Proven Practice

Configuring Controller 8.2 to use Active Directory authentication

Product(s): Controller 8.2

Area of Interest: Infrastructure

Copyright

This document is maintained by the Best Practices, Product and Technology team. You can send comments, suggestions, and additions to BestPractices-ProductandTechnology@cognos.com.

Contents

1 Introduction

1.1 Purpose

This document is intended to demonstrate how best to configure Controller 8.2 to use Active Directory authentication (i.e. using Windows A.D. users/groups directly inside the Controller 8 application itself).

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

NOTE: This document supersedes my previous document ("`Configuring Controller 8 to use Active Directory authentication`" – dated 2006).

1.2 Disclaimer

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

There are an infinite variety of possible customer I.T. environments, many different ways to install/configure Controller 8.2, and therefore the advice in this document may have to be modified by the customer to fit in with their needs/environment. Your Cognos technical consultant (who installed your Controller server(s)) will be the best person to advise on any extra necessary changes.

NB: This guide is intended as a "quick-start" guide, for the most popular of environments. The official documentation takes precedence over this document.

1.3 Assumptions

This document is based on Controller 8.2 (released Summer 2007). However, it *may* be correct for future releases of Controller.

Generally we shall assume that it is a simple server environment (i.e. only one Controller 8.2 application server).

2 Overview

Cognos 8 Controller can use the following 3 different types of security logon authentication methods:

- Native
  - this is the default method, where the users/passwords are entirely stored inside the Controller database itself)
- Cognos 8
- Windows

To configure Controller 8 to use Cognos 8 (or Windows Authentication), you must perform 3 steps:

1) Configure Controller 8 to run with authenticated access
2) Add Controller users to the Cognos roles
3) Map Controller roles to the Cognos 8 users

Typically, the customer's:

- I.T. department would perform task (1)
- Finance 'Superuser'(s) would perform (2) and (3).

This document will demonstrate how to perform these 3 tasks.

3 Configure Authenticated Access

3.1 Disable Anonymous Access

On the Controller 8 application server:

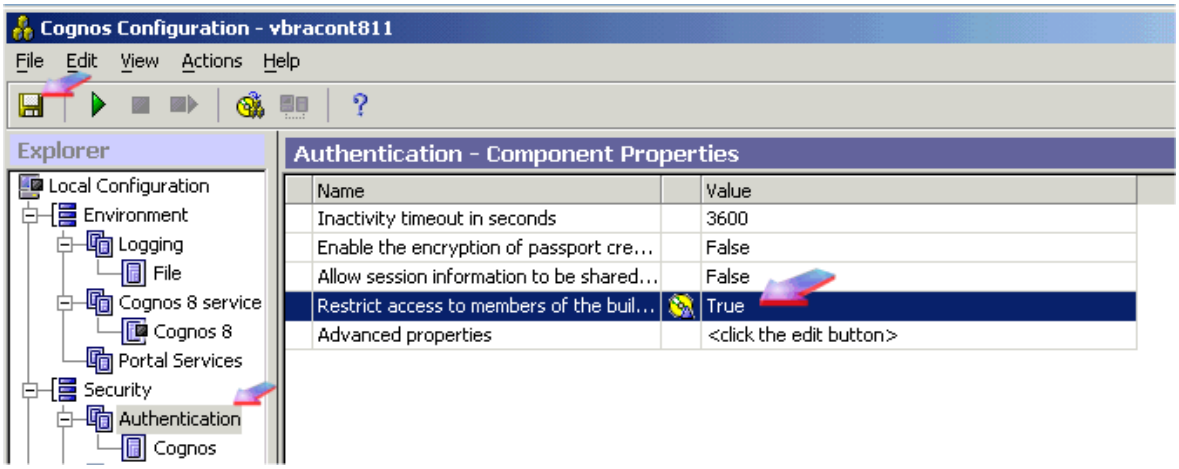
- Start **Cognos Configuration** from the Start Menu
- In the Explorer window, under Security, Authentication, click Cognos
- Change Allow anonymous access (from True) to False
- Click **File** - **Save**.

Now, you will notice that users are required to provide logon credentials when they access Cognos resources.

