases	2
Create root certificate	2
Migrate the internet certifier into Domino	3
Issue internet certificate to a user	4
Accept the certificate into the id-file and export the certificate	5
Convert the certificate from PKCS#12 format to Java Keystore format	6
Import the internet root certificate into the Domino Directory and cross certify it	7
Use policies to push the internet cross certificate to users	9
Sign the features and plugins and import into the update site	11
Import widget into the widget catalog	12
Extend policy with a Desktop Settings document to provision Java extensions to end-users	12

Prerequisites

I will assume that you

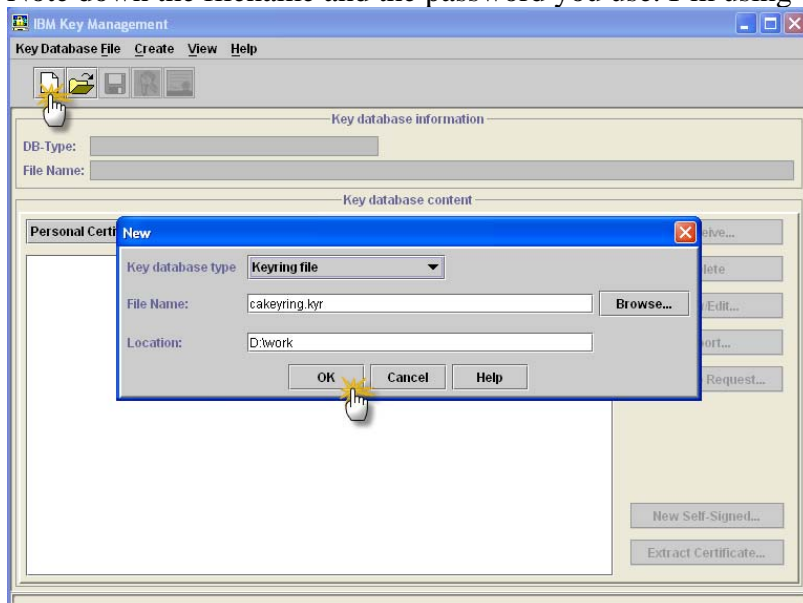
- are using and have started the CA process server task (load CA)
- have downloaded a Java Developer Kit and added the “bin”-directory of the install to the PATH of your machine so you can use jarsigner.exe and keytool.exe
- are fairly well founded in the Lotus Domino and Lotus Notes clients and terminology

Create databases

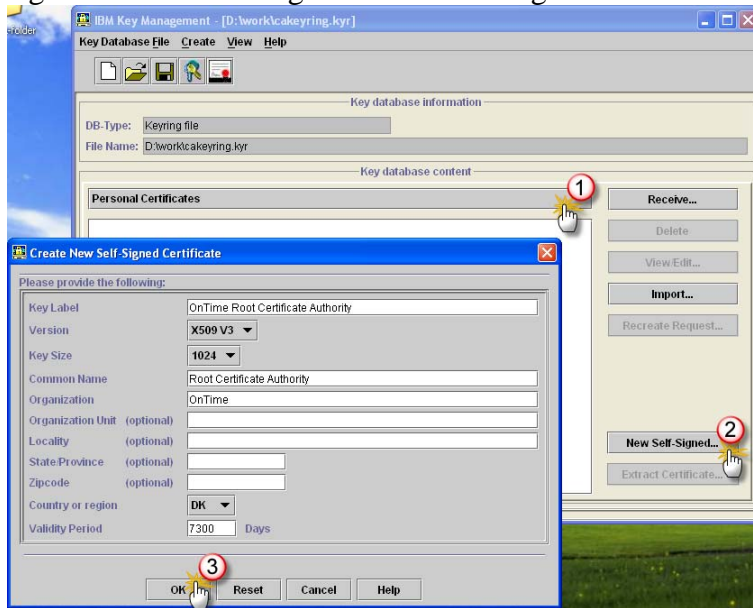
1. Using Notes create an Eclipse update site database on a Domino server
 - a. Template: "Eclipse Update Site" (advanced template)
 - b. Filename: updatesite.nsf
2. Using Notes create a widget catalog database on a Domino server
 - a. Template: "Widget Catalog" (advanced template)
 - b. Filename: widgetcatalog.nsf

Create root certificate

1. Start iKeyman
2. Create keystore for your root certificate authority (CA) using a “Key database type” of “Keyring file”.
3. Note down the filename and the password you use. I’m using d:\work\cakeyring.kyr



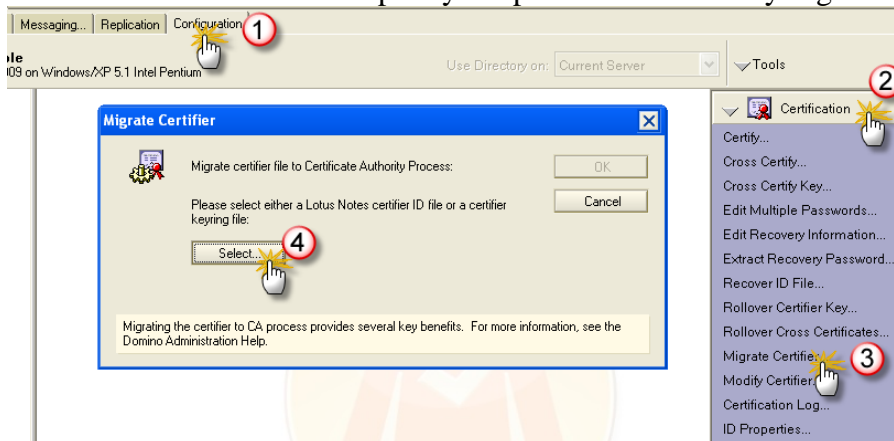
4. Change to the “Personal certificates” section using the dropdown and create a new self-signed certificate using the “New Self-Signed...” button the lower right corner.



