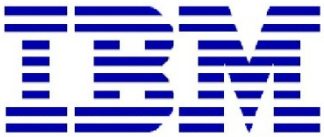


Proven Practice

Applying Cognos 8 Security to Controller 8.5.1 FAP

Product(s): IBM Cognos Controller

Area of Interest: Infrastructure

Copyright and Trademarks

Contents

1 Introduction

1.1 Purpose

This document is designed to be a simple/basic guide (complete with screenshots) for how to configure Controller 8.5.1 to that the FAP (TM1) functionality uses Cognos 8 Security.

This document is intended to be utilised by IBM Cognos (and partners) technical consultants, to help perform this configuration in '**simple / standard**' environments.

It is also possible for less-experienced people (for example customer's I.T. departments) to use this document too, **so long as**:

- It will be a simple/standard implementation of Controller
- The customer accepts responsibility for any problems that may arise from the use of this document
    - In other words, the customer accepts that IBM's recommendation is always to employ an experienced IBM Cognos Technical Consultant to help them install Controller.
    - Employing an experienced IBM technical consultant will ensure that the risk is minimised of unexpected issues arising from an upgrade.

By following these "best practices" the intention is to make Controller configuration as easy as possible, with the minimum of possibility for errors/issues.

The author suggests that experienced technical consultants can also use this document as an 'aide-memoir', i.e. a concise set of instructions for installing the software as per current best practices, for typical situations.

1.2 Applicability

This document is based on installing Controller 8.5.1 RTM (released July 2010)

1.3 Exclusions and Exceptions

There are an infinite variety of possible customer I.T. environments/needs/specialist requirements. Therefore, IBM has intentionally made Controller flexible to give the customer many different ways to install/configure Controller 8.5.1. Therefore the advice in this document may have to be modified by the reader to fit in with their specific needs/environment.

Although this document demonstrates proven practices suitable for most environments, it is not necessarily perfect for all environments.

Employing an experienced IBM Cognos technical consultant to upgrade your Controller server(s) is always the recommended & ideal scenario.

This document is not intended to entirely replace the official 'standard' documentation (located on the install CDs) such as:

- `tm1_install.pdf` – IBM Cognos TM1 - Installation Guide

Instead you can use this guide as a concise summary companion to the official documentation. In any event of overlap, the standard documentation takes precedence.

NOTE: This document was last updated by the author February 22nd 2011.

2 Important Notes, Tips and WARNINGS

2.1 Hints & TIPS

Throughout this document, there will be hints & tips in blue boxes such as this one:

TIP: Ignoring the tips may cause the Controller system to be slow, unreliable or have long-term issues.

In addition, there are will be VITAL information inside red boxes

WARNING: If the information in these boxes is ignored, the Controller system is likely not to work at all correctly.

Many of the author's tips and recommendations refer to IBM's excellent knowledgebase, which contain the IBM "Technotes" (previously known as "KB articles"). This can be found here:

http://www-01.ibm.com/software/data/cognos/products/cognos-8-controller/support/search.html

It is absolutely VITAL that the reader uses this **knowledgebase** resource, since it is an invaluable help for almost all issues.

In addition, all public **Proven Practice** documents can be found here:
http://www.ibm.com/developerworks/data/library/cognos/cognosprovenpractices.html

2.2 Server name conventions – FQDN and NetBIOS

Throughout this document, the author shall talk about configurations that refer to the **<servername>** of your Controller server. There are two main conventions for server naming:

1. NetBIOS – for example '`MYSERVERNAME`'
2. FQDN – for example '`MYSERVERNAME.uk.companyname.com`'

Alternatively, you may even be using something else to refer to your servers. For example, you may want to use a "virtual" DNS name (for Disaster Recovery purposes).

Whatever naming convention that you choose, you *must* use the SAME (correct) version of your server name at *all* times, to retain consistency.

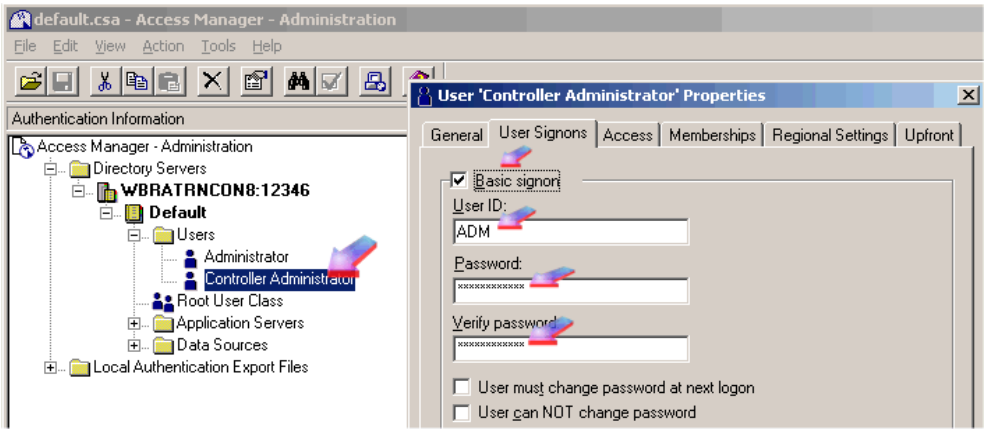
WARNING: To summarise, customers should typically use NetBIOS or FQDN names **throughout their entire configuration/deployment**, but not both (a mixture).
Using a mixture of naming conventions will cause complications/problems later.

3 Definitions, Prerequisites and General Overview of process

3.1 Definition of term "Cognos Access Manager" (CAM)

Before continuing, be aware that when referring to the term 'Access Manager' people can mean two very different things. When people say "Access Manager" they can mean two very different things:

1) **"Access Manager"** – a tool that was distributed with earlier Cognos products (typically Series 7 products, and other products such as Cognos Planning 7.3 etc.).
   - *Typically this would involve installing a dedicated Cognos-only LDAP source such as SunONE.*
   - *Below is a printscreen of the product/tool in action:*



2) **"Cognos Access Manager (CAM)"** – A component/module of the Cognos 8 BI security subsystem, whose job/role is to handle Cognos 8 security.
   - *Typically, most customers configure this to point to their Microsoft Active Directory.*

In this document, when we mention the term CAM / Cognos Access Manager we are thinking of the second (2) meaning.

In other words, when we say we are using 'CAM' security with TM1, we simply mean that we shall configure TM1 / FAP to use Cognos 8 security.

3.2 Overview of TM1 / CAM security integration

Controller 8.5 RTM came bundled with TM1 9.4.1. Authorization for the CAM users in TM1 9.4.1 needed to be defined in TM1 through standard TM1 functionality. Controller users and authorization groups were not published.

To solve that issue, the following security modes are now available when using Controller/ FAP **8.5.1** and TM1 **9.5.0**:

(1) Basic Security Mode

 # Can be used in both TM1 9.4.1 and TM1 9.5:

Controller users and authorization groups are published and can be leveraged if CAM authentication is not used to access the FAP cube (for example from the TM1 Excel plug-in, but not from BI).

Note: TM1 users and authorization groups are deleted at initial publish.

(2) CAM Security Mode

 # For TM1 9.4.1:

All CAM users in Controller will be published but without the integrated security from Controller existing in the TM1 cube.

 # For TM1 9.5:

Integrated security between Controller and TM1. This means that users and authorization groups in Controller are published to TM1. Then for all CAM users present in TM1, the CAM user ID will be connected to the Controller user ID (provided the CAM information has been maintained in Controller) and get the appropriate authorization group(s).

TM1 Security Mode Settings not supported by Controller 8.5 FP1 will abort the initial publish process and the datamart will be set to Error. The following TM1 API security modes are not supported:

- **Distributed** - Distributed implies that the TM1 server is a distributed server that accepts connections without specifying any credentials.
- **Mixed** - Mixed implies that the TM1 server accepts user authenticating either using Basic authentication or Windows Integrated Authentication.
- **WIA** - WIA implies that the TM1 server accepts connections that can authenticate based on Windows Integrated Authentication.

TIP: For more information on TM1 Security mode settings, search for "`IntegratedSecurityMode`" in this document, and also see separate IBM Technotes such as #1449693.

3.3 Choice of Security Provider (AD, LDAP, NTLM etc.)

Cognos 8 BI can integrate with almost any type of security provider. However, this document shall assume that the customer would like to integrate with the most popular option (Microsoft Windows Active Directory).

3.4 Warning

Please note that:

- The steps inside this chapter may have already been done by the customer already
- This document is NOT designed to be an in-depth document for how to configure Cognos 8 security.
  - Instead, it is designed to concentrate on how FAP/TM1 integrates with it
- This document shall choose all the 'default' options for configuration
  - Some customers will want/need to choose different settings/values
- For more/full details on how to configure Cognos 8 BI security, see separate IBM Technotes:
  - http://www-01.ibm.com/support/docview.wss?uid=swg21380097
  - http://www-01.ibm.com/support/docview.wss?rs=0&uid=swg21380098
  - http://www-01.ibm.com/support/docview.wss?uid=swg21380099

TO SUMMARISE:

- This document describes a SIMPLIFIED method of configuring Controller to use Cognos 8 BI security.
- You **must** read the FULL documentation (see links above) to understand all the optional steps that this document intentionally skips
- For example, see the documentation relating to the following concepts which this FAP document intentionally does NOT cover:
  - Choosing between using **Kerberos delegation** or **Remote_User** variable
  - Using the optional **chaseReferrals** and/or **MultiDomainTrees** options

3.5 VITAL: Ensure that all the following steps are performed when logged on as the Cognos/Controller 'service account' Windows user

In general, customers will have already created a Controller/Cognos "service account". This is a Windows domain user (for example "`DOMAIN\Controller_system`") under which many of the Controller processes run.

- For example, the Controller COM+ application should be running under this account

Again in general, this service account will be the one that will be running other Cognos-related processes (for example the TM1 Admin server Windows service).