3.2 Restrict User Access to the Cognos Namespace

On the Controller 8 application server:

- Inside Cognos Configuration, under Security, click Authentication
- change the value of Restrict access to members of the built-in namespace to True
- File - Save



3.3 Configure Controller 8 Components to Use Active Directory Server - PART ONE: Configure an Active Directory Namespace

TIP: *For Cognos 8 Controller to work properly with Active Directory Server, ensure that the Windows user group 'Authenticated users' has 'Read' privileges for the Active Directory folder where users are stored. The customer's I.T department's Active Directory administrator can help you with this.*

On the application server:

- launch **Cognos Configuration**
- under Security, right-click Authentication, and then click New resource, Namespace

TIP: *Do not delete the Cognos namespace. It contains authentication data that pertains to all users and is required to save the configuration. If you were ever to delete this new*

namespace (using Cognos Configuration), you must complete the process by ALSO deleting it in the "Cognos Connection" portal. For more info, see Appendix #4
Important:

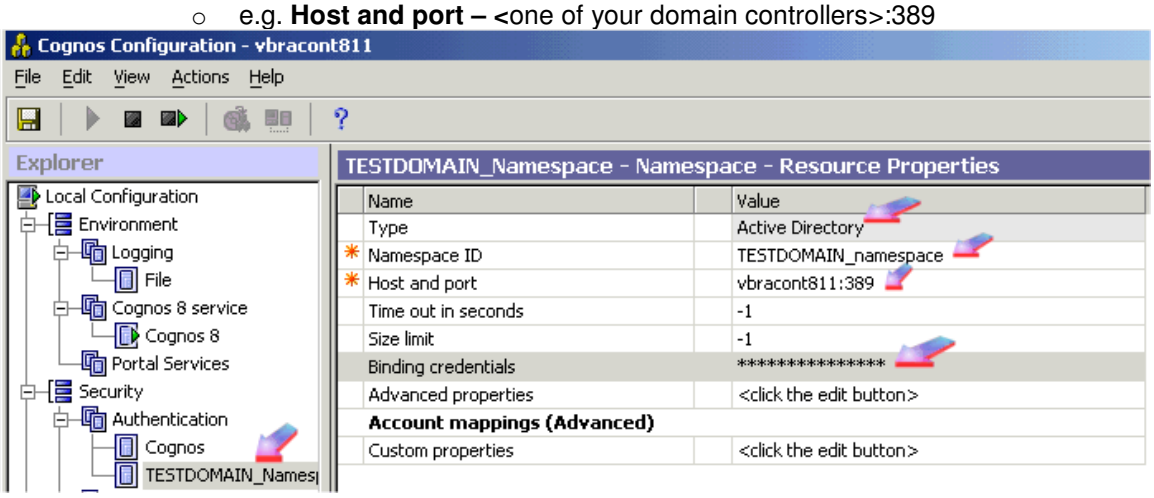
- In the **Name** box, type a name for your authentication namespace (e.g. "<DOMAIN>", and ensure the "**Type**" is set to "**Active Directory**"

NOTE: In my examples/printscreens, I've called the namespaces "`<DOMAIN>_namespace`". This is just for visibility. You probably would prefer to just call it "`<DOMAIN>`".

- **Namespace ID** property: specify a unique identifier e.g. "`TESTDOMAIN`"

TIP: I have used '`TESTDOMAIN_namespace`' in the print-screens in this document

- 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 <u>most</u> environments, there is **no need** to fill in the section 'Binding credentials' (because most Windows domains allow anonymous LDAP querying).*

- *TIP: If you specify Binding Credentials (i.e. if you fill in this section), then (in some environments) it can lead to performance problems*
- *This is because it causes Cognos to 'unbind' its original user and re-bind as the 'specified' user*
- *This can lead to a delay if the domain controller is not on the same LAN (for example, one customer's logon was delayed from 2 seconds to 5 seconds by using binding credentials).*

*Therefore, only fill in the 'Binding credentials' section if your "test" (see later) fails. If authentication fails, specify a Windows user ID and password for the **Binding credentials** property.*

- *Use the credentials of a Windows user who has at least 'search' and 'read' privileges for that server.*
- *This should be a domain user who can 'see' the folders inside the AD where the Controller users are located. This will probably be the Controller service account (e.g. `DOMAIN\Controller_admin`)*

- Click **File** – **Save**
- Test the connection, by right-clicking the new authentication resource and click **Test**.
- **Restart** the Cognos 8 service

3.4 OPTIONAL – ADVANCED CONFIGURATION: Include or Exclude Domains Using Advanced Properties

For more information, see Appendix #3 at end of this document

3.5 Decide which IIS authentication method to use

The Cognos 'provider' can use 2 different methods (of integrating with the IIS web server) to provide single signon:

- Kerberos delegation
  - This is the default method
- "Remote_User"

Why would you wish to use "Remote_User" variable?

