HIPAA Concerns: Implementing Tight Data Security

Chris Sherwin
Dunn Solutions Group

Business Objects
INSIGHT
AMERICAS 2006
DunnSolutionsGroup

Breakout Information (Hidden Slide)

- **HIPAA Concerns: Implementing Tight Data Security**
  - HIPAA regulations mandate that only authorized users can view medical data. This session focuses on how to implement data security for your data warehouse such that data security is seamlessly integrated into your ad hoc reporting environment. A well-implemented data security model addresses three goals: (1) security is enforced for ad hoc reporting, as well as shared corporate and private documents, (2) security has a minimal impact on query performance, and (3) the security model is easy to maintain as your user requirements change. Learn how to plan for data security when designing your data model, your universe, and enterprise security in order to achieve these three goals.

Implementing Tight Data Security

HIPAA concerns

- **Health Insurance Portability and Accountability Act of 1996**
  - HIPAA for short is a Federal Regulation impacting the distributing and sharing of individually identifiable health information (called PHI)
  - Only those with explicitly granted access are allowed to view PHI
  - Data that is not 'individually identifiable' can be more readily viewed and distributed
- **Getting the right access to the right people**
  - Giving users access to all the information they need to be best able to do their own jobs
  - Ensuring no-one has access to any PHI they are not authorized to view
- **Not Just a HIPAA problem**
  - Similar data security issues exist in any industry

Topics

- **Goals and Overview**
- **Object-Level Security**
- **Row-Level Security**
- **Data-Value (Masking) Security**
- **Summary**
- **Q&A**

Goals and Overview

Goals – what are we trying to achieve?

- **Integrated into the environment**
  - Data security enforced for adhoc reports
  - Data security enforced for shared documents
  - Data security minimizes chances of an accidental breach
- **Minimal Performance Impact**
  - Query performance similar to unsecured performance
- **Ease of Maintenance**
  - Expandable/adaptable security model
  - How hard is it to add one more User? Object? Universe?

Goals and Overview

Overview – what are we talking about?

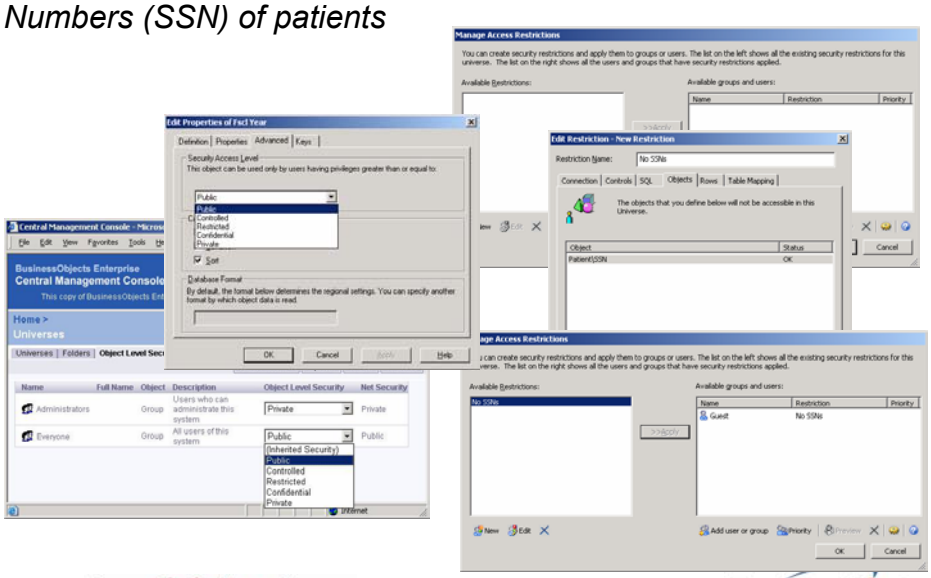
- **What are we covering?**
  - Object-level security
  - Row-level security
  - Data-value (masking) security
- **What are we not covering?**
  - Report/category/universe security model
  - Keeping users from sharing secure data

Topics

- Goals & Overview
- Object-Level Security
- Row-Level Security
- Data-Value (Masking) Security
- Summary
- Q&A

Object-Level Security

Scenario – only some users can view the Social Security Numbers (SSN) of patients



Object-Level Security

What is it?

