

The low down on Notes plugin distribution and provisioning

Mikkel Flindt Heisterberg
Senior Solution Architect, IntraVision Aps

About me

- Notes/Domino developer
- Design Partner for Domino NEXT
- Sametime / Java / DB2 / WebSphere / web
- Active blogger: lekkimworld.com
- Speaker at Lotusphere
- Numerous articles for THE VIEW
- LotusScript.doc / 
- .com/lekkim



What's this session about?

Use Domino policies to seamlessly and transparently provision, install and manage Java extensions on the Notes 8.x Standard client.

Control Notes clients to only allow the extensions we, as administrators, allow them to install or we install for them.

So what do we need?

- Signed Java extension to install
- Notes/Domino 8.5.1 policies
 - Previously the policy controls we needed wasn't in place
- Widget Catalog
- Certificate management



Java extensions

- In "Eclipse speak" Java extensions are really two things – plugins and features
- Plugins and features are delivered as JAR-files
 - They are just ZIP-files with a certain directory structure
- JAR-files may be signed ie. it may be verified that the file hasn't been changed since being signed
- The signature information is kept inside the JAR-file along with the code



Plugins and features

- It's important to distinguish between plugins and features
- Only features can be installed using the UI
- Features reference plugins
- Plugins are where the functionality is



Plugin and feature anatomy

Plugin

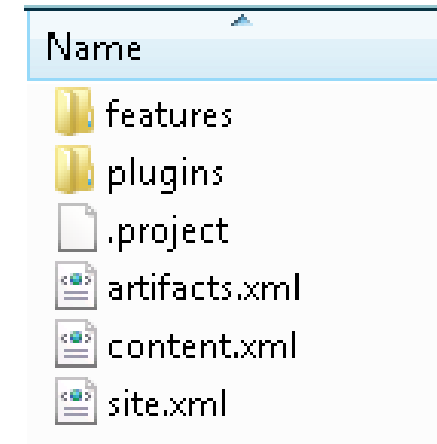
- META-INF/MANIFEST.MF
 - Contains plugin version info and dependencies
- plugin.xml
 - Extension points used / exposed
- Java code
 - Well duh!
- Resources
 - Localization, images, properties etc.

Feature

- feature.xml
 - Which plugins make up the feature (incl. which versions)
 - License, copyright etc.
 - Where to go for updates to this feature

Eclipse Update Site

- Where you install features from
- Made up of three parts
 - "features"-directory
 - "plugins"-directory
 - site.xml
- May be contained in a zip-file, may be a directory on local disk or network share, accessible over HTTP or NRPC (Notes only)
- Lotus Domino ships with an "Eclipse Update Site" template (accessible using HTTP and NRCP)
 - It's easy to use and we like easy!



Why do we need control?

1. Java extensions run with VERY broad permissions
2. No runtime execution control list (ECL) for Java extensions (yet!) so we need control at install time



Why do we need passports?

- Immigration officials have trust in my identity because it's stated in my passport
- They don't trust me but they trust the Danish government to issue passports to its citizens
- By holding a Danish passport they trust me to be a Danish citizen and of a given identity

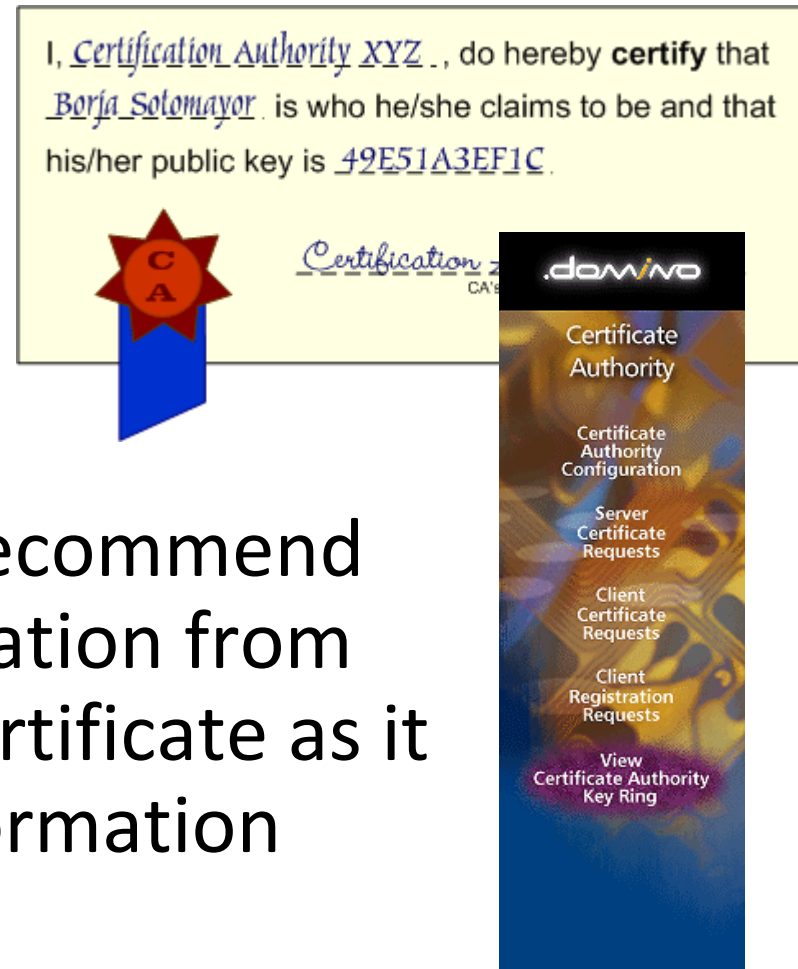


Certificates are passports for software

- Digital certificates are used to establish trust between pieces of software
- Uses public key cryptography
- A certificate has to be issued by someone
 - I may issue one to myself a.k.a. a self-signed certificate
- How do we decide who to trust? That's where we need a certificate authority such as VeriSign, Thawte or our selves...