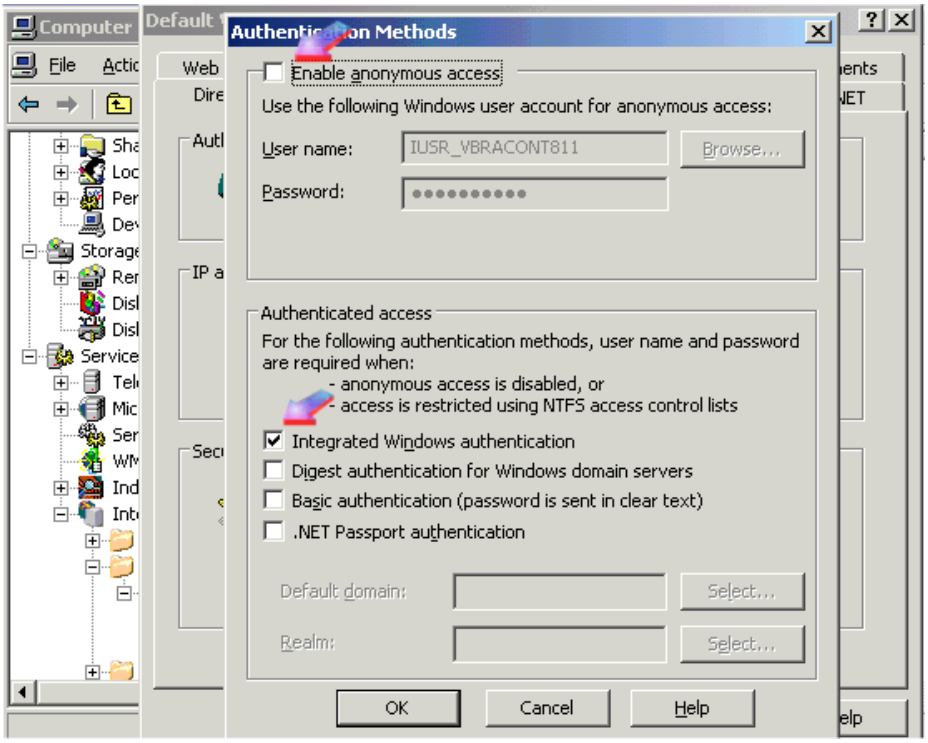
For example, (see document "Cognos 8 Controller Readme Updates (English)" - `rdm_ctrl_updates.pdf`) **if you have an NT4 domain**, you need to use an "LDAP" *not* Active Directory namespace.

To quote this document: *"This problem occurs because the Cognos 8 Active Directory provider uses ADSI protocol and Kerberos delegation for authentication in a single signon environment. When Microsoft Internet Explorer runs on Windows NT, it cannot authenticate to the IIS server using Kerberos delegation. When your system is configured for Windows Integrated Authentication, for the single signon to work with IIS, you must (a) configure Cognos 8 to communicate with the Active Directory server using the LDAP provider. (b) configure the external identity mapping property to read the REMOTE_USER environment variable.*

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

TIP**:** *"Integrated Windows Authentication" was formerly named "NT Challenge Response".*

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



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

TIP: By doing this, we are enabling "Windows Authentication" via the configuration of Internet Information Services (IIS). This will mean that (from now on), after users log on to client computers with their Windows username and password, they are not prompted with further logons when they run Cognos Controller or the Cognos Controller Excel Add-in.

3.7 Configure Controller 8 Components to Use Active Directory Server - PART TWO: Enabling Single Signon Between Active Directory Server and Cognos 8 Controller Components

OPTION1: Steps for Single Signon *Using Kerberos Delegation*

After enabling 'Windows Integrated Authentication', skip to the next step.

OPTION2: Steps for Single Signon *Using "`Remote_User`" variable*

After enabling 'Windows Integrated Authentication', perform the following ***(in addition)*** on every computer where you installed Content Manager:

- Launch Cognos Configuration
- In the Explorer window, under Security, Authentication, click the Active Directory namespace
- Click in the **Value** column for **Advanced properties** and then click the **edit** button
- In the **Value - Advanced** properties window, click **Add**
- In the Name column, type `singleSignonOption`
- In the Value column, type `IdentityMapping`
- Click **OK.**

=> The Active Directory provider now uses REMOTE_USER for single signon

Tip: *To switch back to Kerberos delegation, edit Advanced properties and, in the Value column, type* ***`KerberosAuthentication`***

4 Add Cognos Controller Users to the Cognos Controller Roles

4.1 Using the Cognos Connection portal

Inside this section, we shall use the portal to:

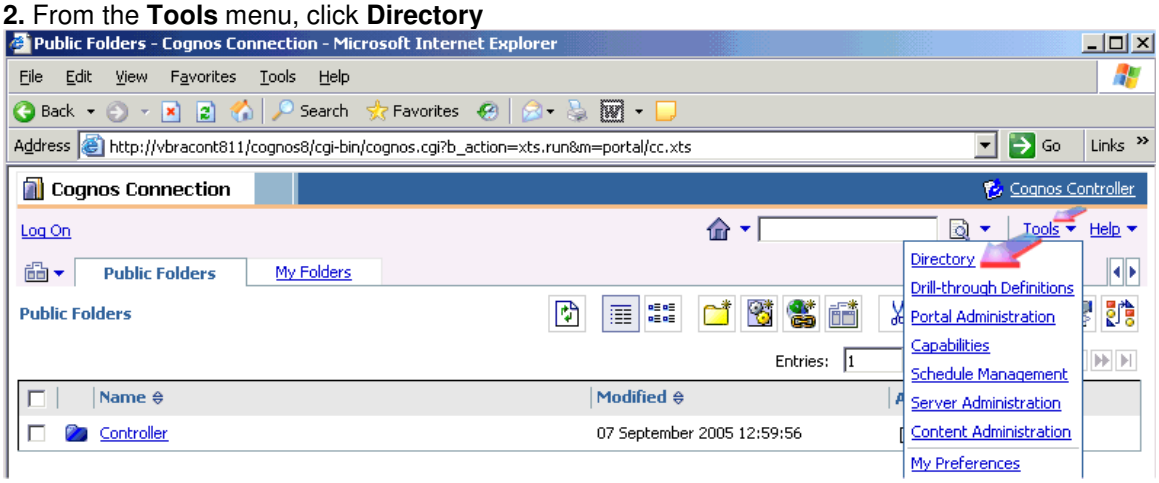
- remove the 'Everyone' group from the Cognos built-in roles and groups
- ensure that authorized users belong to at least one Cognos built-in role or group:

Steps

1. Open Cognos Connection

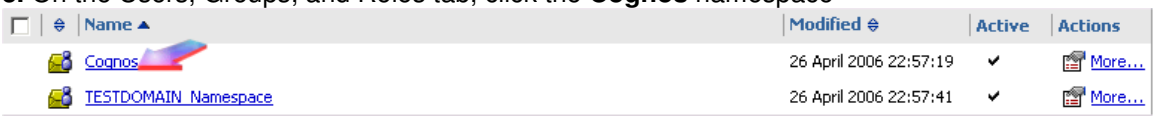
`e.g. http://<application_server_name>/cognos8`

2. From the **Tools** menu, click **Directory**

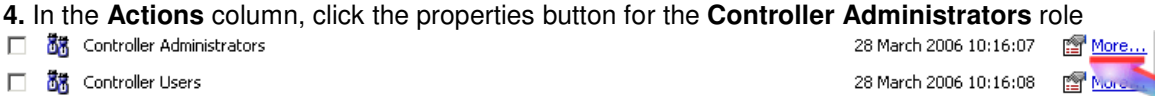


TIP: In my example here, my domain's NETBIOS name is "TESTDOMAIN".