- **Prevents users from being able to use objects**
  - By preventing access to the object, access to the data is denied
  - Two models exist
- **Security access levels**
  - Objects assigned security access level
  - Users/groups assigned security access for each universe
  - Users can only see objects for their security access and above
- **Security restricting objects**
  - Assign lists of restricted objects to each user/group

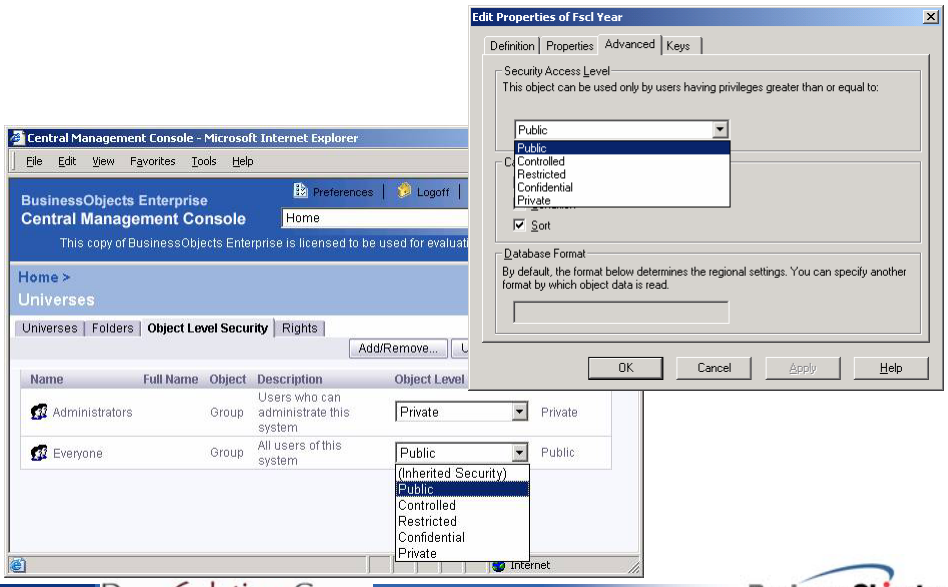
Object-Level Security

Security access levels

- **Security access level for objects**
  - Assigned access level to each objects
  - Public (least restrictive) → Private (most restrictive)
- **Security access level for users/groups**
  - Users/groups assigned security access for each universe
  - Public (least access) → Private (most access)
- **Prevents users from being able to use objects**
  - Users can only see objects for their security access and above
  - Single spectrum of restrictions per universe

Object-Level Security

Setting security access level for an object and then for a group



DunnSolutionsGroup
Business Objects

Object-Level Security

Security access levels - meeting our goals

- **Integrated into the environment**
  - ☺ Automatically part of adhoc reports
  - ☹ Security is ignored for distributed reports
- **Minimal performance impact**
  - ☺ Zero runtime performance hit
- **Ease of maintenance**
  - ☺ Simple model minimizes chances of complexity creep
  - ☹ Difficult/impossible to give a user access to one object without others
  - ☺ Adding a new user or universe object fairly easy
  - ☹ Is all or nothing – user can see all values in field or none

DunnSolutionsGroup
Business Objects

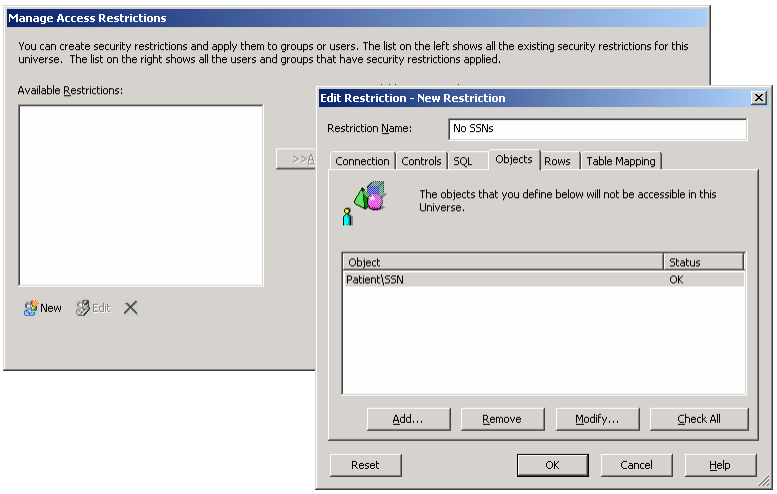
Object-Level Security

Security restricting objects

- **Create lists of restricted objects**
  - As many lists as needed, each independent
- **Assign restricted lists to users/groups**
  - Assign a restriction configuration to as many users/groups as desired
  - Complexity when user belongs to multiple restricted groups