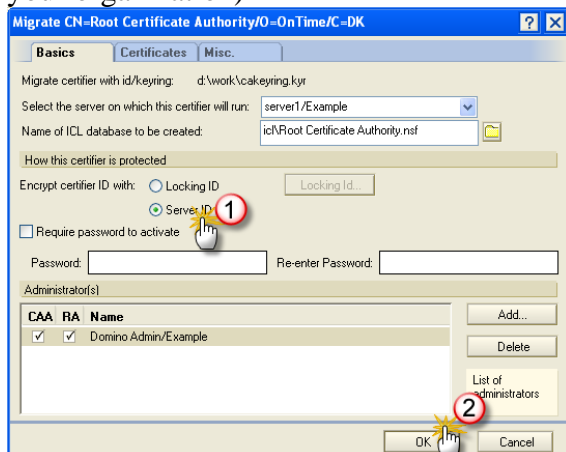
5. Close and iKeyman application

Migrate the internet certifier into Domino

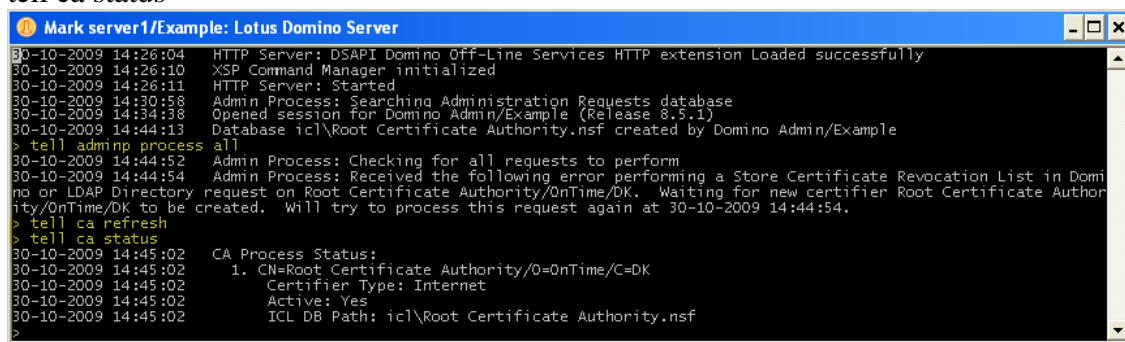
1. Open the Domino Administrator client
2. Change to the “Configuration” tab, open the “Certification” tool-section on the right and click “Migrate Certifier...”. Now click the “Select...” button to select the keyring file you created above. When asked specify the password for the keyring file.



3. Choose to encrypt certifier with the server ID (or follow whatever guidelines you have in your organization)

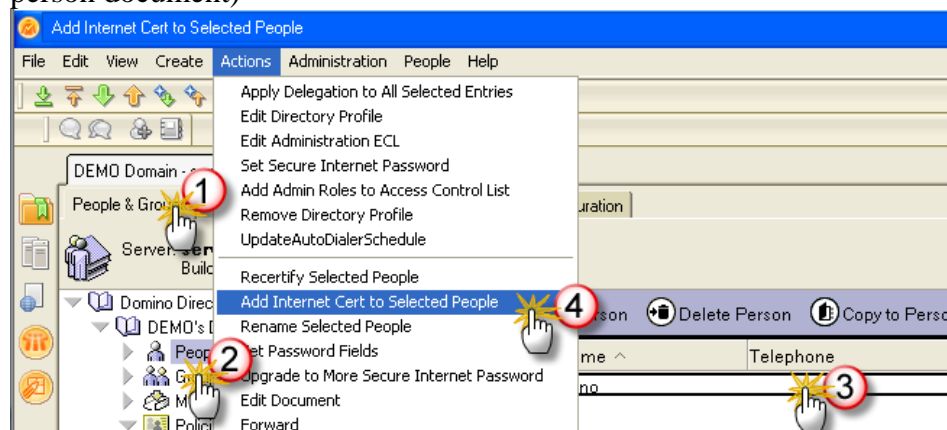


4. Now wait a few minutes until the certifier has been migrated in Domino. You'll see a message on the server console once this has been done.
5. Change to the Domino server console
6. Refresh the CA process and verify that your certificate has been successfully migrated using the following server console commands:
 - a. tell ca refresh
 - b. tell ca status

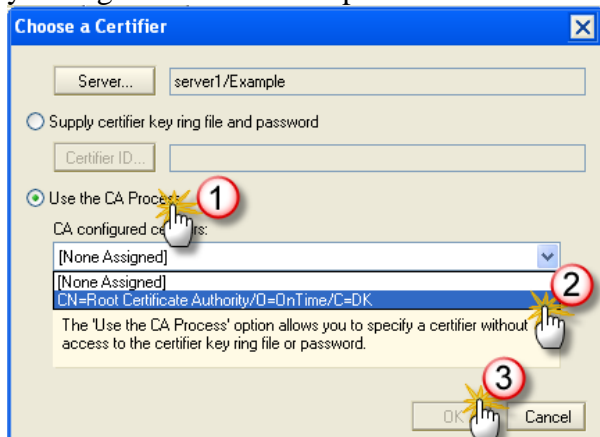


Issue internet certificate to a user

1. In the Domino Administrator client switch to the "People & Groups" tab
2. Select the user to issue the certificate to and choose Actions\Add Internet Cert to Selected People (**Please note:** The user(s) you select must have an e-mail address specified in their person document)



3. In the “Choose a Certifier” dialog choose to use the CA process and select the certificate you migrated into the CA process above. Then click OK.