3. On the Users, Groups, and Roles tab, click the **Cognos** namespace



4. In the **Actions** column, click the properties button for the **Controller Administrators** role



5. Click the **Members** tab.

6. To add members, click **Add** and choose how to select members:

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

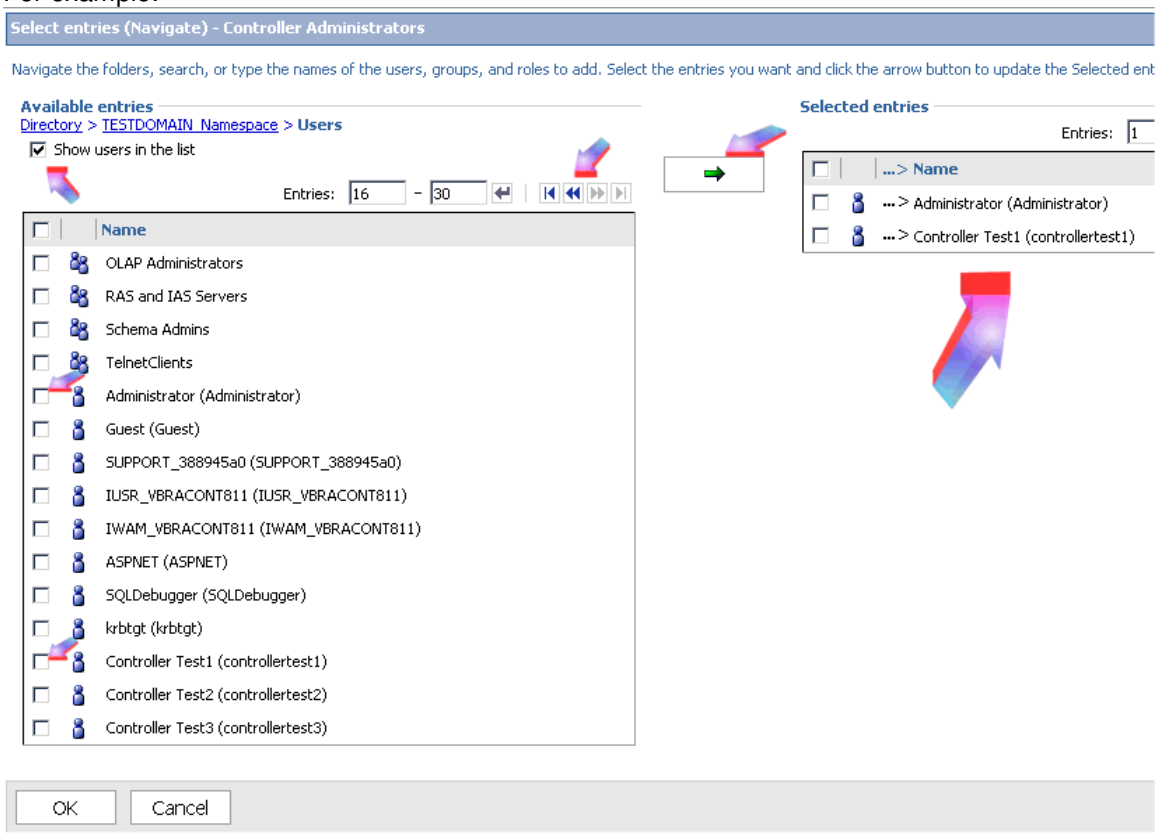
Method#3 – Manually type in entries:
Manually type the name of entries you want to add: click **Type** and type the names of groups,roles, or users using the following format, where a semicolon (;) separates each entry:

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

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

7. Click the right-arrow button and when the entries you want appear in the **Selected entries** box, click **OK**.

For example:

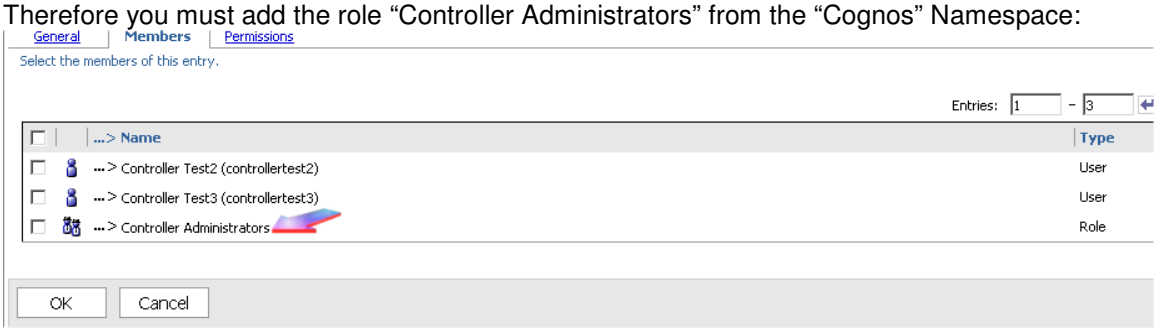


8. TIP: For Security purposes, on the **Members** tab, if there is an "**Everyone** namespace", click it, and then click **Remove**.

9. Click **OK**.

10. Repeat steps 4 to 8 for the **Controller Users** role, and click **OK**

Tip: The **Controller Administrators** role must be a member of the **Controller Users** role. Therefore you must add the role “Controller Administrators” from the “Cognos” Namespace:

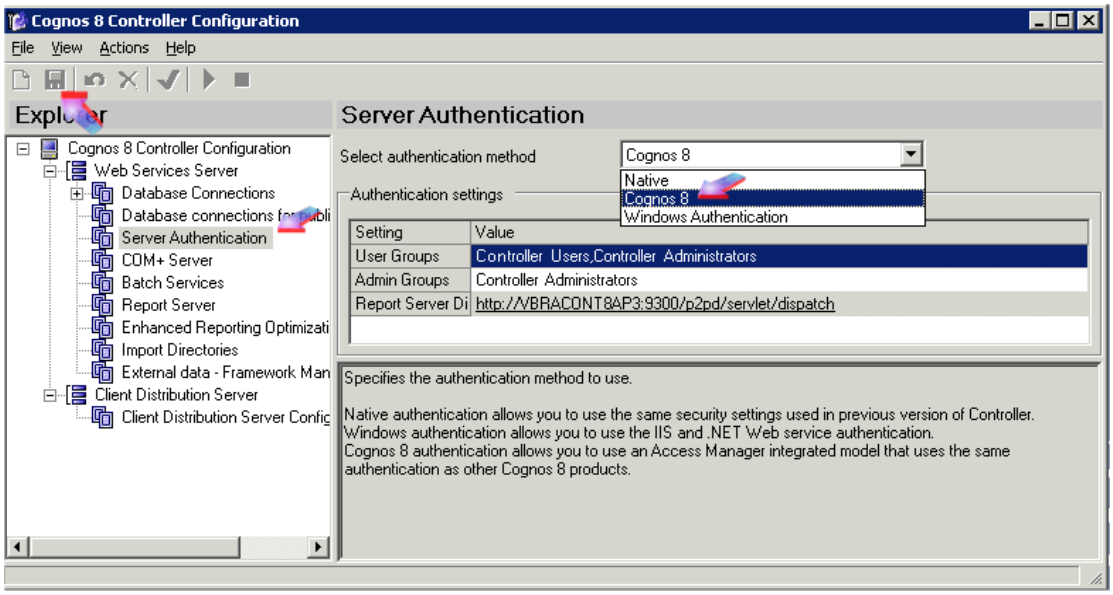


5 Map Cognos Controller Users to Cognos 8 Users

5.1 Configure Controller to use Cognos 8 Authentication

On the Controller application server:

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



- Click ‘save’

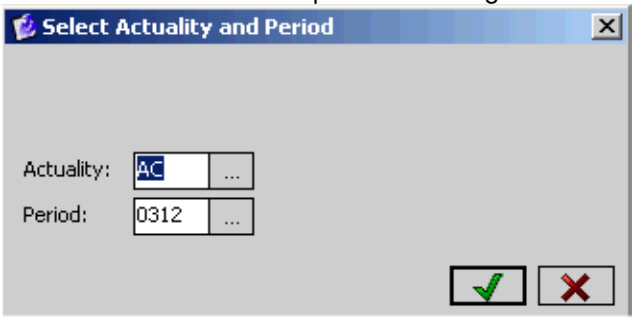
5.2 Create an association between the users defined in the Controller application, and those defined in the Cognos 8 namespace roles

After you add Cognos Controller users to the Cognos Controller roles, you must create an association between the users defined in the Cognos Controller application and those defined in the Cognos 8 namespace roles.

Important: *Associations can only be created by a user who has been configured as a member of the Controller Administrators role in Cognos Connection*

- Logon to Windows using a username that is a member of the ‘Controller Administrators’ role in Cognos Connection
- Launch Cognos Controller

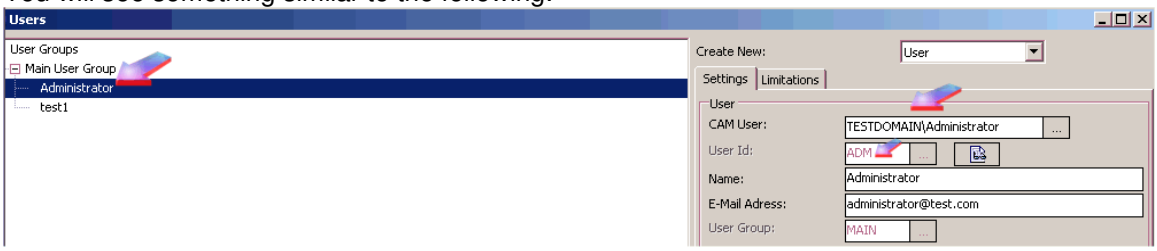
Notice how you are **not** asked for a username/password to logon with:



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 (e.g. in this case TESTDOMAIN\ADMINISTRATOR).