⇨ **VITAL RECOMMENDATION**:
All the following instructions/configuration should be done whilst logged on with this 'service account' Windows user (for example `DOMAIN\Controller_system`).

Failure to adhere to this recommendation may make troubleshooting any problems much more difficult later.

4 Configure Cognos BI to use Cognos 8 Security

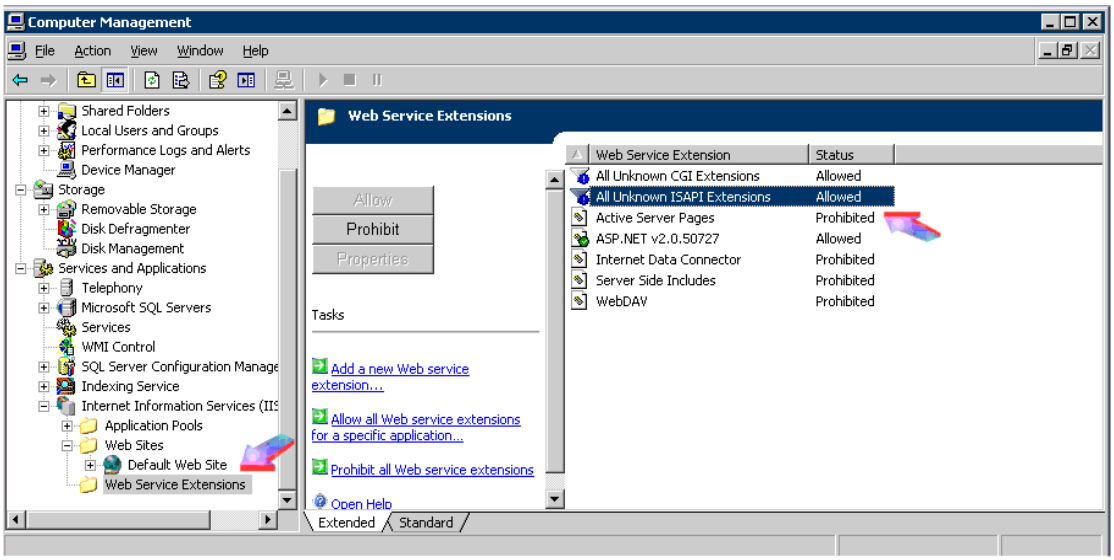
4.1 Ensure that Report Server is set to use ISAPI (not CGI)

The default setting for the Cognos 8 BI report server is to use CGI (not ISAPI). In 90% of circumstances/situations this is perfectly OK.

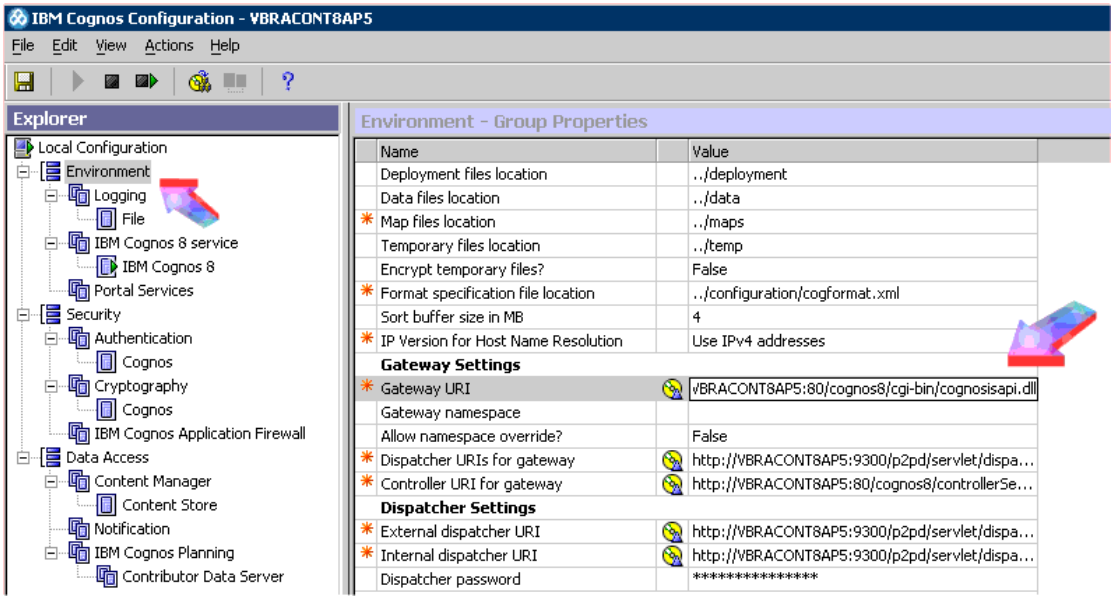
However, in certain circumstances (for example when testing Single Sign On (SSO) remotely via Microsoft Remote Desktop (RDP)) using CGI can cause a problem (see Technote 1380204).

Therefore, the author recommends that (before continuing) ensure that your Controller system is set to use ISAPI, by performing the following steps:

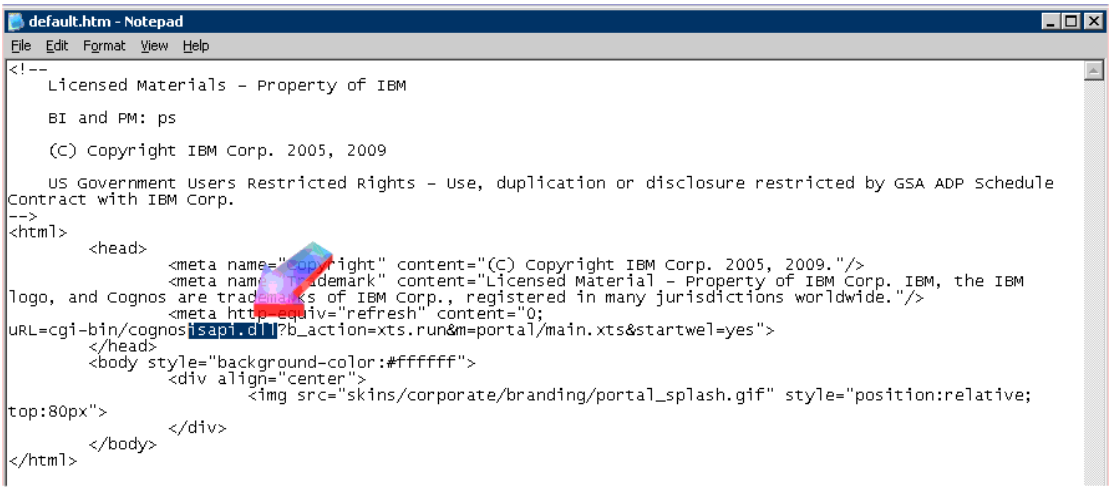
- On the **Cognos 8 BI Report Server**, inside the Microsoft **IIS** administrative manager tool, ensure that "**Allow unspecified ISAPI modules**" is ticked



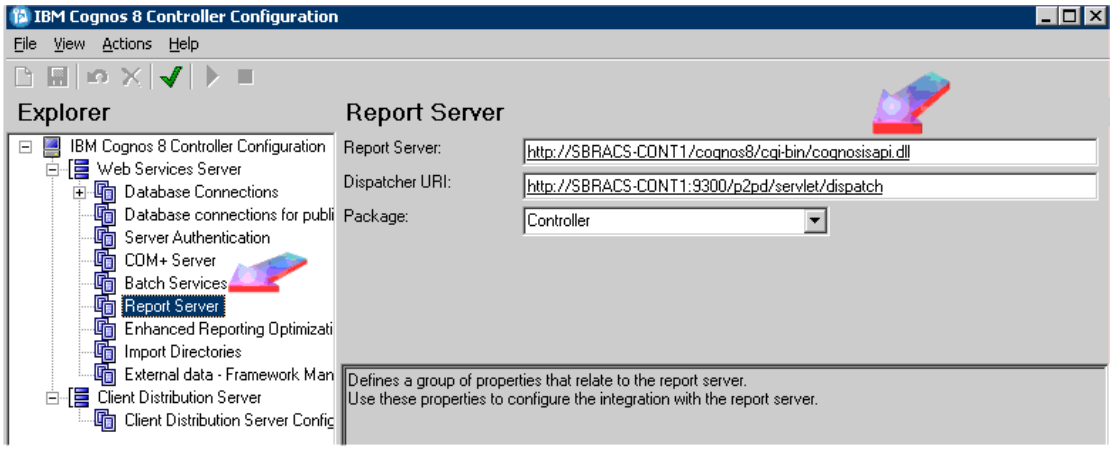
- Launch **Cognos Configuration**
- Locate "**Environment**" – and then search for "**Gateway URI**"
- Modify the entry from "**cognos.cgi**" to instead have "**cognosisapi.dll**" at the end of the value



- Click "**Save**"
- Restart the Cognos8 BI service
- Launch the following (assuming Cognos BI was installed into default location):
  `Notepad.exe c:\program files\cognos\c8\webcontent\default.htm`
- Modify the entry from "**cognos.cgi**" to "**cognosisapi.dll**" instead



- Repeat the above for the file `c:\program files\cognos\c8\webcontent\index.html`
- Finally, on the **Controller** application server, launch "**Controller Configuration**"
- Inside the "**Report Server**" section, change the setting to use **cognosisapi.dll**:



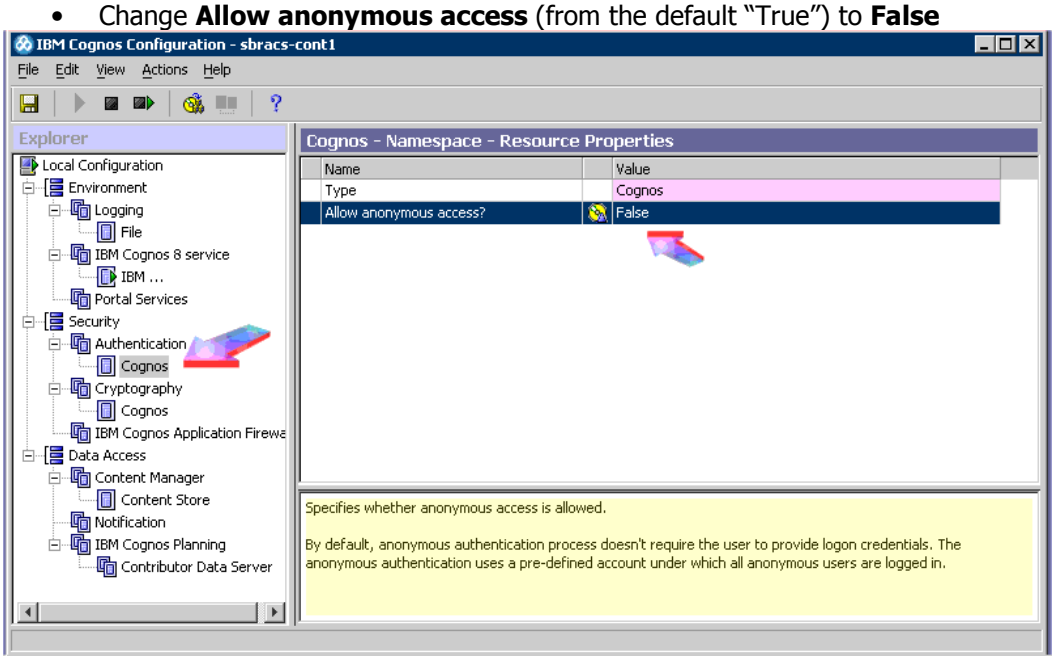
Finally, **before continuing**, ensure that you launch Controller and ensure that Standard Reports work OK.

TIP: For full details of the above, see the author's companion document "Installing & Configuring IBM Cognos Controller 8.5.1 server - Proven Practice".

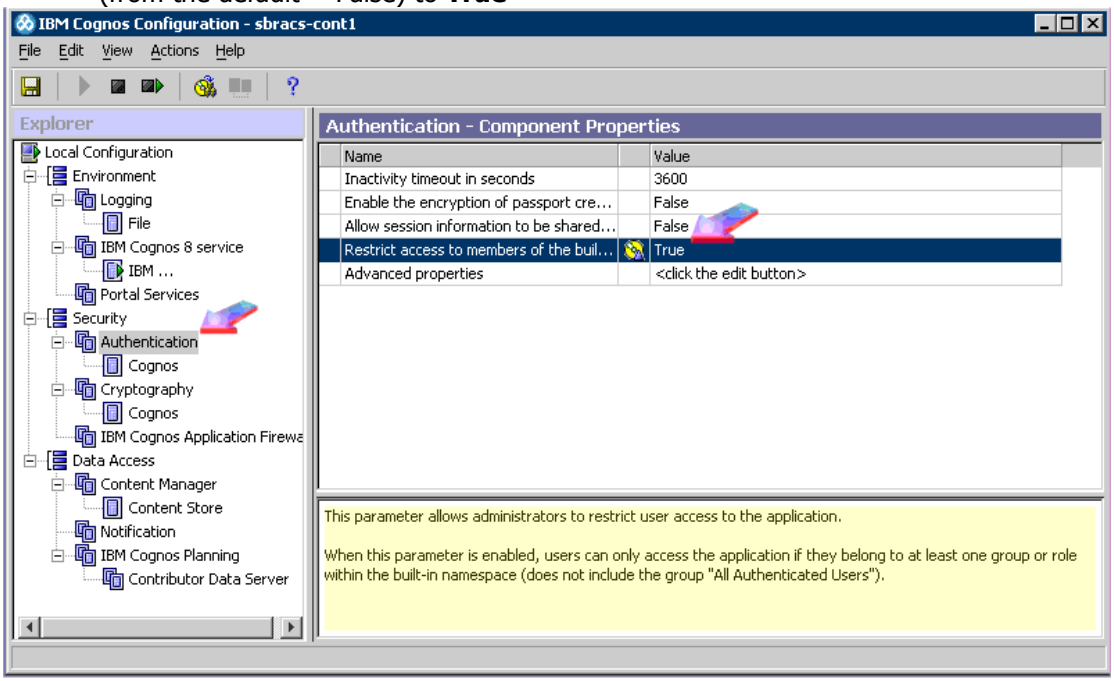
4.2 Disable Anonymous Access & Restrict User Access to the Cognos Namespace

Obtain some downtime (no users on the system). Then, on the Controller 8 application server:

- Start **IBM Cognos Configuration** from the Start Menu
- In the **Explorer** window, under **Security**, **Authentication**, click **Cognos**
- Change **Allow anonymous access** (from the default "True") to **False**



- Under **Security**, click **Authentication**
- Change the value of **Restrict access to members of the built-in namespace** (from the default = False) to **True**



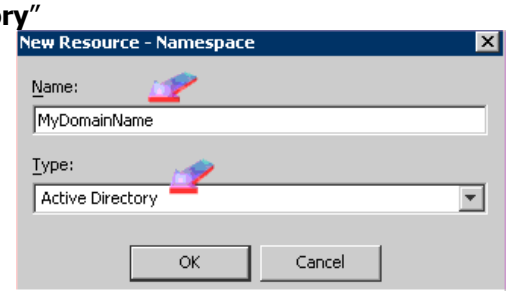
- Click **File** - **Save**.

4.3 Configure an Active Directory Namespace

Again inside **Cognos Configuration:**

- Under Security, right-click **Authentication**, and then click **New resource**, **Namespace**

- In the **Name** box, type a name that you want to give to your authentication namespace (for example "`MyDomainName`"), and ensure the "**Type**" is set to "**Active Directory**"



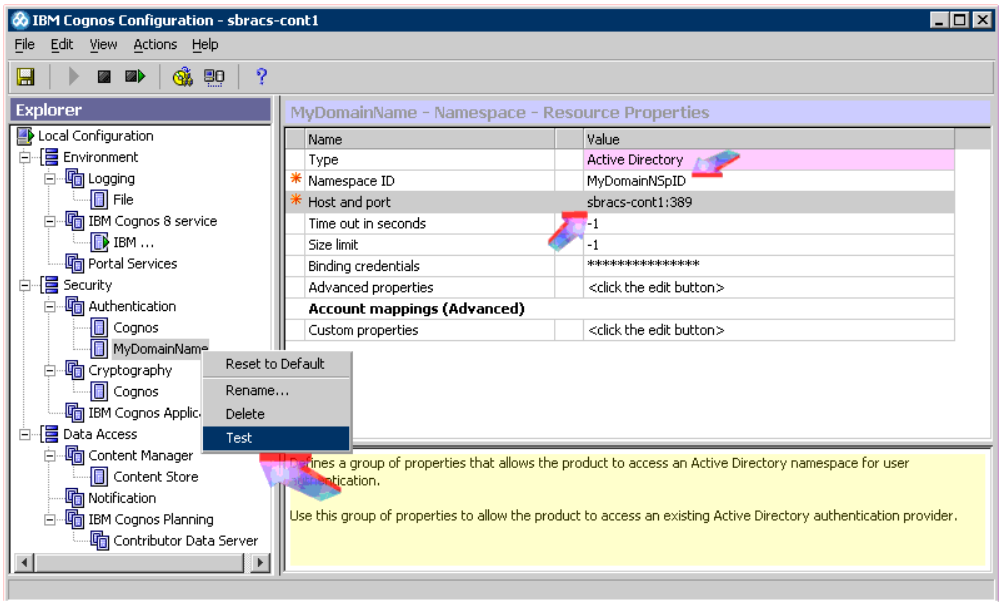
- **Namespace ID** property: Note how this does **not** have to be the same as the 'Name'. To demonstrate the difference, I have called it "`MyDomainNSpID`"

IMPORTANT: This value is going to be very important (used widely later) to please get this value correct from the very start!

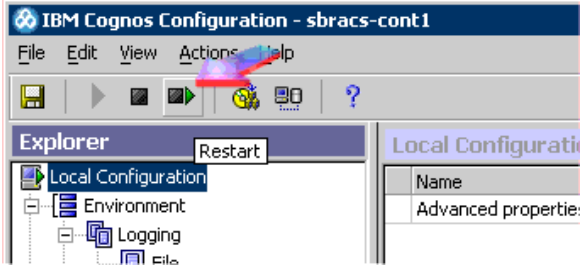
- Specify the values for all other required properties to ensure that Cognos 8 components can locate and use your existing authentication provider
    - e.g. **Host and port – <**one of your domain controllers>:389

IMPORTANT:
*In most environments, there is **no need** to fill in the section 'Binding credentials' (because most Windows domains allow anonymous LDAP querying).*

- Click **File** – **Save**
- Test the connection, by right-clicking the new authentication resource and click **Test**:



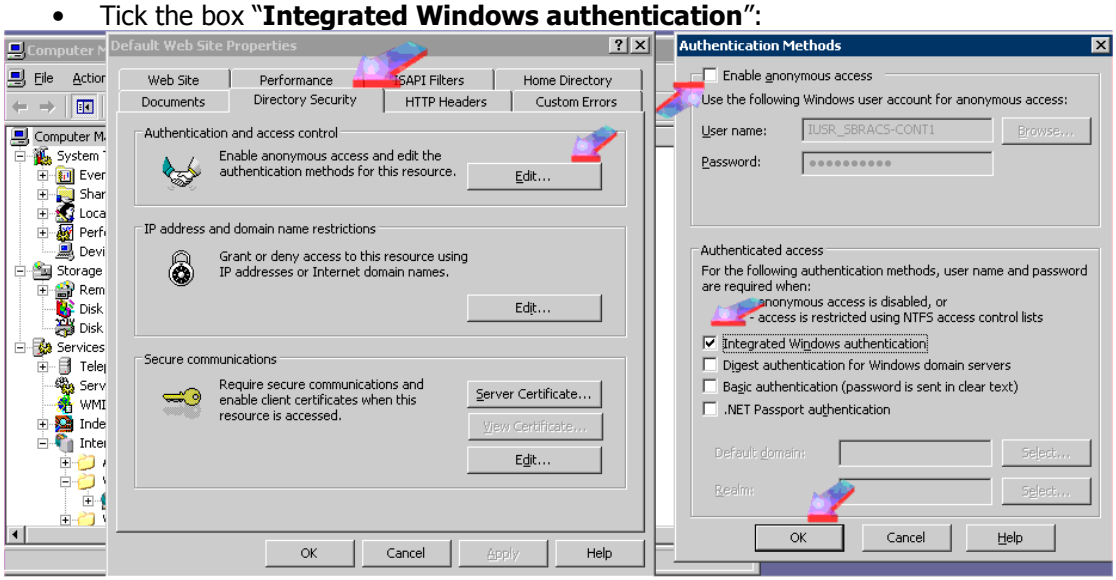
- Finally, **Restart** the IBM Cognos 8 service by clicking on the icon:



4.4 Enable "Integrated Windows Authentication" on the IIS Web server

To enable **Windows Integrated Authentication** on the IIS Web server (typically on the "**Default Website**") simply:

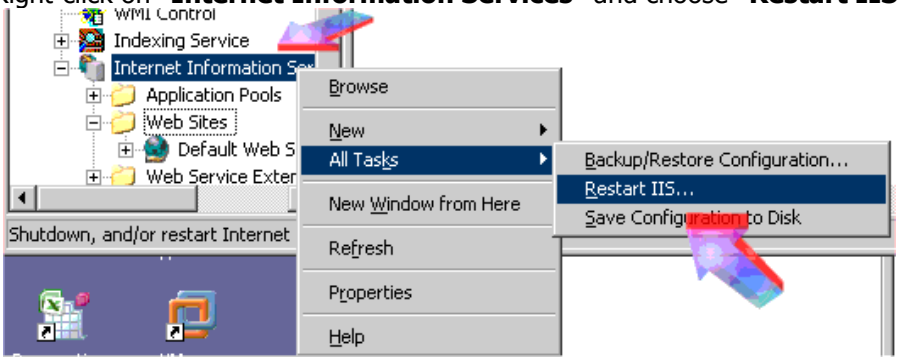
- Right-click on "**Default Web Site**" and choose "properties"
- Click tab "**Directory Security**"
- Under "**Authentication and access control**" click "**Edit**"
- Untick the box "**Enable anonymous access**"
- Tick the box "**Integrated Windows authentication**":



NOTE: The application server must be part of the domain where the users are located.

- Click **OK**, **OK,** Select ALL**, OK**

- Right-click on **"Internet Information Services"** and choose **"Restart IIS":**



4.5 Enable "Single Sign On" on the application server

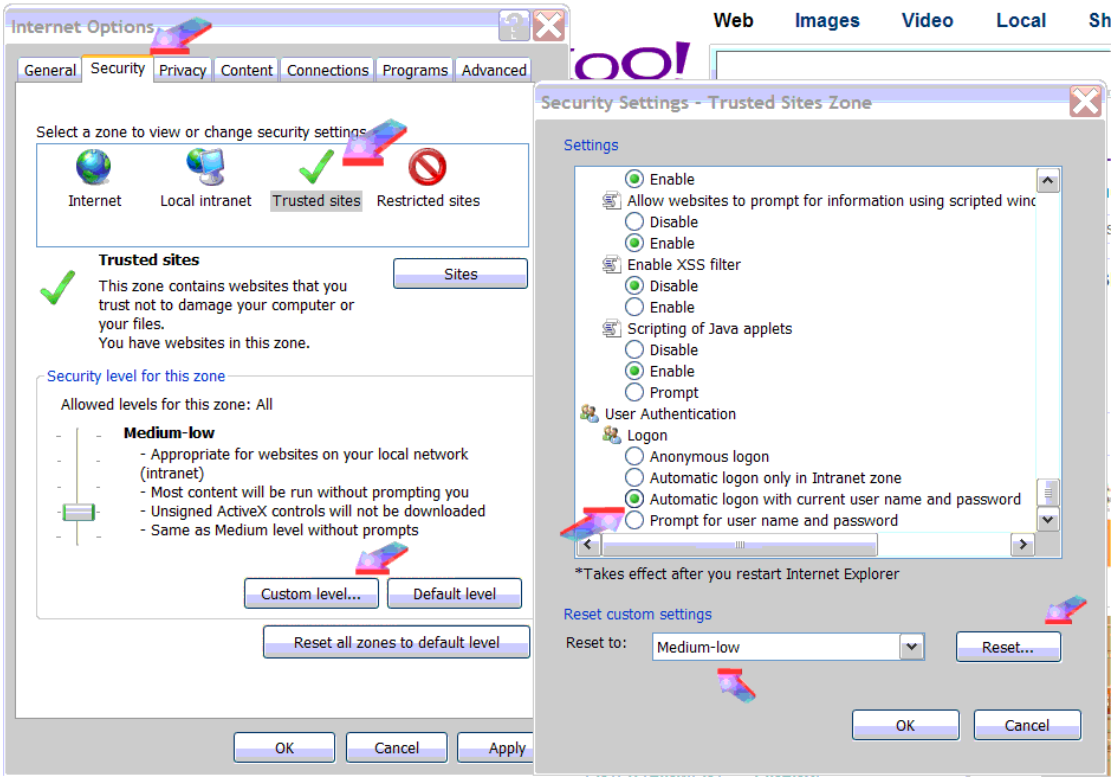
VITAL:
To repeat an earlier section, **especially for this section** the following instructions need to be done whilst logged onto the server with the same 'service account' Windows user (for example `DOMAIN\Controller_system`) that runs the TM1 server Windows services.

- Launch **Internet Explorer**. Click "**Tools – Internet Options**"
- Click "**Security tab**". Highlight "**Trusted sites**"
- Click "**sites**"
- If the box "Require server verification (https)... is ticked, then **UNTICK** this box
- Type the Report server's website (for example **http://biserver**) into the box, and click "Add"

NOTE:

- This server is the one that you will use inside the file "tm1s.cfg" (see later in this document)
- Ensure that you use the SAME naming convention (NetBIOS or FQDN) as you use elsewhere in these instructions

- Click "**OK**"
- Ensure that **'Trusted sites'** is still selected
- Click "**Custom Level**"
- Change the value inside "Reset to" to "**Medium - Low**"
- Click "**Reset**"
- Click "**yes**" to confirm that you want to change the settings
- Scroll to the bottom of the 'Security Settings' list
- Change the "**User Authentication - Logon**" settings from "Automatic logon only in Intranet zone" to "**Automatic logon with current user name and password**"

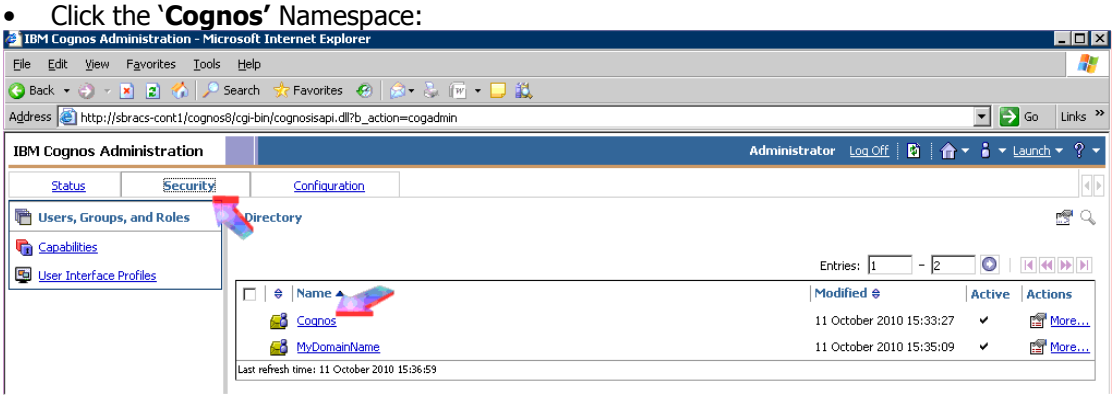


- Click "OK"
- Click "yes" to change the settings
- Click "OK"

5 Configure Controller to use Cognos BI Security

5.1 Configure Users and Groups inside the Cognos Connection portal

- Open Cognos Connection (for example http://<application_server_name>/cognos8)
- If prompted, click "**Administer IBM Cognos content**"
- Click **'Security'** tab
- From the **Tools** menu, click **Directory**
- Click the '**Cognos'** Namespace:



- In the **Actions** column, click the properties button for the **Controller Administrators** role:

- Click the **Members** tab
- Click **Add**
- Browse/navigate through your new namespace (for example "**MydomainName**") and choose all the users who are 'superusers' on the Controller system, plus also the Controller "COM+" Windows user account

TIP: There are several methods for adding users. Choose the one that is most convenient for you:

Method#1 - Choose from listed entries, using the GUI:

- Click to open the appropriate namespace (e.g. 'TESTDOMAIN')
- Navigate and open the folder (e.g. 'Users') that contains the Windows Domain User(s) that you wish to add
- Tick the box 'Show users in the list'
- Tick the checkboxes next to the user(s) (and/or groups and roles) that you wish to add (on the left hand side of the screen)

Method#2 - Search for entries:
Click **Search** and in the Search string box, type the phrase you want to search for. For search options, click **Edit**, **Find**, and click the entry you want

Method#3 – Manually type in entries:
Manually type the name of entries you want to add: click **Type** and type the names of groups,roles, or users using the following format, where a semicolon (;) separates each entry:

```
namespace/group_name;namespace/role_name;namespace/user_name;
```