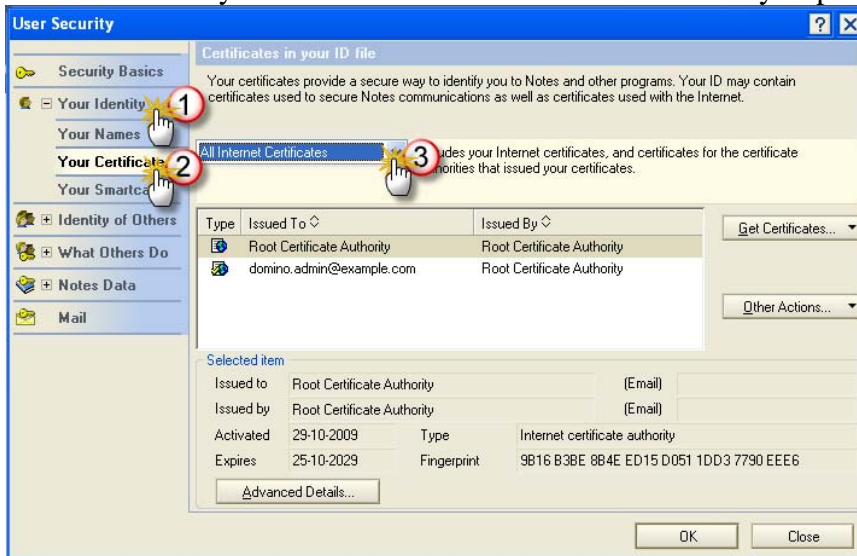
4. Choose the length of time to certify the user for and complete the process. If the process fails it's usually because no e-mail address is specified for the user(s).
5. Wait a few minutes and make sure the new certificate has been added to the Internet Certificate tab in the users person document



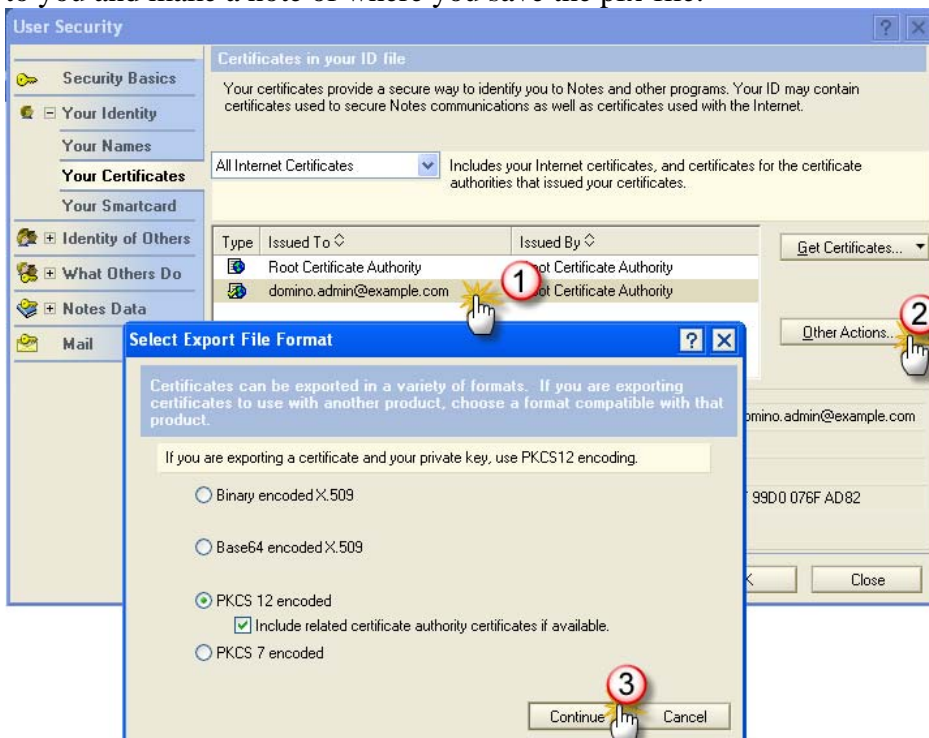
Accept the certificate into the id-file and export the certificate

1. Change to the Notes klienten and authenticate with the home server of the user. This is easiest done by pressing Ctrl-F5 and then opening the mail file from the server.