Domino Certificate Authority

- Remember it?
- The template ships with Domino and you can use it to create a PKI for internet certificates
- If you're not in the US I recommend using the iKeyman application from IBM to create the root certificate as it doesn't require state information



Certificates as they relate to Notes

- All Notes users have a certificate issued by an organization or an organizational unit
 - The organization trusts organizational units to issue certificates
 - We all trust each other since we have a common certificate
- Notes ships with a public key infrastructure a.k.a. PKI
- Used to encrypt and sign data
- We call these "Notes certificates"

- For Java extensions we need an equivalent infrastructure but for internet certificates ("SSL certificates")

Two kinds of certificates

- In Notes we may also use internet certificates
 - Secure web access aka. HTTPS
 - Secure e-mail aka. S/MIME
- An internet certificate differs from a Notes certificate but the internet certificate for a user may be kept in the id-file (on the server it is kept in a key-ring file)
- Just like a Notes certificate may be used to verify a user identity so may an internet certificate

Trusting/deploying the internet cert.

- As with Notes certificates we trust internet certificates by cross-certifying them
- We deploy using Domino policies and the important piece is in the Security Settings document
 - This is new with Domino 8.5.1
- If you're on a pre-8.5.1 release you may roll your own but upgrading is probably easier...

Java signatures and Notes

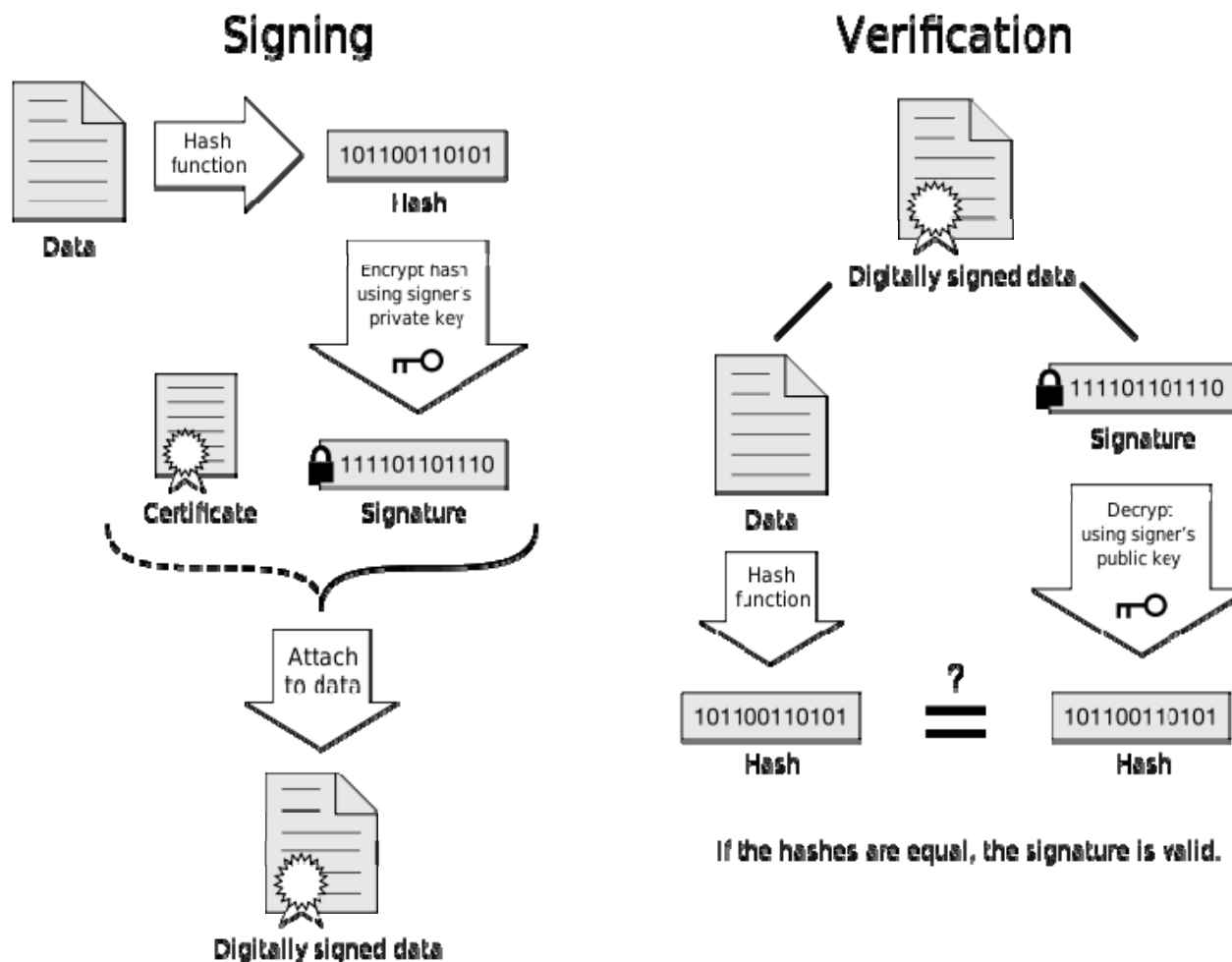
- Java signatures are verified by the Notes client at Java extension install time
- The public keys used to verify signatures are kept with the internet certificates
- Notes keeps internet certificates in the personal NAB (and private keys in the id-file)
- We only need to concern ourself with the internet certificates when discussing Java extension



Signing a JAR-file

- The Java Development Kit (JDK) ships with `jarsigner.exe` to sign JAR-files
- To sign: `jarsigner myfile.jar myalias`
- When signing we need a private key and a Java keystore to hold the key

What does it mean to sign something?



