



Spotlight on Security in Cognos 8.3 and Transformer 8.3

Background

With the introduction of ReportNet and Cognos 8 in the 2004/2005 timeframe, Cognos began pursuing an open systems approach related to namespace support. The basic concept behind this approach is that: authentication would come from the 3rd party namespace and that specific grant to content and data could be maintained via a number of namespace options. While these changes have been favorable to clients from an infrastructure perspective, they have raised other administrative complexities that are worthy of discussion. With the introduction of Cognos 8.3, Cognos has made another strategic improvement to the BI platform – adding an open security model to its multi-dimensional tool. A key improvement Transformer 8.3 is its ability to integrate with 3rd party namespaces.

How the security model works

Authentication

In the Cognos 8 world user authentication always happens via the clients' underlying namespace (e.g., Active Directory, Netgrity, etc). Using the underlying namespace for authentication is key because users are authenticated to the network at sign-on and are granted access to key network resources like file shares and printers based upon their network logon.

Organizations also have excellent controls in place on a local basis to facilitate human resources changes that impact user adds, changes, and expirations.

Access to BI Content and Data

Granting access to BI content and data is another key aspect of the Cognos security model. The underlying concept here is that by creating groups for content and data that users can have a true role appropriate view of information.

In all data security models, groups must be created and maintained within a namespace. With the introduction of Cognos 8 clients have greater choices as to which namespace they want to use to store groups and their associated memberships. This is a key factor related to deployment. Should groups be written to the authenticating namespace? to the Cognos namespace? Or the Access Manager namespace?

Working with the security model

Most organizations have well defined processes regarding their namespaces which are used for network authentication and the provision of network resources. Single sign-on pass through to Cognos is also a reality in many organizations.

However, clients have options regarding which namespace to use for business intelligence security. Most times, the network administrators are not interested in using the authenticating namespace to house the groups and memberships related to business intelligence content and data security.

The remainder of this section describes the options available to clients for maintaining groups for business intelligence content and data security.

<u>Use Authenticating Namespace</u>	Cognos 8 Platform <u>Cognos Namespace</u>	Series 7 <u>SUN One (Access Manager)</u>
Pros <ul style="list-style-type: none">Client only has to support one namespace.	Pros <ul style="list-style-type: none">Provides fine grained access controls for Cognos Connection and Cognos 8 BI.Tightly coupled into the Cognos 8 platform.	Pros <ul style="list-style-type: none">Provides fine grained access controls for Cognos Connection, Cognos 8 BI, and Series 7.Ingrained in any account that has been using Series 7.
Cons <ul style="list-style-type: none">Most network administrators do not want the BI related security groups being proliferated in the authentication namespace.	Cons <ul style="list-style-type: none">Little out-of-the-box automation exists to update the Cognos 8 namespace. SDK is required.Network administrators do not want to support additional namespaces.	Cons <ul style="list-style-type: none">Considered a legacy namespace now that the Cognos 8 namespace is available.Network administrators do not want to support additional namespaces.

Clients who started with Cognos 8 (i.e., no Series 7) typically use a mix of their authenticating namespace and the Cognos namespace to support their BI initiatives. Clients using Series 7 have typically continued to maintain content and data security groups in Access Manager. The Series 7 client base has generally been waiting until the release of Transformer 8 to move to another target namespace.

Transformer 8 and Security

Transformer 8 opens multi-dimensional OLAP up to 3rd party namespaces and the Cognos namespace. In Series 7, Transformer worked with Access Manager only. This change provides clients with much greater flexibility regarding namespace targets for data oriented access control groups that are used within Transformer when setting up custom views. The choice that clients now have relates to which namespace they want to use to write groups related to data security.

Security Transfer from Transformer 7 to Transformer 8

FirstQuarter has tested very large models in being upgraded to Transformer 8 and has found that security transfers seamlessly from a fully secured Transformer 7 model to Transformer 8. For clients seeking to upgrade their models and carry forward security, this should not be an issue.

Manually Assigning Security in Transformer 8

Security assignment in Transformer 8 uses a similar approach as in Transformer 7.x with a minor twist. The Transformer 8 process requires four steps.

1. Create a custom view and give the custom view a name
2. Link the custom view to one or more groups from the namespace.
3. For each custom view, indicate which data, dimensions, and measures are included/excluded. These determine the true view of the data, dimensions, and measures are visible to the user.
4. Connect the custom view to indicate the cubes may be accessed when the custom view is referenced.

Note: The minor twist between Transformer 7 and Transformer 8 is that in the earlier version steps 1 and 2 were a single step because the user class name *was* the custom view name. Transformer 8 gives greater flexibility when assigning one or more groups to a particular custom view.

This step-by-step is fairly straightforward; however, decomposing the above steps sheds greater light on the process. When implementing security en masse, the following items must be considered.