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

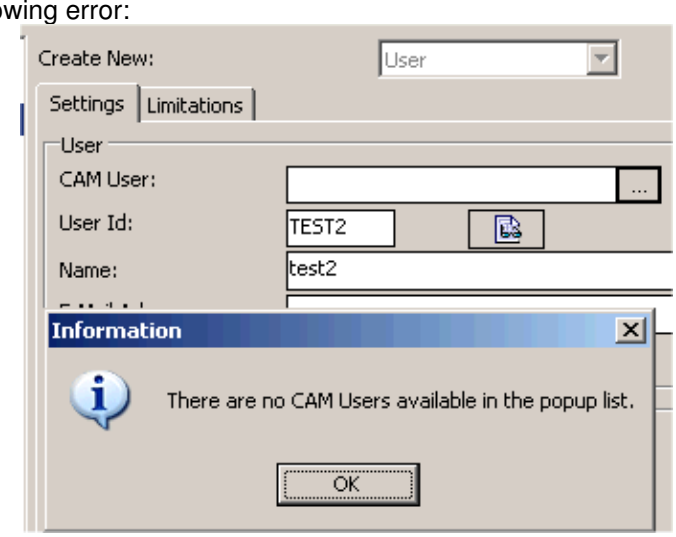
You will see something similar to the following:



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

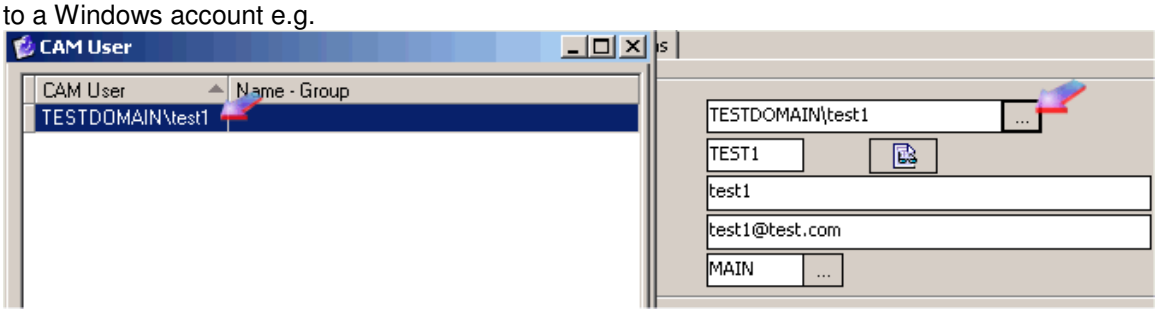
3. In the **Create New** box, click the drop-down arrow and then click **User**.
4. Beside the first **User Id** box, click the browse button, and then select the user as defined in the Cognos 8 namespace roles.

If you get the following error:



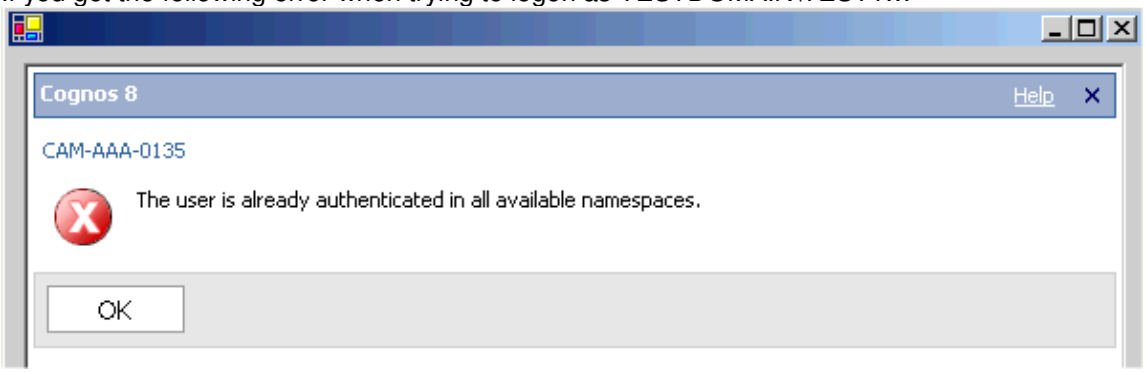
…then it is likely that you need to reconfigure your groups/members inside Cognos Connection. In other words, you need to add users into the groups "Controller Users" and "Controller Administrators".

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.

If you get the following error when trying to logon as TESTDOMAIN\TEST1…



…then perhaps you've not given that user any rights to logon inside the application!