2. Choose “File/Security/User security...” from the menu and change to the internet certificate section and verify that the certificate has been automatically imported into the users id-file



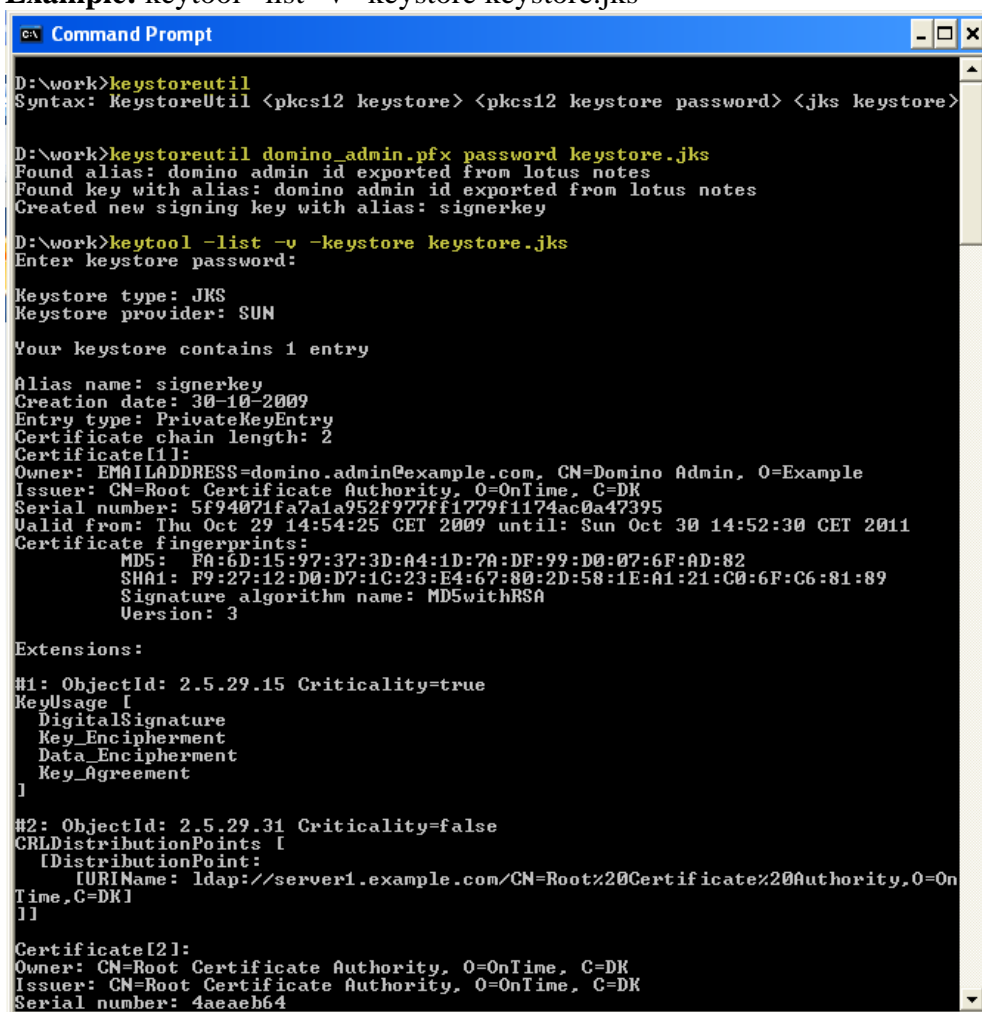
3. To use the certificate to sign Java extensions we need to export it. To export the certificate you have to select the user certificate in the list and then choose “Other actions\Export certificate”. Export the certificate using the PKCS#12 format. Accept the defaults presented to you and make a note of where you save the pfx-file.



Convert the certificate from PKCS#12 format to Java Keystore format

1. Download the KeystoreUtil Java program from <http://lekkimworld.com/keystoreutil> and follow the steps specified there to make it work. Make sure you download it to the same directory as where you saved your pfx-file.

2. Open a Command prompt and change to the directory where you saved the pfx-file above
3. Using the KeystoreUtil program convert the pfx-file to Java Keystore format using a command like the following: `keystoreutil <pfx-file> <password> <Java keystore filename>`
 - a. **Example:** `keystoreutil domino_admin.pfx password keystore.jks`
 - b. **Important:** Make a note of the alias generated by the tool. The alias will be “signerkey”.
4. (Optional) Verify the generated Java keystore using the keytool command
 - a. **Example:** `keytool -list -v -keystore keystore.jks`



```
Command Prompt
D:\work>keystoreutil
Syntax: KeystoreUtil <pkcs12 keystore> <pkcs12 keystore password> <jks keystore>

D:\work>keystoreutil domino_admin.pfx password keystore.jks
Found alias: domino admin id exported from lotus notes
Found key with alias: domino admin id exported from lotus notes
Created new signing key with alias: signerkey

D:\work>keytool -list -v -keystore keystore.jks
Enter keystore password:

Keystore type: JKS
Keystore provider: SUN

Your keystore contains 1 entry

Alias name: signerkey
Creation date: 30-10-2009
Entry type: PrivateKeyEntry
Certificate chain length: 2
Certificate[1]:
Owner: EMAILADDRESS=domino.admin@example.com, CN=Domino Admin, O=Example
Issuer: CN=Root Certificate Authority, O=OnTime, C=DK
Serial number: 5f94071fa7a1a952f977ff1779f1174ac0a47395
Valid from: Thu Oct 29 14:54:25 CET 2009 until: Sun Oct 30 14:52:30 CET 2011
Certificate fingerprints:
MD5: FA:6D:15:97:37:3D:A4:1D:7A:DF:99:D0:07:6F:AD:82
SHA1: F9:27:12:D0:D7:1C:23:E4:67:80:2D:58:1E:A1:21:C0:6F:C6:81:89
Signature algorithm name: MD5withRSA
Version: 3

Extensions:
#1: ObjectId: 2.5.29.15 Criticality=true
KeyUsage [
  DigitalSignature
  Key_Encipherment
  Data_Encipherment
  Key_Agreement
]

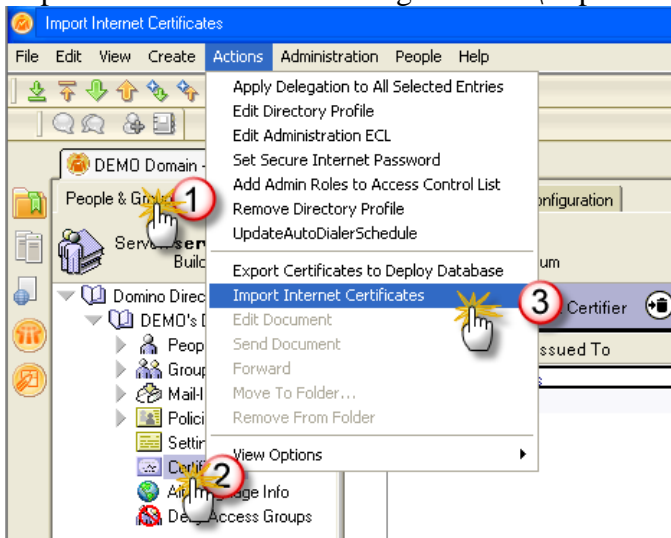
#2: ObjectId: 2.5.29.31 Criticality=false
CRLDistributionPoints [
  [DistributionPoint:
    [URIName: ldap://server1.example.com/CN=Root%20Certificate%20Authority,O=OnTime,C=DK]
  ]
]

Certificate[2]:
Owner: CN=Root Certificate Authority, O=OnTime, C=DK
Issuer: CN=Root Certificate Authority, O=OnTime, C=DK
Serial number: 4aeab64
```