Deploying the Java extension

- You deploy Java extensions using MyWidgets and a widget catalog
- A widget is just a XML document
- We call the XML document a "widget descriptor"
- The widget descriptor may be crafted by hand or using the new "features and plugins" widget type in Notes 8.5.1

Remember: Extensions for Notes has to be packaged as features before they can be deployed

Where is the information you want to use to create your widget?

- Notes View, Document, or Form
- Web Page
- Feed
- Google Gadgets
- Features and Plugins

Widget descriptor (1/4)

```
<?xml version="1.0" encoding="UTF-8"?>
<webcontextConfiguration version="1.1">
<palletItem contributeToSideshelfOnStartup="false" doubleClickCommandId=""
  id="1534574583" imageUrl="" modified="false" title="Test widget"
  providerId="com.ibm.rcp.toolbox.prov.provider.ToolboxProvisioning"
  url="http://server1.example.com/__c125764a004795e6.nsf">
  <data><installManifest><![CDATA[
    <install>
      <installfeature id="com.example.feat1" name="Test widget"
        version="1.0.0">
        <requirements>
          <feature id="com.example.feat1" version="1.0.0"
            match="perfect" />
          <feature id="com.example.feat2" version="2.0.0"
            match="perfect" />
        </requirements>
      </installfeature>
    </install>
  ]]></installManifest></data>
</palletItem>
</webcontextConfiguration>
```

URL where the Eclipse update site is – may use the NRPC protocol if hosted on Domino

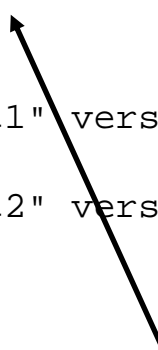
Widget descriptor (2/4)

```
<?xml version="1.0" encoding="UTF-8"?>
<webcontextConfiguration version="1.1">
<palletItem contributeToSideshelfOnStartup="false" doubleClickCommandId=""
  id="1534574583" imageUrl="" modified="false" title="Test widget"
  providerId="com.ibm.rcp.toolbox.prov.provider.ToolboxProvisioning"
  url="http://server1.example.com/__c125764a004795e6.nsf">
  <data><installManifest><![CDATA[
    <install>
      <installfeature id="com.example.featl" name="Test widget"
        version="1.0.0">
        <requirements>
          <feature id="com.example.featl" version="1.0.0"
            match="perfect" />
          <feature id="com.example.featl2" version="2.0.0"
            match="perfect" />
        </requirements>
      </installfeature>
    </install>
  ]]></installManifest></data>
</palletItem>
</webcontextConfiguration>
```

Part of the payload is the install manifest specifying what to install / uninstall...

Widget descriptor (3/4)

```
<?xml version="1.0" encoding="UTF-8"?>
<webcontextConfiguration version="1.1">
<palletItem contributeToSideshelfOnStartup="false" doubleClickCommandId=""
  id="1534574583" imageUrl="" modified="false" title="Test widget"
  providerId="com.ibm.rcp.toolbox.prov.provider.ToolboxProvisioning"
  url="http://server1.example.com/__c125764a004795e6.nsf">
  <data><installManifest><![CDATA[
    <install>
      <installfeature id="com.example.featl" name="Test widget"
        version="1.0.0">
        <requirements>
          <feature id="com.example.featl" version="1.0.0"
            match="perfect" />
          <feature id="com.example.featl2" version="2.0.0"
            match="perfect" />
        </requirements>
      </installfeature>
    </install>
  ]]></installManifest></data>
</palletItem>
</webcontextConfiguration>
```



We specify the feature to install by its ID and which version we want to install as there might be multiple versions of the same feature on the update site...

Widget descriptor (4/4)

```
<?xml version="1.0" encoding="UTF-8"?>
<webcontextConfiguration version="1.1">
<palletItem contributeToSideshelfOnStartup="false" doubleClickCommandId=""
  id="1534574583" imageUrl="" modified="false" title="Test widget"
  providerId="com.ibm.rcp.toolbox.prov.provider.ToolboxProvisioning"
  url="http://server1.example.com/__c125764a004795e6.nsf">
  <data><installManifest><![CDATA[
    <install>
      <installfeature id="com.example.featl" name="Test widget"
        version="1.0.0">
        <requirements>
          <feature id="com.example.featl" version="1.0.0"
            match="perfect" />
          <feature id="com.example.featl2" version="2.0.0"
            match="perfect" />
        </requirements>
      </installfeature>
    </install>
  ]]></installManifest></data>
</palletItem>
</webcontextConfiguration>
```

And we specify the requirements for the installation of the feature – notice that the feature itself is a requirement...