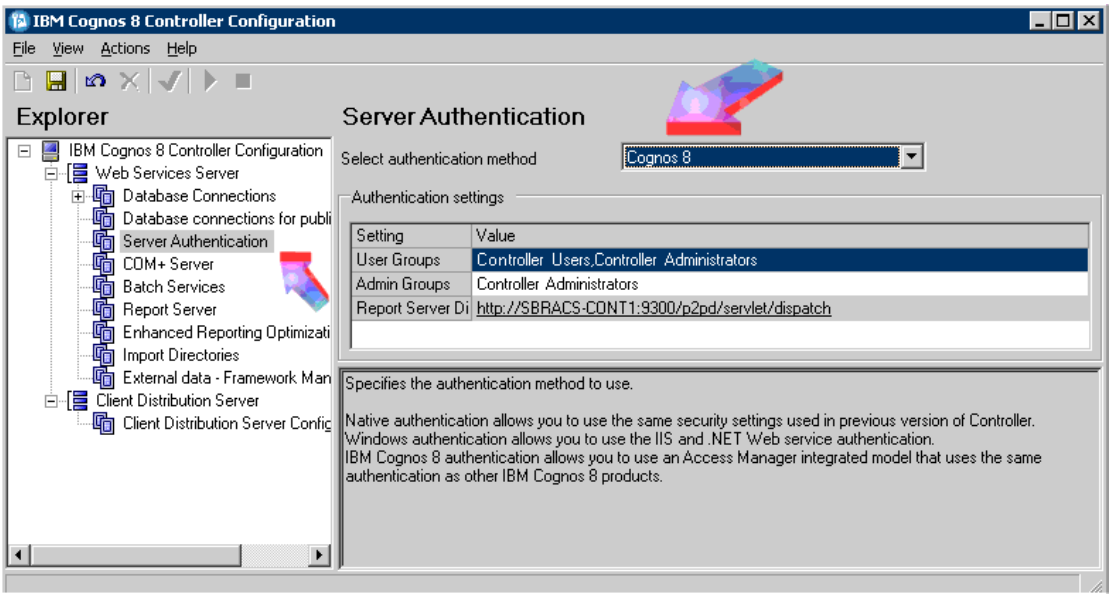
Here is an example: `Cognos/Authors;LDAP/scarter;`

- Repeat the above steps for the **Controller Users** role, but this time:
  - Add the 'normal' users to this role
  - Also add the Cognos namespace group "Controller Administrators" into this role too

- For top security, remove the group 'Everyone' from this role.

5.2 Configure Controller to use Cognos 8 Authentication

- Launch Cognos Controller Configuration
- Change the security authentication setting from "native" to "**Cognos 8**" authentication

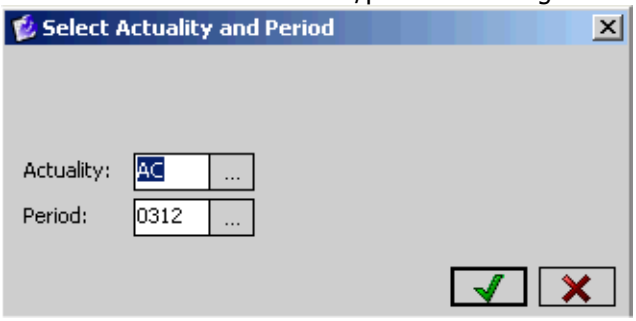


- Click 'save'

5.3 Map Cognos Controller Users to Cognos 8 Users

In other words, we shall now create an association between the users defined in the Controller application, and those defined in the Cognos 8 namespace roles:

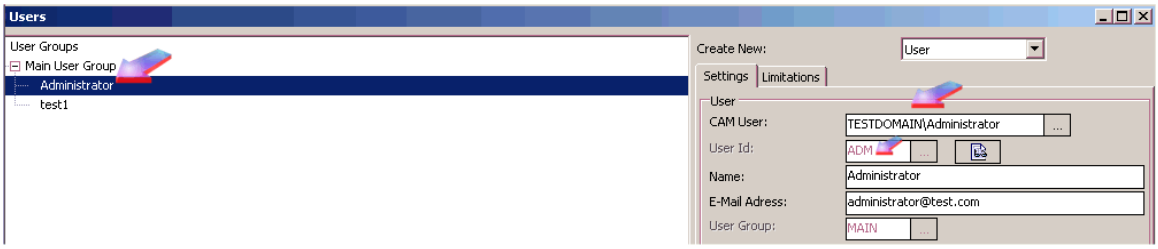
- Ensure that you are logged into Windows **using a Windows username that is a member of the 'Controller Administrators' role in Cognos Connection**
- Launch Cognos Controller
- Notice how you are **not** asked for a username/password to logon with:



This is because the first time you launch Controller (after having performed the above) Controller automatically links the user "ADM" (i.e. the Controller user called "Administrator") with whoever the Windows user is who has just logged on

2. From the **Maintain** menu, click **Rights**, **Users**.

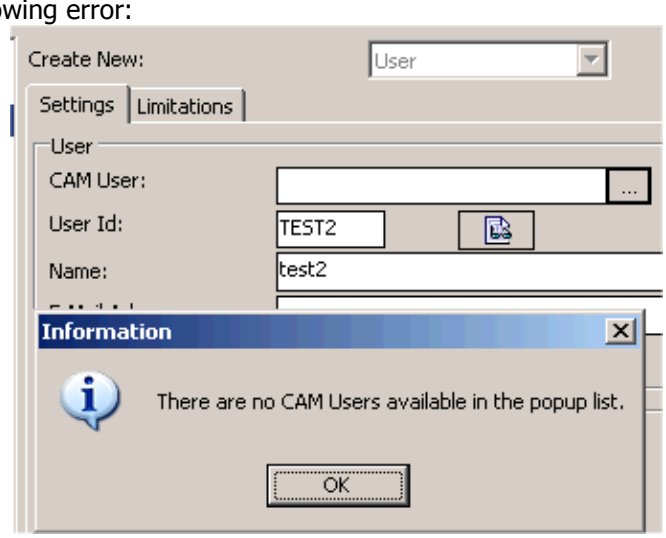
You will see something similar to the following:



In other words, *in this database that we've just logged onto* (although it will **not** affect **all** the databases – e.g. 'live', 'test', 'training') the user ADM is now associated with the Windows user TESTDOMAIN\Administrator

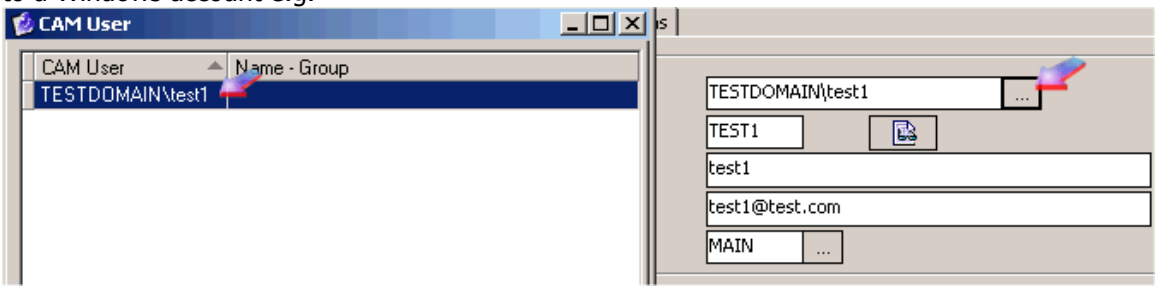
3. In the **Create New** box, click the drop-down arrow and then click **User**.
4. Beside the first **User Id** box, click the browse button, and then select the user as defined in the Cognos 8 namespace roles.

If you get the following error:



…then it is likely that you need to reconfigure your groups/members inside Cognos Connection. In other words, you need to add users into the groups "Controller Users" and "Controller Administrators".

Once you ensure that there are valid users inside the relevant groups (Controller Users and Controller Administrators) then you should be able to create new users, and new associations to a Windows account e.g.



5. Beside the second **User Id** box, click the browse button, and then select the user as defined in
the Cognos Controller database.
6. In the **Name** box, type the name of the Cognos Controller user.
7. In the **E-Mail Address** box, type the email address for the Cognos Controller user.
8. Beside the **User Group** box, click the browse button, and then select the user group for the
Cognos Controller user.
9. Under **Options**, select the appropriate checkbox to identify the user.
You can identify the user as either a Cognos Controller User or Cognos Controller Administrator.
You can add optional comments for the user, as well as the user's location.
10. Click Save.