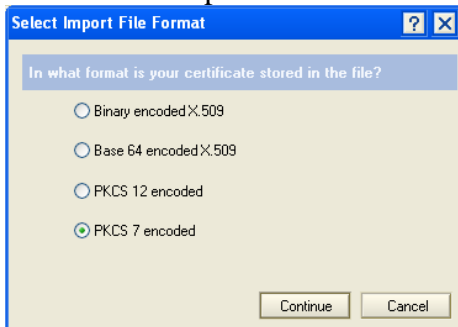
Import the internet root certificate into the Domino Directory and cross certify it

3. Change to the Domino Administrator client
4. Change to the "Certificates" view on the "People & Groups" tab

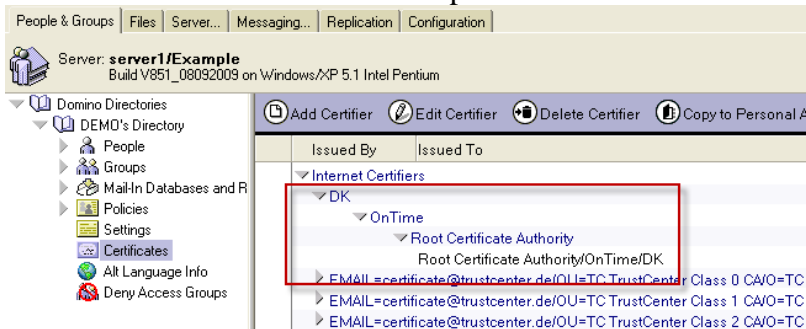
5. Import the root certificate using “Actions\Import Internet Certificates”



6. Import the pfx-file you exported above as a **PKCS#7** file so only the public key of our root certificate is imported

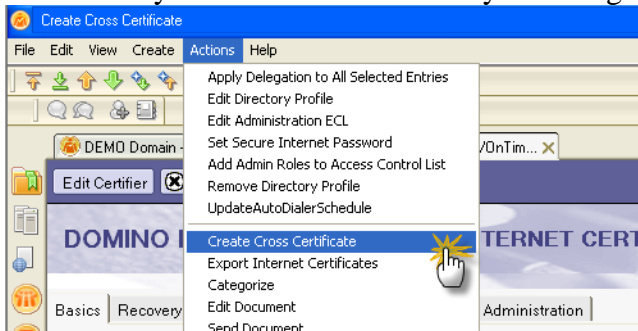


7. Refresh the view and locate the imported certificate in the view



8. Open the certificate document

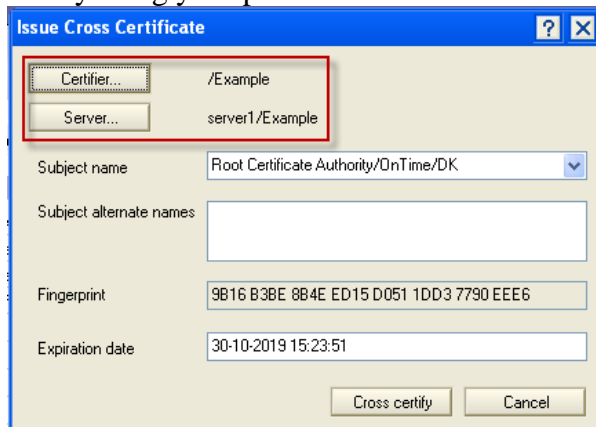
9. Cross certify the internet certificate by choosing “Actions\Create Cross Certificate”



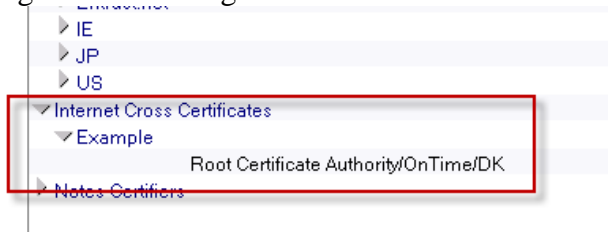
- a. In the "Create cross certificate" dialog choose your root certificate and select OK.