- **Custom view naming:** A methodology should exist for naming custom views.
- **Creation of groups in the namespace:** Groups must exist in the namespace (occurs in Step 2) or must be created. A methodology should exist for naming groups.
- **Memberships:** Users must be linked to groups in the namespace (occurs in Step 2) in order to provide access to the data.

When implementing security in Transformer 8, securing data en masse continues to be an issue for large corporate or governmental clients.

Security Automation in Transformer 8

With Transformer 8, security automation is available via MDL scripting. In Transformer 7, security automation was available through both MDL scripting and OLE Automation interfaces.

Securing Cognos with FirstQuarter's ProTools

Business intelligence is all about sharing information, but often enterprises can only deploy after the security hurdle is cleared. FirstQuarter's security console for Cognos, "ProTools" helps you broadly secure and scale the deployment of your business intelligence applications. With ProTools you can simplify, centralize, and scale your Cognos deployments.

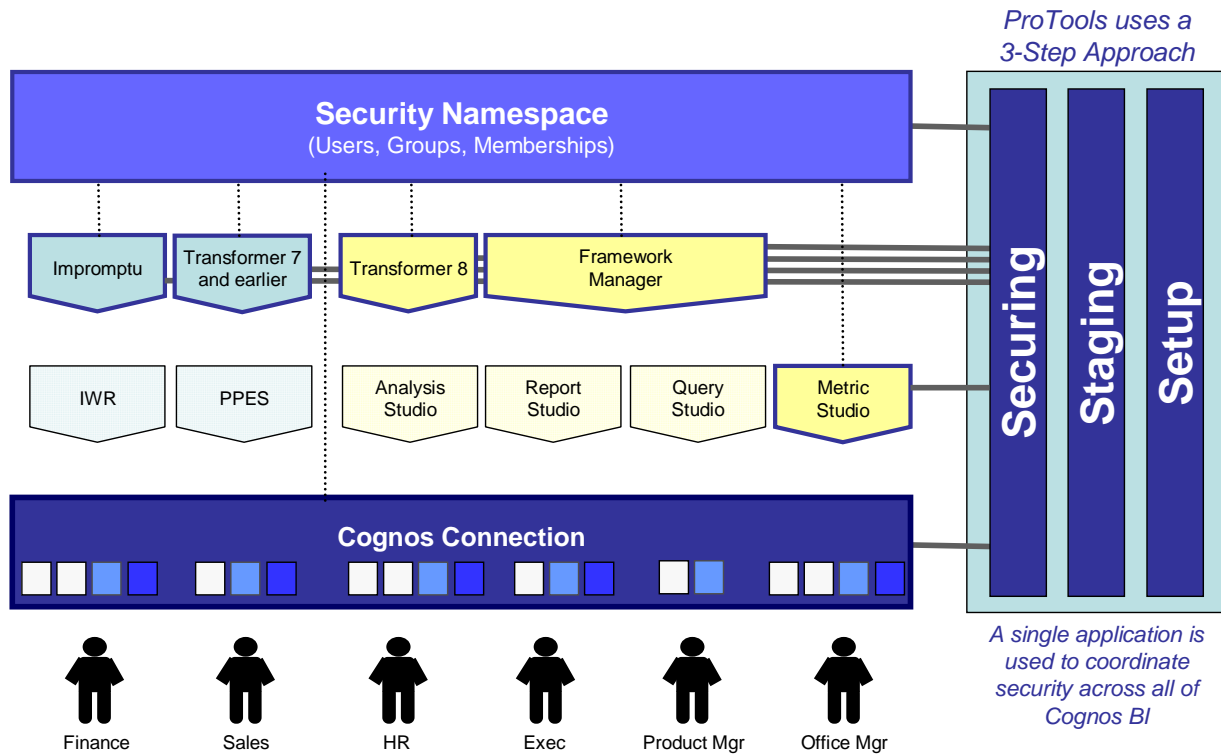
- Broadly deploy role appropriate access to data
- Implement complex security designs in less than a day.
- Cut security maintenance tasks by 90%
- Simplify, centralize, and streamline security administration
- Provide security reporting for data security audit purposes

ProTools helps you scale your deployments and clear complex security hurdles.

ProTools is a Powered by Cognos application that applies security across all of Cognos BI.

ProTools Security Console for Cognos BI

ProTools is a unified security console for securing Cognos Business Intelligence



The solution allows organizations to secure Cognos en masse and clear the final hurdle to deployment.

Implementing security is a cascading challenge

Implementing the vision of true role appropriate views to data is a difficult challenge because...

- even small security deployments can require thousands of steps to implement manually
- security must be implemented 100% correctly 100% of the time
- security is time consuming to implement
- security is tied to ongoing license controls
- security is forever changing
- security audits require that organizations maintain historical details about granted access

For more information...

FirstQuarter, Inc.
1060 First Avenue
Suite 400
King of Prussia, PA 19406

Contact sales@firstquarter.net
or call 610.768.8048