Live demo

Desktop settings (1)

Desktop Settings : Default desktop settings

Basics | Smart Upgrade | Applications | **Widgets** | Dial-up Connections | Accounts | Name Servers | SSL | Applet Security

Widget Settings		How to apply this setting:	Inherit from parent policy
Widget catalog server:	server1/Example	Set value whenever modified	<input type="checkbox"/> Inherit
Widget catalog application name:	widget_catalog.nsf	Set value whenever modified	<input type="checkbox"/> Inherit
Widget catalog categories to install:	Our Widgets, Provisioned Plugins		<input type="checkbox"/> Inherit
Enable Live Text:	Enable		<input type="checkbox"/> Inherit
Show the My Widgets panel in the sidebar:	Yes	Set value whenever modified	<input type="checkbox"/> Inherit
Restrict the addition of widgets to specific types:	Disable		<input type="checkbox"/> Inherit
Restrict provider IDs for installation/execution:	Disable		<input type="checkbox"/> Inherit
Restrict extension point IDs for installation/execution:	Disable		<input type="checkbox"/> Inherit
Create and manage an action:	Enable		<input type="checkbox"/> Inherit
Create and manage recognizers and content types:	Yes		<input type="checkbox"/> Inherit
Enable default recognizers:	Enable		<input type="checkbox"/> Inherit
Send widgets using e-mail:	Enable		<input type="checkbox"/> Inherit
Install widgets from e-mail or other:	Disable		<input type="checkbox"/> Inherit
Install widgets from catalog:	Disable		<input type="checkbox"/> Inherit
Publish to catalog so others can browse (subject to catalog ACLS):	Disable		<input type="checkbox"/> Inherit

Desktop settings (2)

Desktop Settings : Default desktop settings

Basics | Smart Upgrade | Applications | Widgets | Dial-up Connections | Accounts | Name Servers | SSL | Applet Security | Proxies | Mail | Preferences | Com

Basics | Miscellaneous | Window Management | Regional Settings | Internet | Mail | Instant Messaging | Replication | Network Ports | Fonts and Colors

Window Management		How to apply this setting:	Inherit from parent policy:	Enforce in child policies:
Window management:	New Tab	Set value whenever modified	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
Display sidebar:	Yes	Set value whenever modified	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
<u>On restart, reopen tabs:</u>	Yes	Set value whenever modified	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
Use large icons:	Yes	Set value whenever modified	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
Hide "Feeds" Panel:	No	Set value whenever modified	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
Hide "Day-At-A-Glance" Panel:	Yes	Set value whenever modified	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
Hide "Activities" Panel:	Yes	Set value whenever modified	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
Hide "Sametime Primary Contacts" Panel:	Yes	Set value whenever modified	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
Hide "Sametime Contacts" Panel:	No	Set value whenever modified	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce
Hide "My Widgets" Panel:	No	Set value whenever modified	<input type="checkbox"/> Inherit	<input type="checkbox"/> Enforce

Security settings (1)



Security Settings : Default security settings

Basics | Password Management | Execution Control List | Keys and Certificates | Signed Plug-ins | Portal Settings

On-line Certificate Status Protocol (OCSP) How to...

Enable OCSP checking

Administrative Trust Defaults How to...

▼ Certificate Links

[CN=Demo CA/O=Example/ST=CPH/C=DK](#)

Security settings (2)

Security Settings : Default security settings

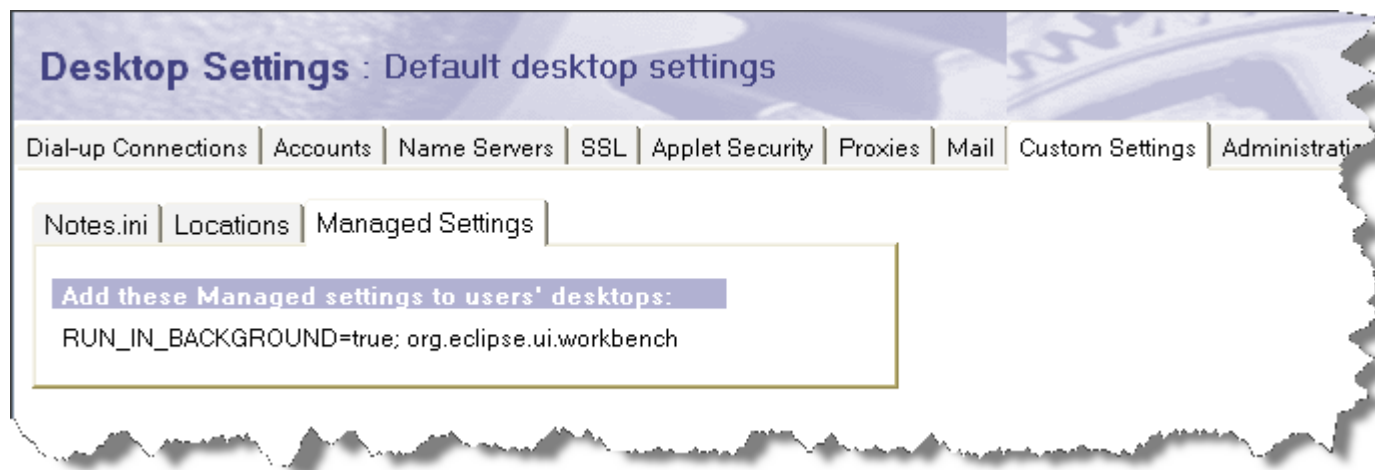
Basics | Password Management | Execution Control List | Keys and Certificates | **Signed Plug-ins** | Portal Server | ID Val