- b. Make sure you cross-certify the internet root certificate on the server and using an organizational or organizational unit certifier depending on your needs. Do not cross-certify using your personal user id.

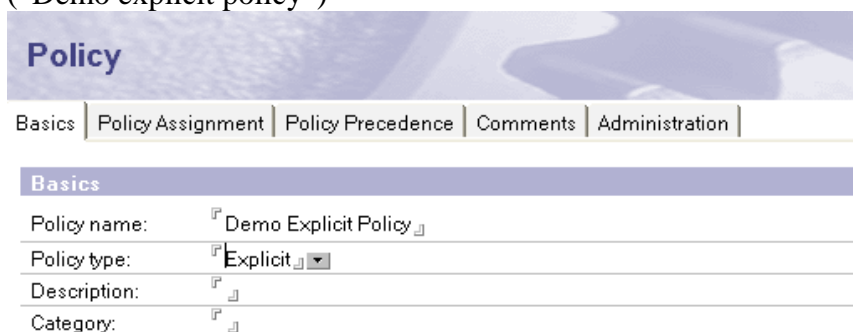


10. Refresh the view and make sure your internet certificate has been cross-certified by the organization or organizational unit

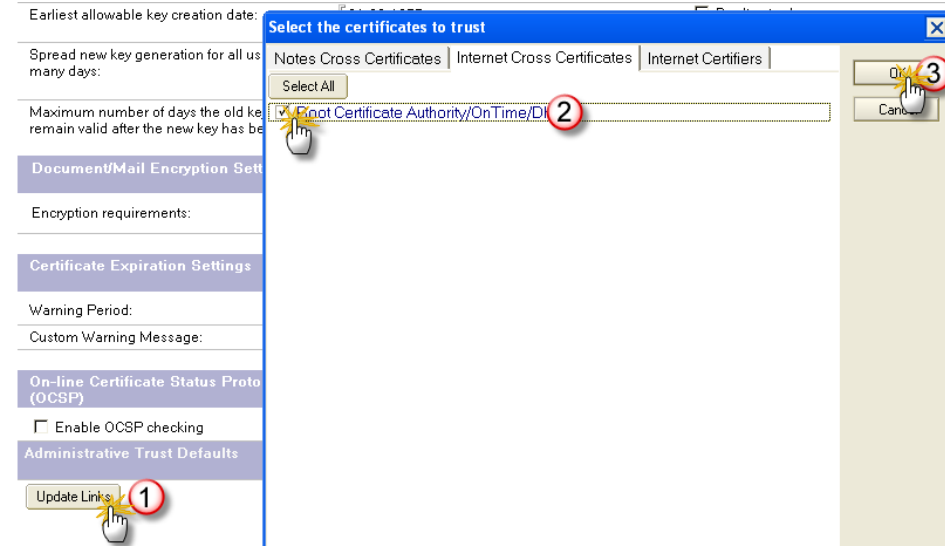


Use policies to push the internet cross certificate to users

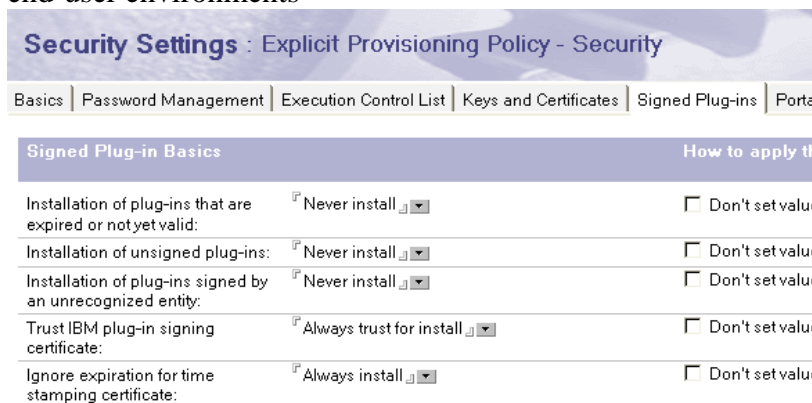
1. Open Domino Directory and switch to the "Policies" view under "People & Groups"
2. Wait a little while until the view indexes are updated. To force an update press Ctrl-Shift-F9.
3. Create a new policy. For this example create it as an explicit policy and give it a name ("Demo explicit policy")



4. Create a Security Settings document and give it a name
 - a. Change to the “Certificates and Keys” tab
 - b. Scroll to the bottom and in the “Administrative Trust Defaults” section click the “Update Links” button.
 - c. Choose “Select Supported” click OK
 - d. In the “Select the certificates to trust” dialog switch to the “Internet Cross Certificates” tab and select the internet cross certificate we created above.