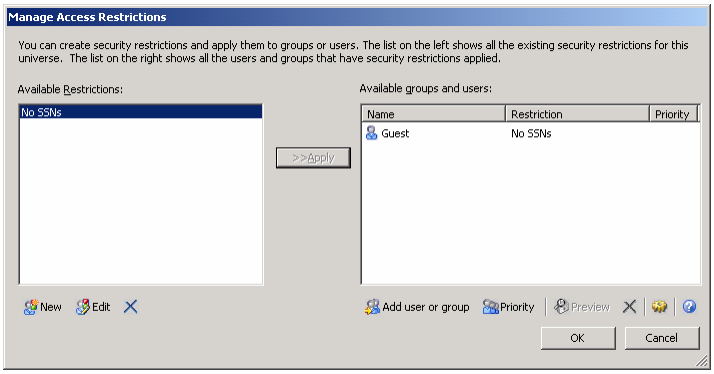
Object-Level Security

Restricting object access – creating a new restriction



Object-Level Security

Restricting object access – applying the restriction to a group



Object-Level Security

Security restricting objects *- meeting our goals*

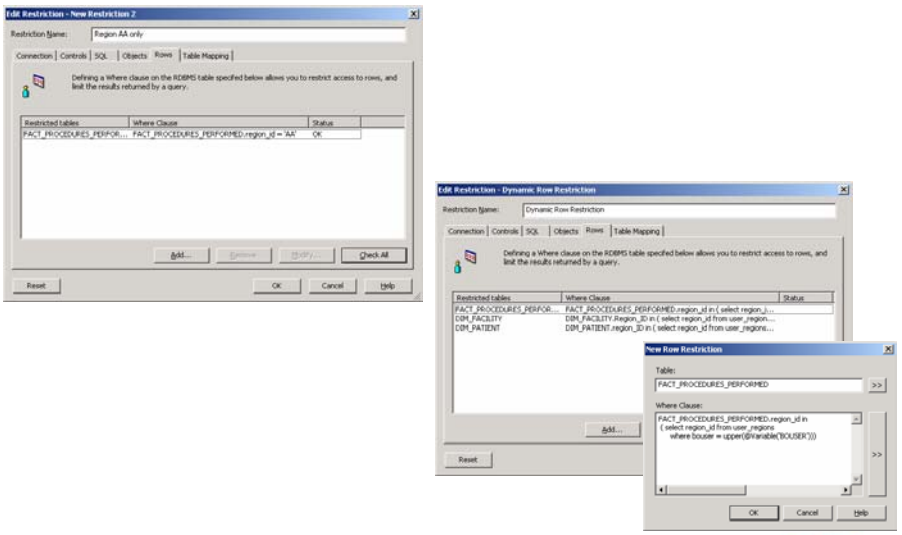
- **Integrated into the environment**
  - ☺ Automatically part of an adhoc report
  - ☹ Security is ignored for distributed reports
- **Minimal performance impact**
  - ☺ Zero runtime performance hit
- **Ease of maintenance**
  - ☺ Fully customizable object lists for each user/group
  - ☹ Memberships in multiple groups and precedence orders makes management complicated
  - ☺ Adding a new user is fairly easy
  - ☹ Adding a new object means updating security in multiple restrictions
  - ☹ Is all or nothing – user can see all values in field or none

Topics

- Goals & Overview
- Object-Level Security
- Row-Level Security
- Data-Value (Masking) Security
- Summary
- Q&A

Row-Level Security

Scenario – users can only view records in specific regions



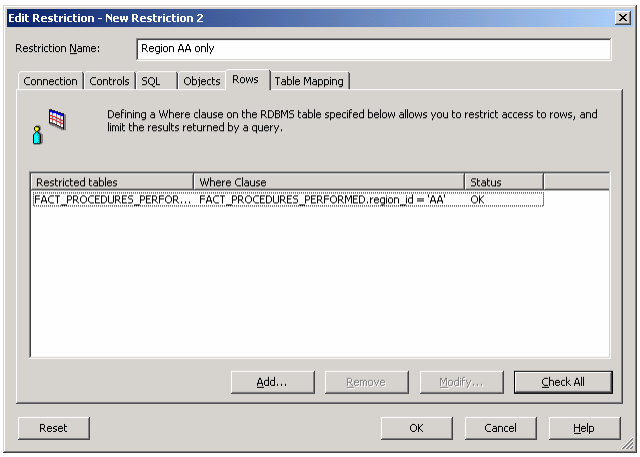
Row-Level Security

What is it?