Signed Plug-in Basics		How to apply this setting:
Installation of plug-ins that are expired or not yet valid:	Never install	<input type="checkbox"/> Don't set value
Installation of unsigned plug-ins:	Never install	<input type="checkbox"/> Don't set value
Installation of plug-ins signed by an unrecognized entity:	Never install	<input type="checkbox"/> Don't set value
Trust IBM plug-in signing certificate:	Always trust for install	<input type="checkbox"/> Don't set value
Ignore expiration for time stamping certificate:	Never install	<input type="checkbox"/> Don't set value

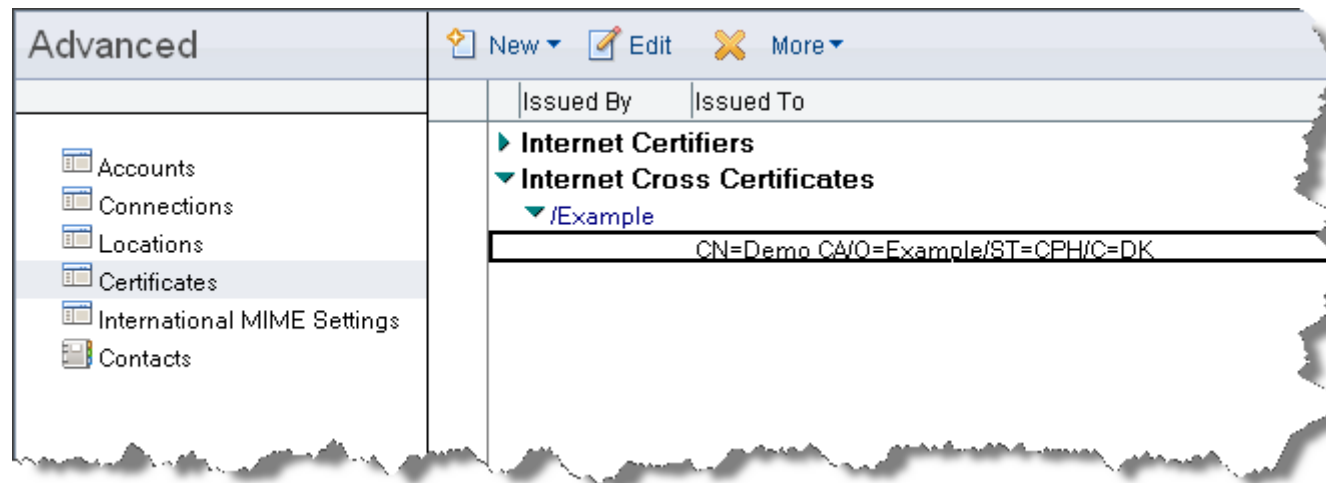
Interesting Eclipse settings

<notes>/data/workspace/.metadata/.plugins/
org.eclipse.core.runtime/.settings

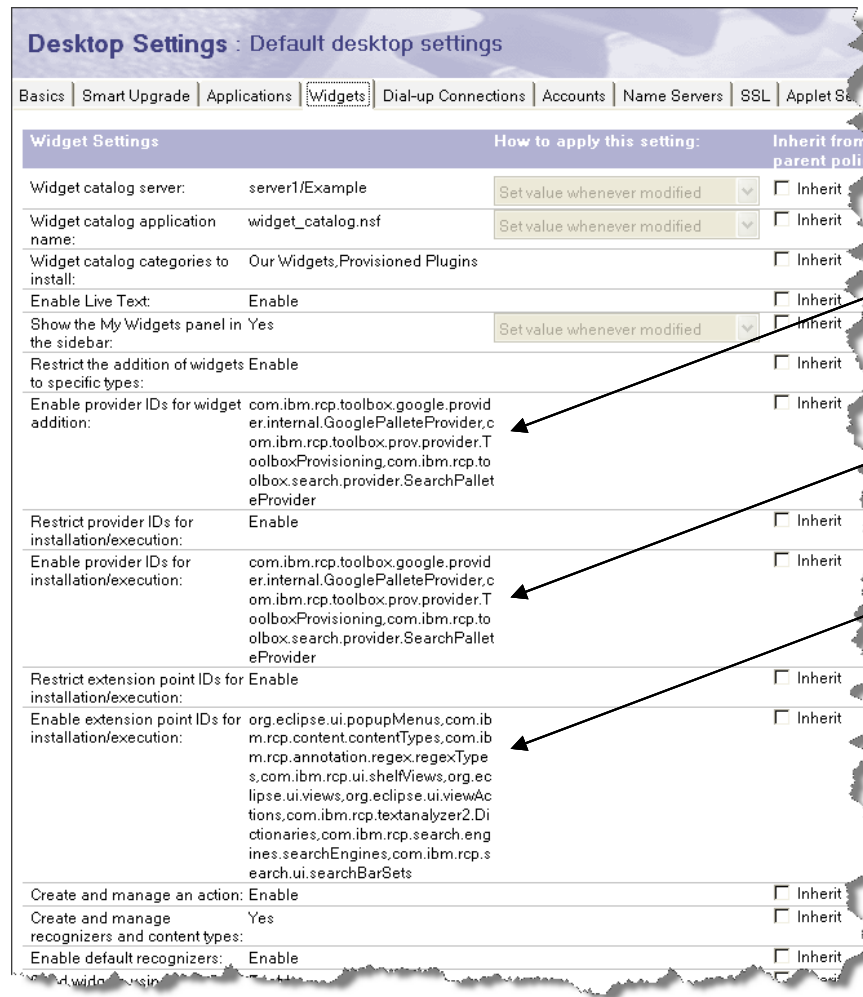
- org.eclipse.ui.workbench.prefs
 - RUN_IN_BACKGROUND=true