- e. (Optional) Change to the “Signed plugins” tab and specify settings for how the Notes client should handle installation of unsigned and/or untrusted Java extensions. I recommend not allowing installation of unsigned and untrusted Java extensions for end-user environments

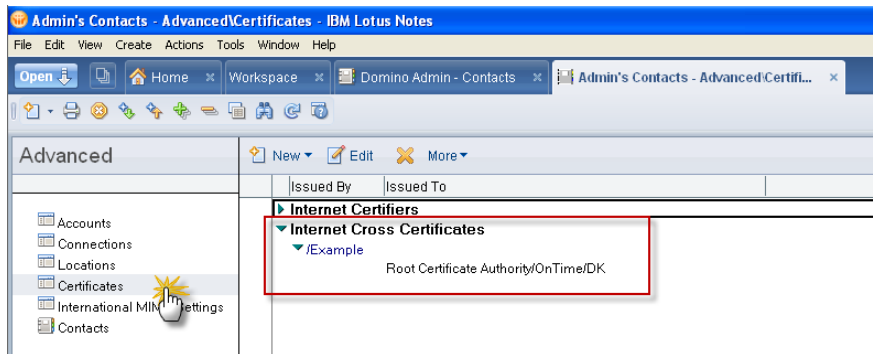


- f. Save and close the Security Settings document
5. Assign the policy you created to a user and make the policy apply to the user. Applying an explicit policy to a user is done on the “Administration” tab under “Policy Management” on the Person document in the Domino Directory.

Please note: After applying/changing a policy for a user it may take some time for it to take effect. To speed things up you may want to perform the following steps:

- a. Open the personal name and address book of the user you’re applying the policy for.
- b. Switch to the hidden (\$Policies) view and delete all the documents in the view. If soft-deletions are enabled be sure to also empty the Trash.
- c. Restart the Notes client.
- d. Authenticate to the home server and open the mail database on the home server.

6. After the policy has been applied you should see the internet cross certificate in the personal name and address book of the user



Sign the features and plugins and import into the update site

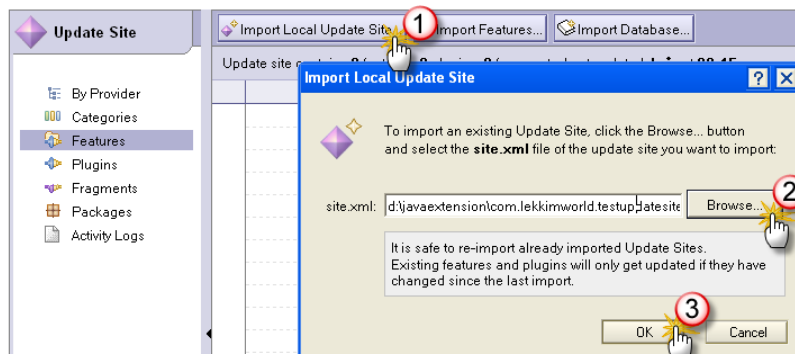
1. Open a Command prompt
2. Change to the directory where you have an Eclipse update site on disk containing the features you would like to install
3. Sign the features and plugins using jarsigner.exe and the Java keystore you created earlier
 - a. For each of the JAR-files (for features and plugins) run jarsigner.exe using a syntax similar to this:

```
jarsigner -keystore <path to Java keystore> -storepass <password of Java keystore> <path to feature/plugin to sign> <key alias>
```

Example commands for signing two features and two plugins:

```
jarsigner -keystore d:\work\keystore.jks -storepass password com.lekkimworld.testupdatesite\plugins\com.lekkimworld.testplugin1_1.0.0.jar signerkey  
jarsigner -keystore d:\work\keystore.jks -storepass password com.lekkimworld.testupdatesite\plugins\com.lekkimworld.testplugin2_2.0.0.jar signerkey  
jarsigner -keystore d:\work\keystore.jks -storepass password com.lekkimworld.testupdatesite\features\com.lekkimworld.testfeature1_1.0.0.jar signerkey  
jarsigner -keystore d:\work\keystore.jks -storepass password com.lekkimworld.testupdatesite\features\com.lekkimworld.testfeature2_2.0.0.jar signerkey
```

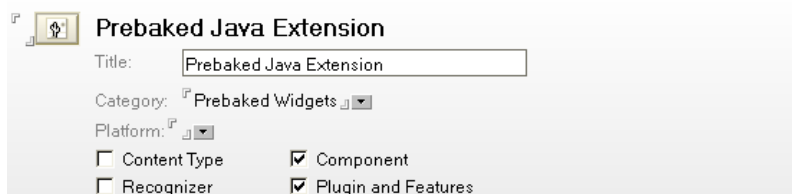
4. Switch to Notes and open the Eclipse Update Site database you created above
5. Click "Import local update site" and browse to the path where the site.xml of the Update Site on disk is stored and click OK. The plugins and features are now imported into the Notes database.



6. Write/update your widget descriptor and make sure the widget descriptor contains the correct URL address for the update site. Use "Actions/Show URLs..." in the Eclipse Update Site database to see the URL of the update site.

Import widget into the widget catalog

1. Open the widget catalog database you created above and create a new widget
2. Specify a name, a description, a category and attach the widget descriptor for you Java extension



Prebaked Java Extension

Title:

Category:

Platform:

Content Type Component

Recognizer Plugin and Features

Description

The Description field is used to provide a short description for this widget. This short description is or two.