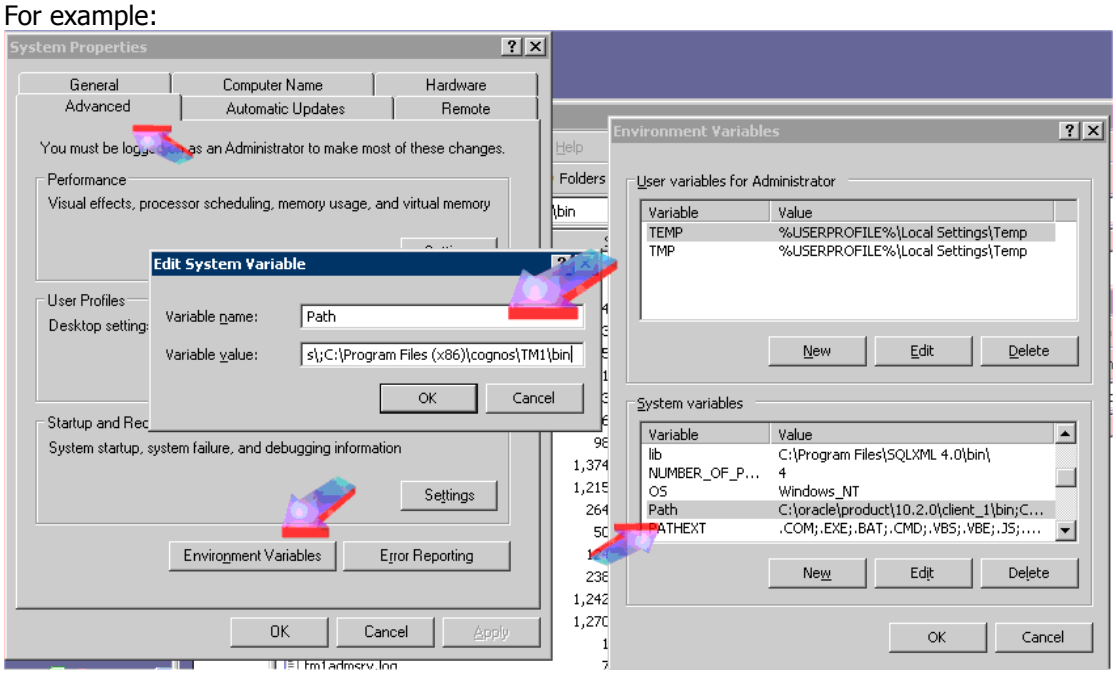
6 Configure FAP to use Cognos 8 security

6.1 Ensure that the server's PATH system variable points to the TM1 BIN

If necessary, modify the server's PATH system environment Variable to add …TM1\bin\:

TIP: By default, this location is: `C:\Program Files\cognos\TM1\bin\`

For example:



6.2 Set the security to be 'mixed' to add a new network user

- On the relevant server, open the 'tm1s.cfg' file (that relates to your FAP publish) in NOTEPAD

TIP: By default, the settings will currently be:

```
IntegratedSecurityMode=1
<……>
#ServerCAMURI=http://servername:9300/p2pd/servlet/dispatch
#ClientCAMURI=http://servername/cognos8/cgi-bin/cognosisapi.dll
#ClientPingCAMPassport=900
#CAMPortalVariableFile=templates\ps\portal\variables_TM1.xml
```

- Modify the settings so that they are similar to:

```
IntegratedSecurityMode=2
servercamuri=http://servername:9300/p2pd/servlet/dispatch
clientcamuri=http://servername/cognos8/cgi-bin/cognosisapi.dll
ClientPingCAMPassport=900
CAMPortalVariableFile=templates\ps\portal\variables_TM1.xml
```

6.3 Set the TM1p.ini file to allow import from the CAM security

- Ensure that you are logged onto the TM1 server using the Windows user that runs the TM1 services
    - Typically this means logging on with the Controller COM+ Windows user (the Controller 'service' Windows account)
- Click "START – RUN"
- **%appdata%** <enter>
- Open subfolder "**Applix**" then "**TM1**"
- Open the file TM1p.ini inside NOTEPAD

TIP: By default, the settings will currently be:

```
AllowImportCAMClients = F
CognosGatewayURI =
```

- Modify the settings to have the following values:

```
AllowImportCAMClients = T
CognosGatewayURI = http://servername/cognos8/cgi-bin/cognosisapi.dll
```

6.4 Change FAP Service properties to allow import

- Open the FAPService.properties file in NOTEPAD

TIP: By default, this is located here:
`C:\Program Files\cognos\c8\server\FAP\FAPService.properties`

TIP: By default, the settings will currently be:

```
#clientcamuri=http://<camservername>/cognos8/cgi-bin/cognos.cgi
```

- Modify the settings to have the following values:

```
clientcamuri=http://servername:80/cognos8/cgi-bin/cognosisapi.dll
```

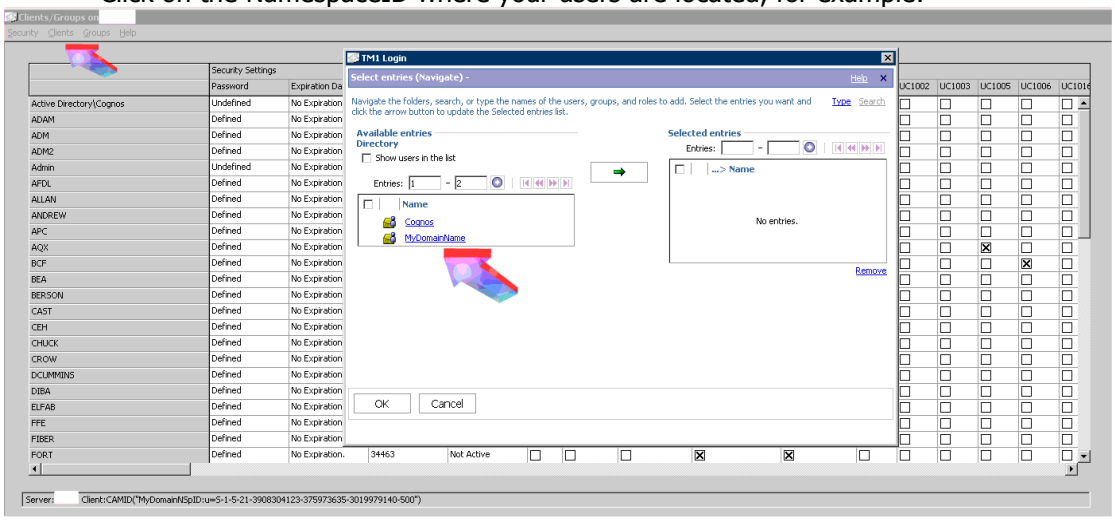
- Afterwards, stop and start TM1

6.5 Define a CAM user to Function as a TM1 Administrator

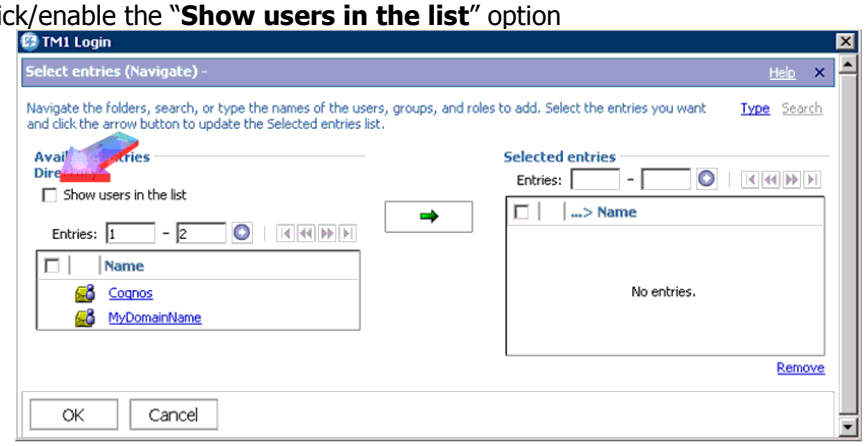
To successfully administer TM1 while using IBM Cognos 8 authentication, an existing Cognos user must be added to the TM1 ADMIN group. This Cognos user will be used to import Cognos groups into TM1.

- From the start menu, launch TM1 **Architect**
- Inside the "TM1 Architect: Server Explorer" Window, expand "**TM1**"
- Double-click on the TM1 server (for example **'TEST'**) that you have created earlier
- Logon using a TM1 database login (for example user **'Admin'**)
- **Right-click** on server (for example 'TEST') and choose "**Security - Clients/Groups**"
- Inside the new Window, click "**Clients - Add New Client**")

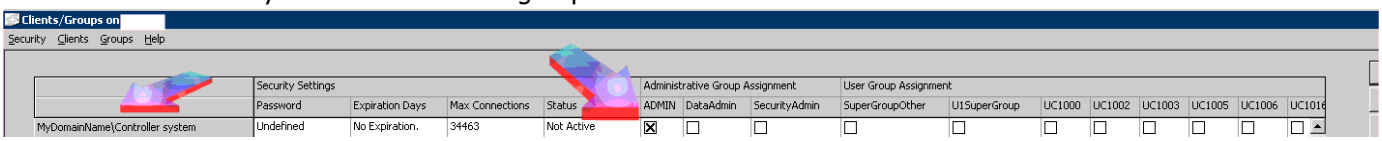
- Click on the NamespaceID where your users are located, for example:



- Tick/enable the "**Show users in the list**" option

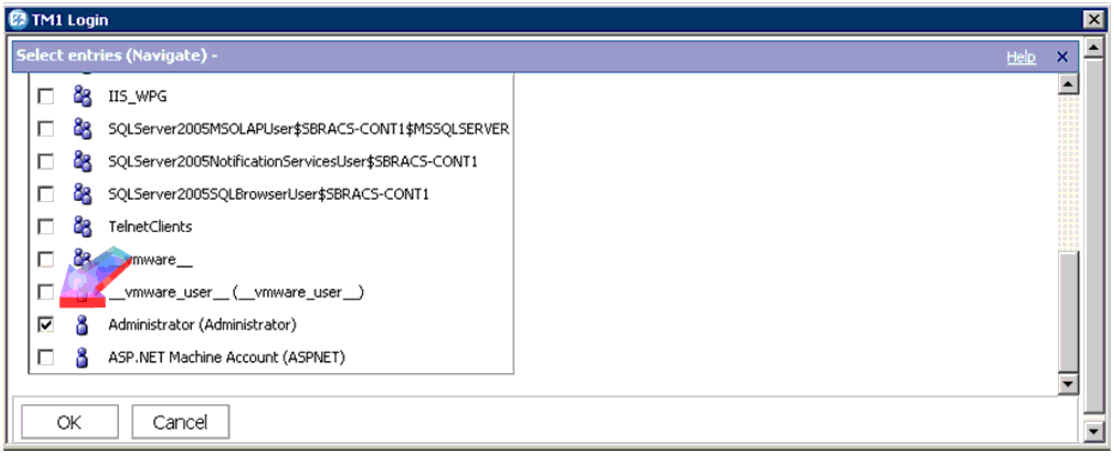


- Navigate to the directory containing the Cognos user (for example `Namespace\Controller_system`) that you want to define as a TM1 administrator.
- Select ("tick") the user.
- Click the green arrow button to move the selected user to the Selected Entries list.
- Click OK to import the Cognos user into TM1.
- Once you have added your user (for example "MyDomainName\Controller_system") you can tick the TM1 group "ADMIN" next to their name:

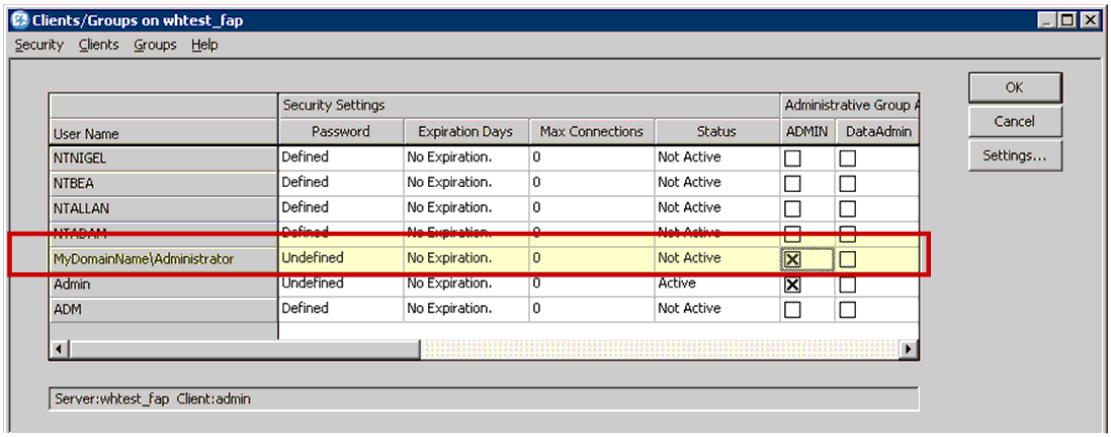


Further Example

TIP: Here is another example, where we have chosen the user "Administrator"…



…and here we have ticked the box 'ADMIN' for this user:



6.6 Import Cognos Groups into TM1

In the earlier section (6.4) we defined a Cognos user as a TM1 administrator. This Cognos user can now import Cognos groups into TM1. You should import only the Cognos groups that you want to allow to access the TM1 server.

1. In the Server Explorer, double-click your TM1 server. The **Cognos logon** dialog box appears.
2. Log on as the Cognos user that you have defined as a TM1 administrator.
3. From the Server Explorer, click **Server**, then **Security**, then **Clients/Groups**.
4. From the **Clients/Groups** window, click **Groups**, then **Add New Groups**. The **Select Entries** dialog box appears.
5. In the **Names** box, click the namespace to which you are currently connected.

Note:

- Only groups from the namespace to which you are connected can be imported into TM1.
- Other namespaces may appear in the **Name** box, but you cannot import groups from them.

6. Navigate through the directory structure and select the Cognos groups you want to import into TM1.
7. Click the green arrow button to move the selected user to the **Selected Entries** list.
8. Click **OK** to import the Cognos groups into TM1.

If you review the User Group Assignment section of the Clients/Groups window, you should see the Cognos groups added to your server.

6.7 Create users

TIP: When a TM1 server is configured to use *"IBM Cognos 8 authentication"*, you cannot create new clients directly on the TM1 server.

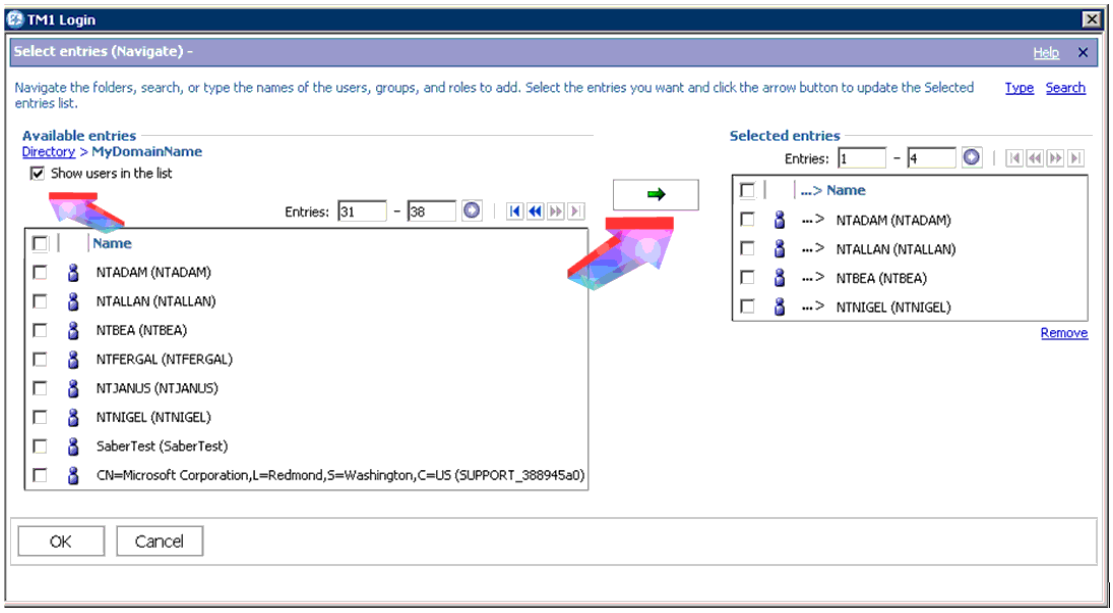
- *Instead, all client administration is performed in IBM Cognos 8.*

When a Cognos user accesses TM1, the user is validated and automatically assigned to the appropriate TM1 groups.

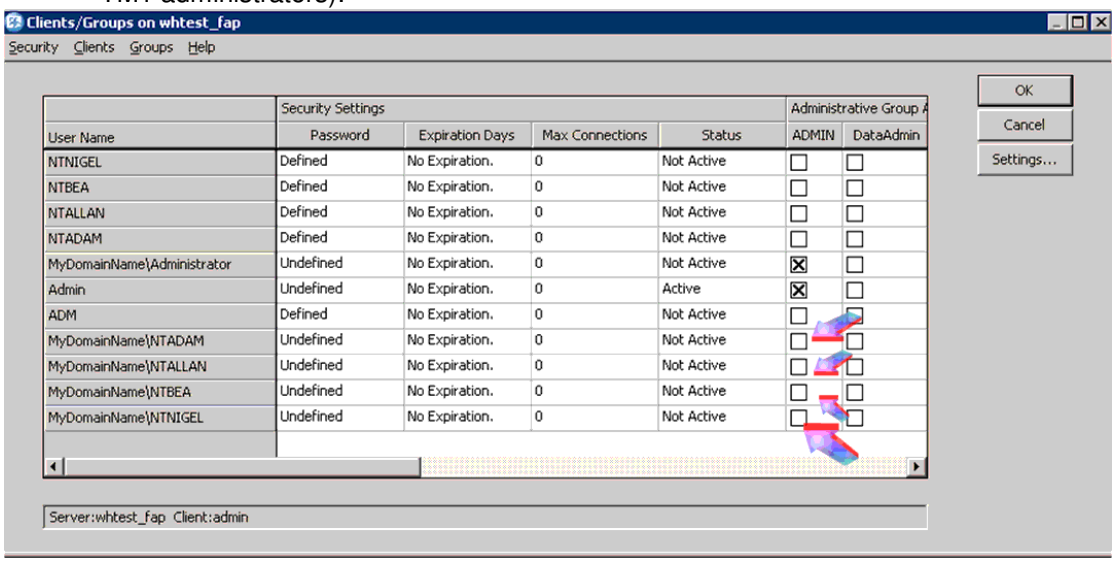
- There is no need to manually assign users to groups in TM1.

However, now that we are currently using "mixed authentication" then to add users to FAP/TM1 you simply repeat the steps in the earlier section (6.4 "Define a CAM user to Function as a TM1 Administrator"):

1. Select all the users that you want to add to the system:



2. However, this time do NOT tick the box "ADMIN" (because these users will not be TM1 administrators):



6.8 Final Miscellaneous TM1 server configuration settings

Change the TM1 authentication (to use CAM only) by opening the tm1s.cfg file in Notepad again, and modify the setting to be:

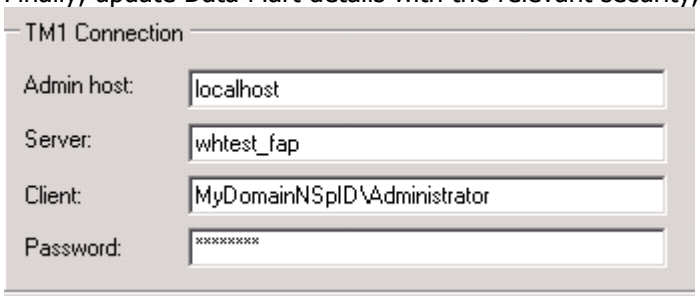
```
IntegratedSecurityMode=5
```

Remember:

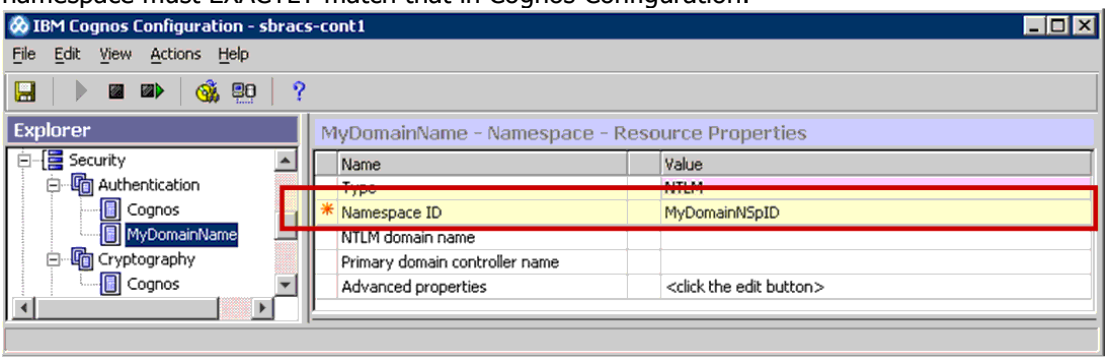
- If using TM1 9.5 (Controller 8.5.1) the value of **5** is correct.
  - In addition, if integrating Cognos Contributor with TM1, then this value should be **5**.
- However, if using older versions TM1 (9.4.1 – which came bundled with of Controller 8.5 RTM) then you need to use the value of **4**
  - However, be aware that there are some known issues/limitations to this version combination, so it is recommended to upgrade TM1 to 9.5 or higher instead.