- **Restricting access to entire records based on security**
  - Additional where clauses are added to queries
- **Where clause tied to each table**
  - Whenever secured table is used where clause added
  - Cannot depend on other tables existing in the query

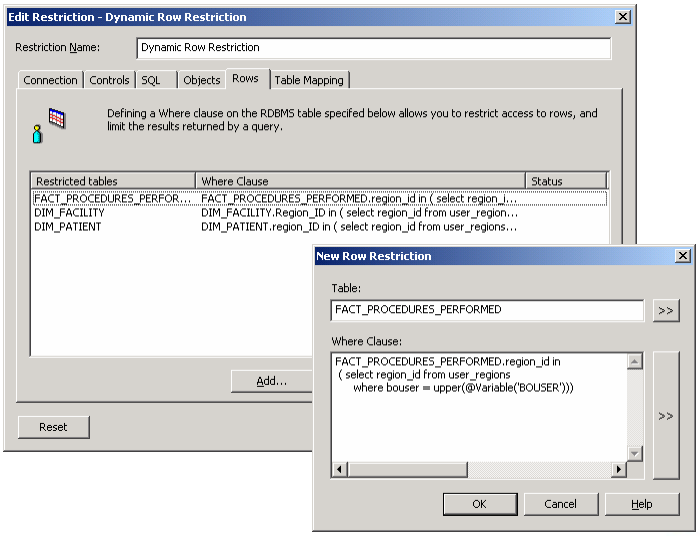
Row-Level Security

Static row restriction



Row-Level Security

Dynamic row restriction



Row-Level Security

Meeting our goals

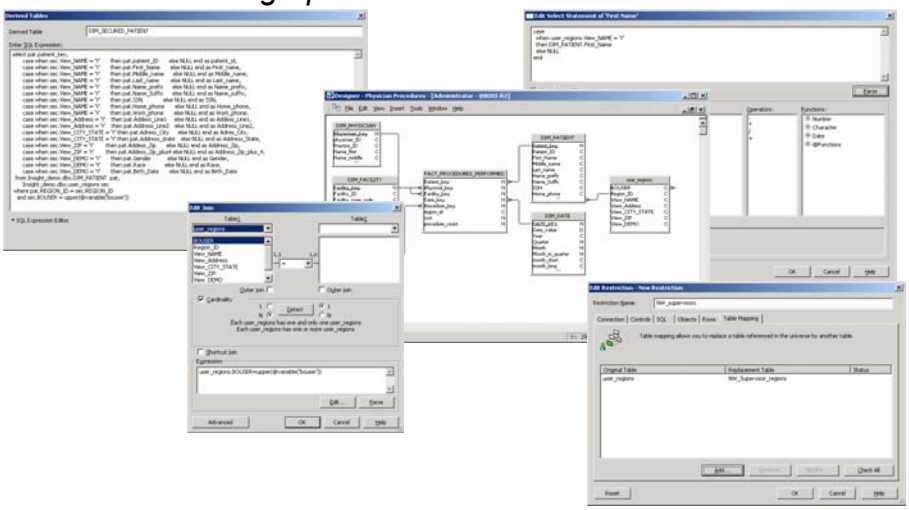
- **Integrated into the environment**
  - ☺ Automatically part of an adhoc report
  - ☺ Distributed reports adjusts to refreshing user
- **Minimal performance impact**
  - 😐 runtime impact depends greatly on queries used
- **Ease of maintenance**
  - ☹ Character limit (250) on row clause limits sophistication of security
  - ☹ Security clause limited to fields within secured tables
  - ☺ Adding new objects on secured tables easy
  - ☹ Difficult to maintain consistent results as user changes queries to include fewer or more secured tables.