Prebaked Java Extension

Attachment

Click the button to choose your XML file from your local file system. The path to your file will appear close your document. If you wish to remove the currently attached file, simply click the "Remove" button.

extension.xml

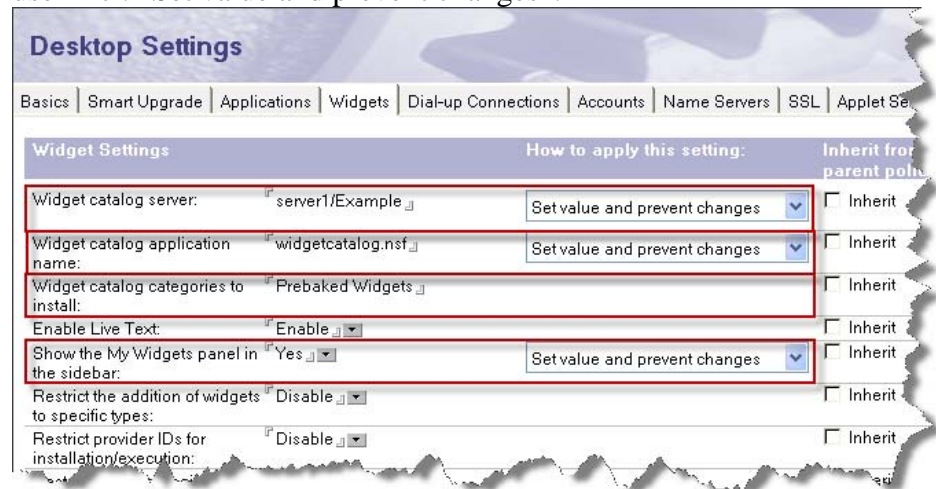
File:  - extension.xml

3. Make a note of the category name as you'll need it when creating the Desktop Settings document below. Here we use "Prebaked Widgets" as the category name.
4. Save and close the widget document.

Extend policy with a Desktop Settings document to provision Java extensions to end-users

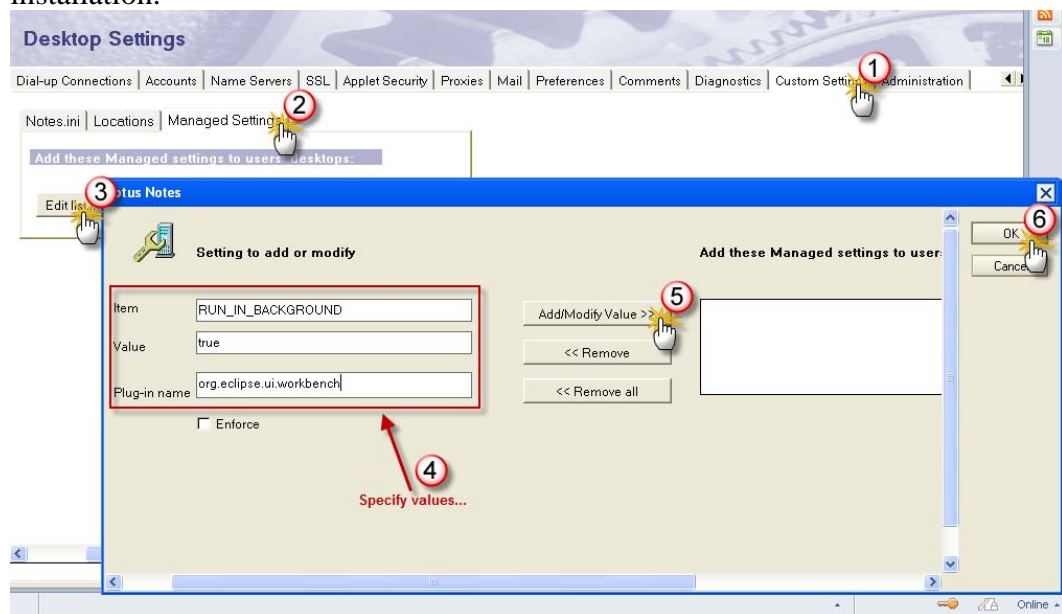
1. Switch to the Domino Administrator client
2. Switch to the policy view edit the policy you created above
3. Create a new Desktop Settings document and give it a name
 - a. (Optional) On the "Basics" tab
 - i. Check "Allow user initiated updates"
Please note: This will enable the File/Application/Install menu options in the Notes client
 - b. On the "Widgets" tab
 - i. Specify the server for the "Widget catalog server" incl. "Set value and prevent changes"
 - ii. Specify the filename for the "Widget catalog application name" incl. "Set value and prevent changes"
 - iii. Specify the name of the widget category you created above in the "Widget categories to install"

- iv. (Optional) Specify that the MyWidgets sidebar should be shown to the end user incl. "Set value and prevent changes".



- c. (Optional) On the "Custom Settings" tab (scroll all the way to right using the small arrows)

Please note: This setting is required to make the install transparent. If this setting is not set the user will see a dialog appear during the Java extension provisioning and installation.



- i. On the "Managed settings" sub-tab
 1. Click "Edit list..." and fill the fields
 - a. Item: RUN_IN_BACKGROUND
 - b. Value: true
 - c. Plug-in name: org.eclipse.ui.workbench
 2. Click "Add/Modify Value"
 3. Click OK
 - d. Save and close the Desktop Settings document
7. Select the Desktop Settings document in the policy
 8. Save and close the policy

9. Make sure the changed policy is applied to the user (see above for pointers on how to speed this process up).

Now when you restart the Notes client the policy should be applied and the signed Java extensions should be provisioned to the user and installed in the Notes client silently.