When deployed to the client



Restrictions, restrictions, restrictions

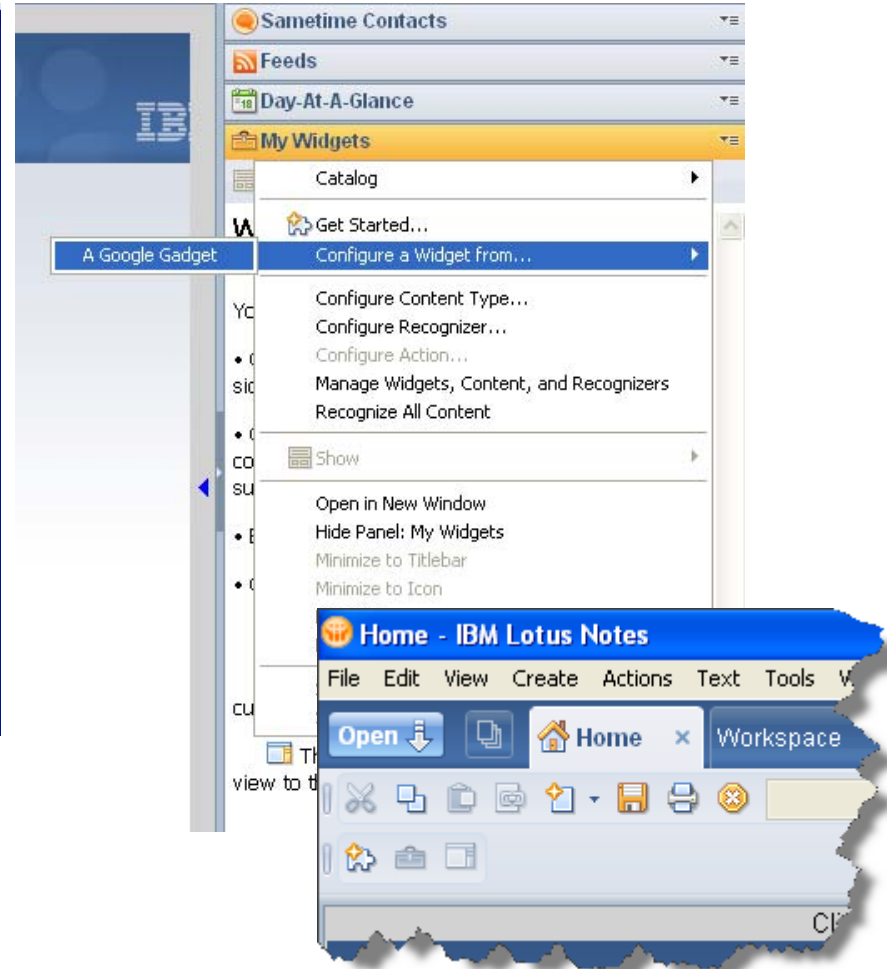
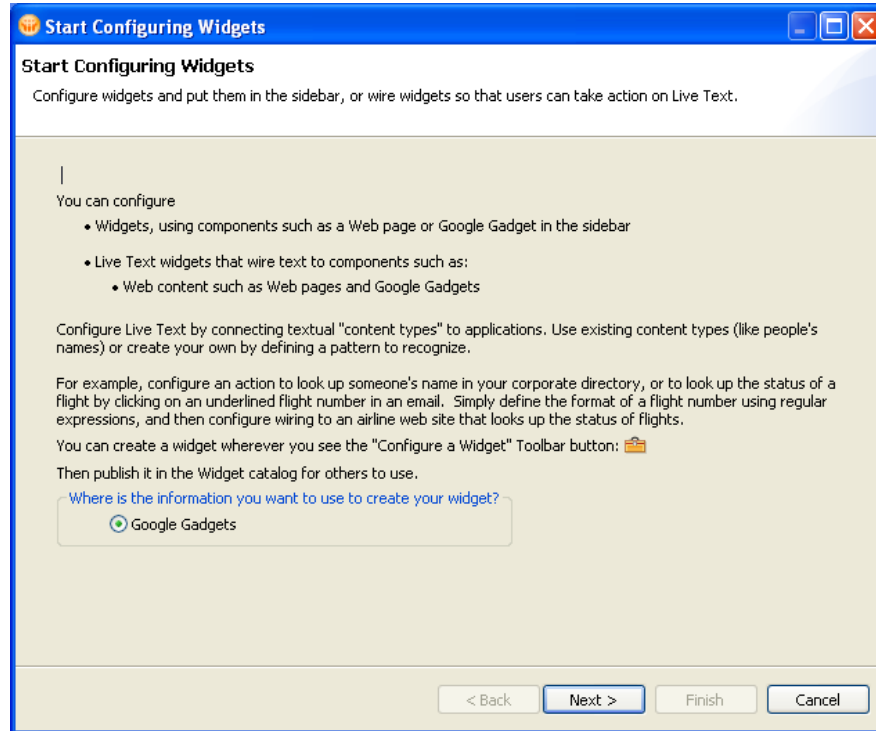