6 Appendices

6.1 Appendix 1 - How to swap between Native and Windows security

During the Controller 'development' phase, you may wish to change from Windows to Native:

- Ensure no users on system
- Launch "*Controller Configuration*"
- Click on "Web Services Server" – "Server Authentication"
- Change "**authentication method**" from "Windows authentication" to "**Native**"

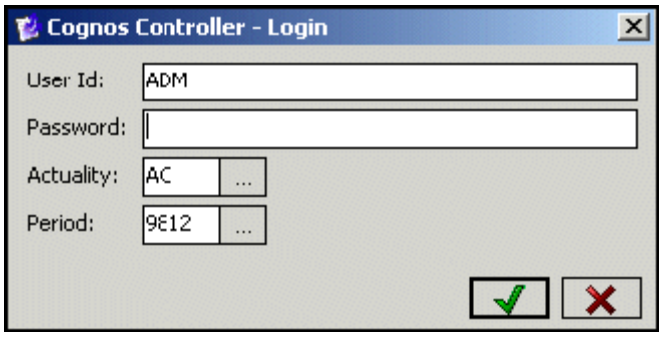
- Launch "*Cognos Configuration*"
- Change Security – Authentication – Cognos – "**Allow Anonymous Access**" from "False" to **True**"
- File – Save
- Restart Cognos 8 Service (using button at top of screen)

How to change from Native to Windows:

Perform reverse of above

6.2 Appendix 2 – Native Authentication configuration

Native authentication is the default authentication method. Login information is configured in the Cognos Controller databases and in the Cognos Controller user interface. Native authentication is the authentication method used in previous versions of Cognos Controller. If Native authentication is enabled, when users log on to Cognos Controller from Cognos Connection or from a URL and have selected a database to log on to, they are prompted to log in.
Users are prompted with the same login window when they log on to Cognos Controller using the Cognos Controller Microsoft Excel Add-in.



If you want to use Native authentication in your Cognos 8 Controller environment, the reporting components must run under anonymous access. When the reporting components run under anonymous access, no login is required. In Cognos Connection, anonymous access is enabled by default. Native authentication provides minimal security in your Cognos 8 Controller environment.

6.3 Appendix 3 – Native Authentication configuration

OPTIONAL – ADVANCED CONFIGURATION: Include or Exclude Domains Using Advanced Properties

When you configure an authentication namespace for Cognos 8 Controller, users from only one domain can log in. By using the Advanced properties for Active Directory Server, users from related (parent-child) domains and unrelated domain trees within the same forest can also log in.

Authentication in One Domain Tree

If you set a parameter named chase_referrals to true, users in the original authenticated domain
and all child domains of the domain tree can log in to Cognos 8 Controller. Users above the
original authenticated domain or in a different domain tree cannot log in.

Authentication in All Domain Trees in the Forest

If you set a parameter named multi_domain_tree to true, users in all domain trees in the forest can
log in to Cognos 8 Controller.

Steps

1. On every computer where you installed Content Manager, open Cognos Configuration.
2. In the **Explorer** window, under **Security**, **Authentication**, click the Active Directory namespace.
3. In the **Properties** window, specify the **Host and port** property:
• For users in one domain, specify the host and port of a domain controller for the single domain.
• For users in one domain tree, specify the host and port of the top-level controller for the domain tree.
• For users in all domain trees in the forest, specify the host and port of any domain controller in the forest.
4. Click in the Value column for **Advanced properties** and click the edit button.
5. In the **Value - Advanced properties** window, click **Add**.
6. Specify two new properties, **chaseReferrals** and **MultiDomainTrees**, with the following values:

Authentication for	chaseReferrals	MultiDomainTrees
One domain	False	False
One domain tree	True	False
All domain trees in the forest	True	True

7. Click **OK**.
8. From the **File** menu, click **Save**.

6.4 Appendix 4 – Delete an Authentication Provider

If they are no longer required, you can delete namespaces that you added or unconfigured namespaces that Cognos 8 Controller components detected after an upgrade.

Important: You must not delete the Cognos namespace. It contains authentication data that pertains to all users and is required to save the configuration. When you delete a namespace, you can no longer log on to the namespace. Security data for the namespace remains in Content Manager until you permanently delete it in the portal. For more information, see the *Administration and Security Guide*.

After you delete a namespace, it appears as Inactive in the portal.

Steps

1. On a computer where you installed Content Manager, open Cognos Configuration.
2. In the **Explorer** window, under **Security**, **Authentication**, right-click the namespace and click
Delete.
3. Click **Yes** to confirm.
The namespace disappears from the **Explorer** window and you can no longer log on to the namespace on that computer.
4. From the **File** menu, click **Save**.
5. Repeat steps 1 to 4 for each computer where you installed Content Manager.
You must now log on to the portal and permanently delete the data for the namespace. For more information, see the *Administration and Security Guide*.