Reboot the entire server (to be sure that all settings are 100% completely registered).

Finally, update Data Mart details with the relevant security, for example:

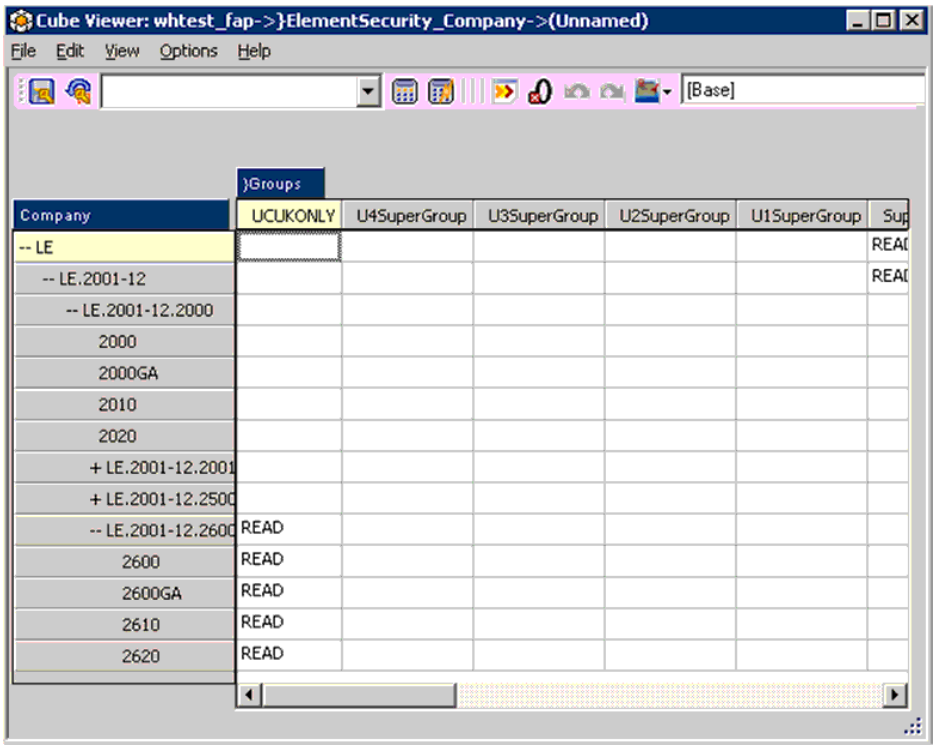


NOTE: The "Client" username **and** password are both CASE SENSITIVE! Therefore the namespace must EXACTLY match that in Cognos Configuration:

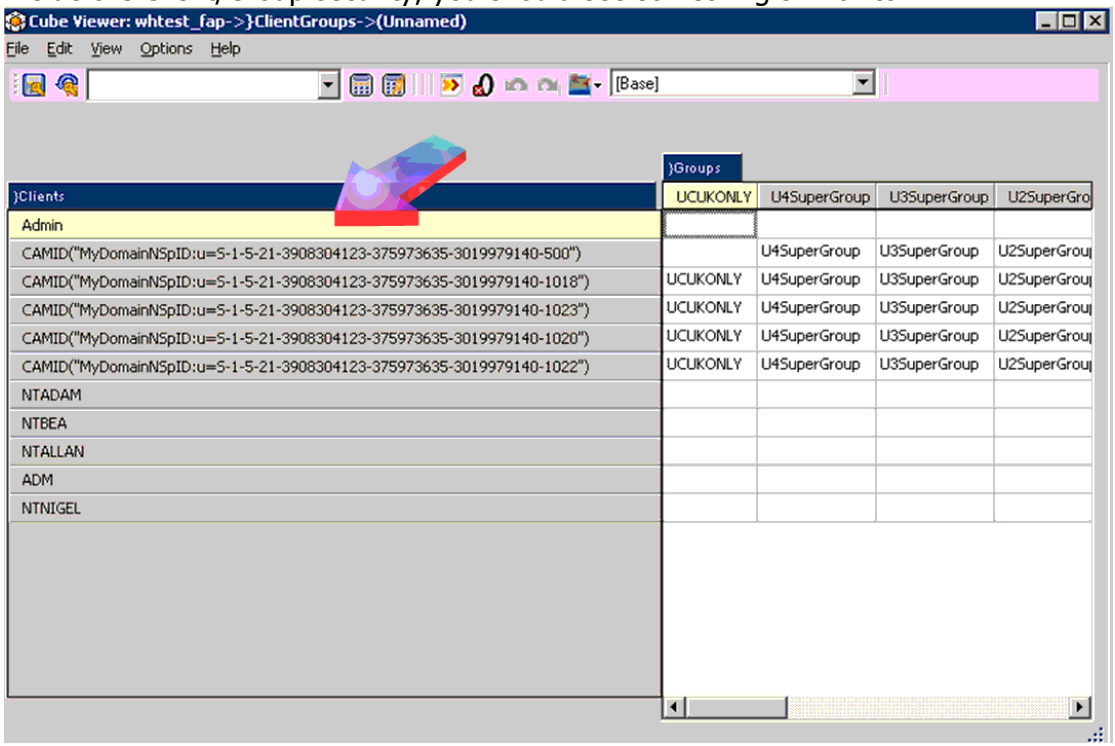


6.9 Testing

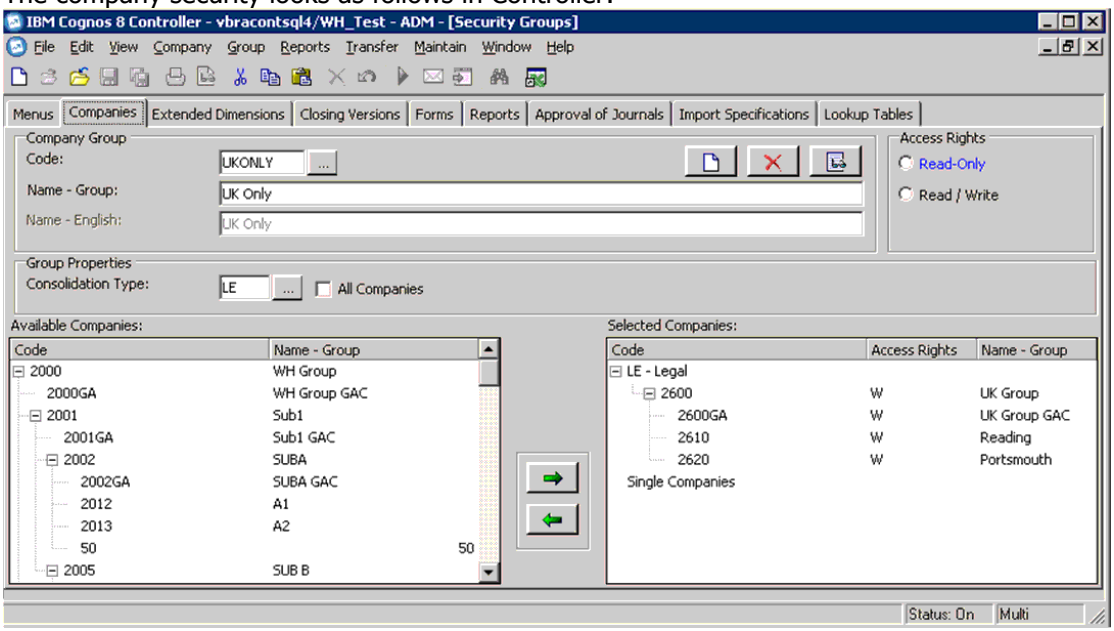
Republish the FAP data mart. Afterwards, check security in the TM1 cube. For example, looking at the Company element security in TM1 you should see something similar to:



Inside the Client/Group security, you should see something similar to:



The company security looks as follows in Controller:



…which matches those in TM1.

6.10 Administering TM1 Object Security

NOTE: While IBM Cognos 8 authentication automatically manages users on the TM1 server, the TM1 administrator must still manage object security to allow Cognos users to view and use TM1 objects.

6.11 Administrator Considerations When Using IBM Cognos 8 Authentication

TM1 administrators should be aware of the following issues when configuring a TM1 server to use IBM® Cognos® 8 authentication.

- Review the description of TM1 security modes 4 and 5 for the IntegratedSecurityMode parameter.
    - You should understand how these different modes control whether or not Cognos 8 users can belong to TM1 user groups.
    - For details, see the description of the IntegratedSecurityMode parameter in the IBM Cognos TM1 *Operations Guide*.
- You cannot use TM1 to permanently assign a Cognos 8 user to another Cognos 8 group.
    - Any user assignment you make in TM1 to a Cognos 8 group is not saved back to Cognos 8.
    - When a Cognos 8 user logs in to TM1, the group assignments in Cognos 8 override any Cognos 8 group assignments made in TM1.
- If you rename a Cognos 8 user after importing that user to TM1, you must then delete the user in TM1 in order to update TM1 with the new user name.