Which widget types may the user create using UI

Which widget types may the user install using UI/policies

Which extension points may the user install using UI/policies

Got a license to Google™



Restrict to widget types

- `com.ibm.rcp.toolbox.google.provider.internal.GooglePalletteProvider`
 - Allow Google gadgets
- `com.ibm.rcp.toolbox.web.provider.WebServicesPalletteProvider`
 - Allow widgets using web pages
- `com.ibm.rcp.toolbox.feeds.FeedPalletteProvider`
 - Allow widgets using feeds (Atom, RSS)
- **`com.ibm.rcp.toolbox.prov.provider.ToolboxProvisioning`**
 - Allows provisioning of Java extensions using widget descriptors
- `com.ibm.notes.toolbox.provider.NotesViewPalletteProvider`
 - Allow Notes views / documents in widgets
- `com.ibm.notes.toolbox.provider.NotesFormPalletteProvider`
 - Allow Notes forms in widgets
- `com.ibm.rcp.toolbox.search.provider.SearchPalletteProvider`
 - Allow widget to go into the search box

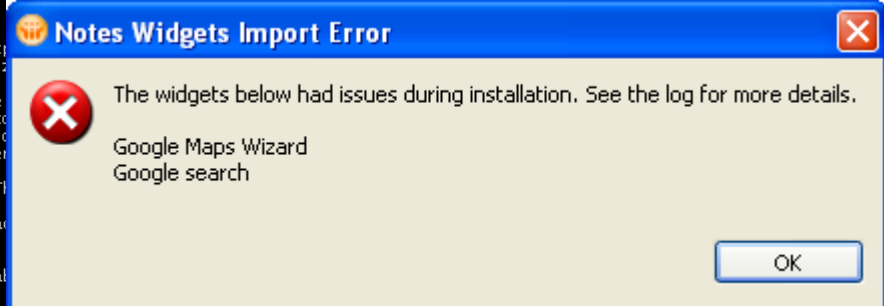
Restrict to extension points

- org.eclipse.ui.popupMenus
- com.ibm.rcp.content.contentTypes
- com.ibm.rcp.annotation.regex.regexTypes
- ***com.ibm.rcp.ui.shelfViews***
- ***org.eclipse.ui.views***
- org.eclipse.ui.viewActions
- com.ibm.rcp.textanalyzer2.Dictionaryes
- com.ibm.rcp.search.engines.searchEngines
- com.ibm.rcp.search.ui.searchBarSets

Pay attention to what you restrict

```

D:\Notes\framework\rcp\ eclipse\plugins\com.ibm.rcp.base_6.2.1.20090804-1912\win32\x86\notes2.exe
JIT - r9_20090213_2028
GC - 20090729_AA
Bootloader constants: OS=win32, ARCH=x86, WS=win32, NL=en
Framework arguments: -dir ltr -NPARAMS /authenticate -RPARAMS -personality com.ibm.rcp
m.ibm.rcp.personality.framework.RCPProduct:com.ibm.notes.branding.notes -plugincustomiz
in_customization.ini
Command-line arguments: -os win32 -ws win32 -arch x86 -dir ltr -NPARAMS /authenticate
m.ibm.rcp.platform.personality -product com.ibm.rcp.personality.framework.RCPProduct:cc
d:\Notes\Data\workspace -plugincustomization D:\Notes\framework\rcp\plugin_customizati
core.internal.logger.frameworkhook.writeSession() ::thread=Start Level Event Dispatch
ernal.logger.frameworkhook
2009/10/12 10:10:11.890 INFO ServiceEvent REGISTERED ::class.method=unknown ::thread=Th
rovisioning
2009/10/12 10:10:11.920 INFO BundleEvent STARTED ::class.method=unknown ::thread=Threa
sioning
12-10-2009 10:10:13.00 [0938:0002-0A30] InitGlobalProcessInfo> PID [2360] != [0]
2009/10/12 10:10:23.968 WARNING NLS missing message: NotesLockStatus in: com.ibm.colla
ssages ::class.method=unknown ::thread=main ::loggername=org.eclipse.osgi
2009/10/12 10:10:23.984 SEVERE CLFW0017E: Cannot install extensions for org.eclipse.ui.views because the administrator
has restricted extension installation. ::class.method=com.ibm.rcp.dynamic.extensions.DynamicExtensionRegistry.loadStore(
) ::thread=Worker-5 ::loggername=com.ibm.rcp.dynamic.extensions
2009/10/12 10:10:24.000 WARNING NLS unused message: com.ibm.collaboration_realtime_imhub_strings_messages$addGroup in: c
om.ibm.collaboration.realtime.notes.messages.messages ::class.method=unknown ::thread=main ::loggername=org.eclipse.osgi
2009/10/12 10:10:23.989 INFO BundleEvent STARTED ::class.method=unknown ::thread=Thread-4 ::loggername=com.ibm.rcp.toolbox
ox.utils
2009/10/12 10:10:24.000 SEVERE CLFW0071E: There were errors loading the Widget extension store. See the log file for mo
re details or contact your help desk. ::class.method=com.ibm.rcp.dynamic.extensions.DynamicExtensionRegistry.<init>() ::
thread=Worker-5 ::loggername=com.ibm.rcp.dynamic.extensions
2009/10/12 10:10:24.109 INFO BundleEvent STARTED ::class.method=unknown ::thread=Thread-4 ::loggername=com.ibm.rcp.toolbox
ox.admin
2009/10/12 10:10:24.111 INFO BundleEvent STARTED ::class.method=unknown ::thread=Thread-4 ::loggername=com.ibm.rcp.toolbox
ox
2009/10/12 10:10:24.112 INFO BundleEvent STARTED ::class.method=unknown ::thread=Thread-4 ::loggername=com.ibm.rcp.toolbox
ox.prov.provider
2009/10/12 10:10:24.343 SEVERE Invalid preference page path: Cache ::class.method=unknown ::thread=main ::loggername=org
.eclipse.ui
2009/10/12 10:10:24.313 INFO BundleEvent STARTED ::class.method=unknown ::thread=Thread-4 ::loggername=com.ibm.rcp.provi
sioning.ui
    
```