Topics

- Goals & Overview
- Object-Level Security
- Row-Level Security
- Data-Value (Masking) Security
- Summary
- Q&A

Data-Value (Masking) Security

Scenario – users can view PHI in some regions but only demographics in others



Data-Value (Masking) Security

What is it?

- **Replacing**
  - Data values user is not allowed to see masked with a generic value
  - Allows users access to general totals where allowed, and detailed information where allowed
- **Two main approaches**
  - Derived tables
  - User-security table join

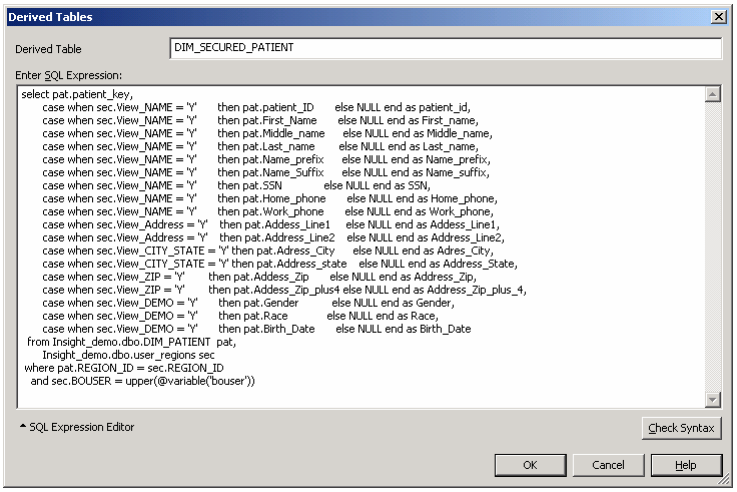
Data-Value (Masking) Security

Derived tables

- **Defining**
  - Like a view, but defined in the universe
  - Derived table definition can reference properties such as the BusinessObjects user name
  - Objects are built from derived field definitions
- **Advantages**
  - Security contained entirely in derived table definition
  - Object definitions simple references to derived table fields
- **Disadvantages**
  - Complex from clauses (entire derived table listed if even one field is referenced)
  - On some databases a derived table disables the use of indexes on joined tables

Data-Value (Masking) Security

Defining a derived table



Data-Value (Masking) Security

Meeting our goals

- **Integrated into the environment**
  - ☺ Automatically part of an adhoc report
  - ☺ Distributed reports adjusts to refreshing user
- **Minimal performance impact**
  - ☹ Disables joining Indexes on some databases
- **Ease of maintenance**
  - ☺ New objects same as unsecured
  - ☺ New users involves small configuration
  - ☹ Derived table: The derived table itself can be complicated to maintain

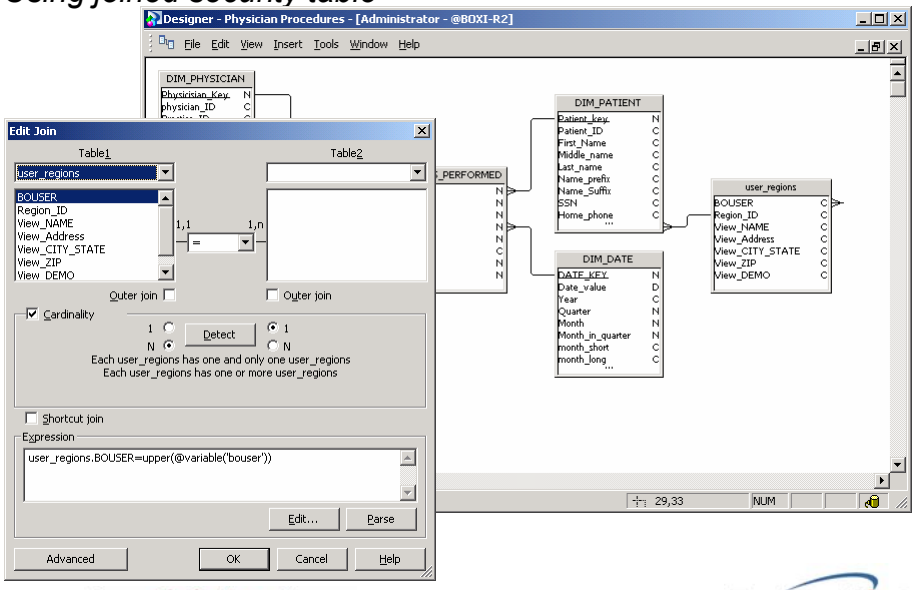
Data-Value (Masking) Security

Joined security table

- **Defining**
  - A table defining security is directly joined
  - Either a single table with a record for every user for each record (or class of records) in secured table
  - Objects defined using both the data table and the security table using case type logic to determine and display either the real value or some generic 'masking' value
- **Advantages**
  - Simple from clauses for queries
  - All joins are table to table, field to field, so indexes should be used
- **Disadvantages**
  - Object definitions are no longer simple field references