	parent pol	
value whenever modified	<input type="checkbox"/> Inherit	
value whenever modified	<input type="checkbox"/> Inherit	
	<input type="checkbox"/> Inherit	
	<input type="checkbox"/> Inherit	
value whenever modified	<input type="checkbox"/> Inherit	
	<input type="checkbox"/> Inherit	
	<input type="checkbox"/> Inherit	
	<input type="checkbox"/> Inherit	
	<input type="checkbox"/> Inherit	
	<input type="checkbox"/> Inherit	

- Enable provider IDs for widget addition: com.ibm.rcp.toolbox.google.provider.internal.GooglePaletteProvider Inherit
- Restrict provider IDs for installation/execution: Disable Inherit
- Restrict extension point IDs for installation/execution: Enable Inherit
- Enable extension point IDs for installation/execution: org.eclipse.ui.popupMenus Inherit
- Create and manage an action: Enable Inherit

ERROR!

```
2009/10/12 10:03:14.046 SEVERE
CLFWW0017E: Cannot install extensions
for org.eclipse.ui.views because the
administrator has restricted
extension installation.
::class.method=com.ibm.rcp.dynamic.ex
tensions.DynamicExtensionRegistry.loa
dStore() ::thread=Worker-4
::loggername=com.ibm.rcp.dynamic.exte
nsions
```

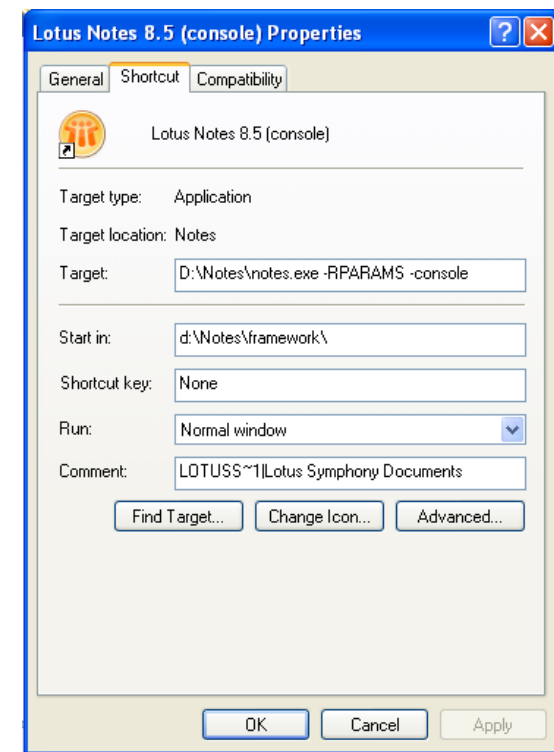
Debugging using OSGi console

```
<notes>/data/workspace/.config/rcpinstall.properties
```

```
– com.ibm.rcp.provisioning.level=FINEST
```

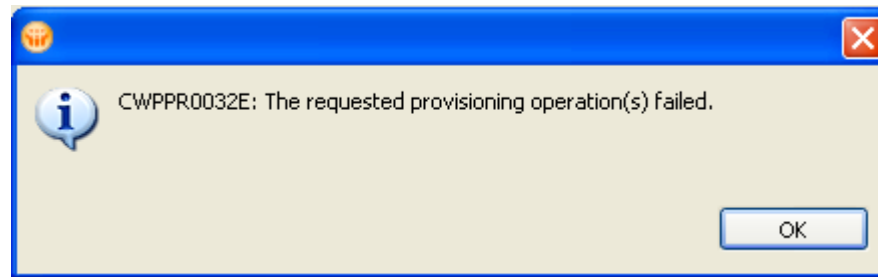
```
– com.ibm.rcp.toolbox.level=FINEST
```

```
<notes>/notes.exe -RPARAMS -console
```



Stay alert

- What then happens when trying to install unsigned feature?
- What if you change a feature after it has been signed?



Caveats

- Be aware that multiple widget categories in the desktop settings must be comma-separated
- There are numerous policy settings controlling MyWidgets you might want to look at while you're at it...
- Sometimes resetting the "categories to install" field to blank doesn't uninstall all widgets and comma separate multiple values
- Don't change the discovery URL using update site template for signed features as this will invalidate the signature
- Pay attention to what you restrict – both for widget types and extension points

Resources

- <http://lekkimworld.com/nllug2009>
 - Presentation, step-by-step demo-script and links will be available from Monday
- Domino Administrator help
 - Internet Certificates
 - Widget Deployment
- Lotus Expeditor Info Center
- Feel free to come by our booth to talk and discuss

Q&A

- But...
- How...
- Doesn't that mean?
- *Give it to me!!* 😊