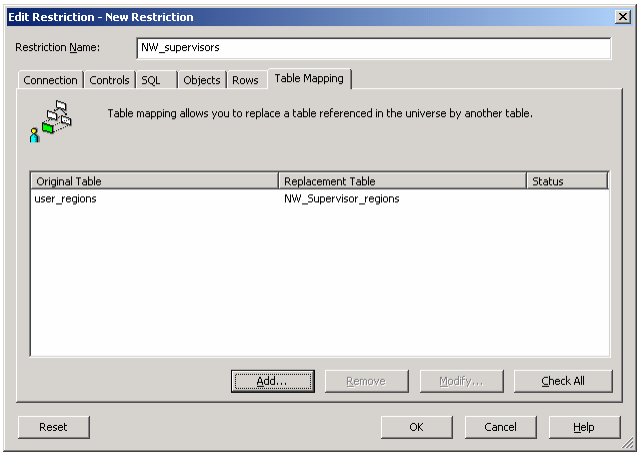
Data-Value (Masking) Security

Using joined security table



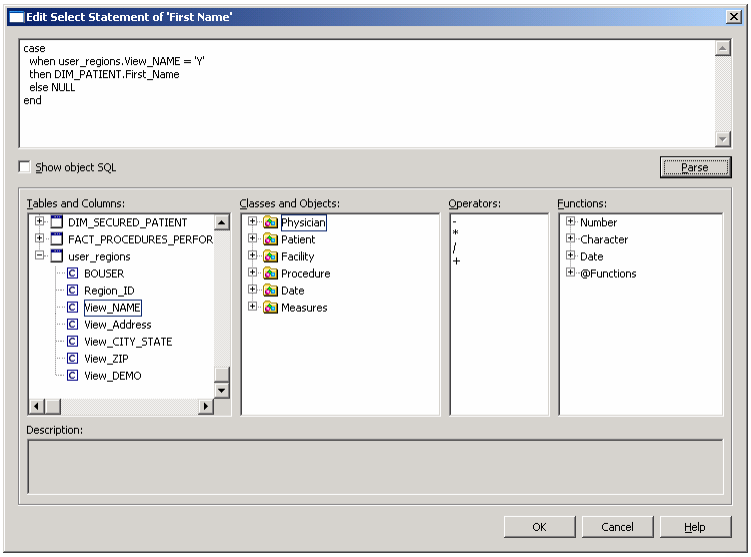
Data-Value (Masking) Security

Using joined security table - variant multiple tables



Data-Value (Masking) Security

Defining objects with joined security tables



Data-Value (Masking) Security

Meeting our goals

- **Integrated into the environment**
  - ☺ Automatically part of an adhoc report
  - ☺ Distributed reports adjusts to refreshing user
- **Minimal performance impact**
  - ☹ Indexes and direct joins minimize impact
- **Ease of maintenance**
  - ☹ New objects more complex
  - ☺ New users usually easy to add, but depends on security model
  - 😐 New universe complicated by need to create several objects

Topics

- Goals & Overview
- Object-Level Security
- Row-Level Security
- Data-Value (Masking) Security
- Summary
- Q&A

Summary

What have we talked about?

- **Three main techniques (plus variants)?**
  - Object-level security
    - Security access levels
    - Security restricting objects
  - Row-level security
    - Static row-restriction
    - Dynamic row-restriction
  - Data-value (masking) security
    - Derived tables
    - Joined security table

Summary

Integration concerns?

- **Using security restrictions for multiple purposes**
  - Object restriction, row-level restricting,table mapping
  - One restriction configuration per group
  - Different types of restrictions need to be maintained together
- **Security being defined twice**
  - Configurations both in database and in the Central Management Console (CMS)
  - Very easy to end up with redundant configurations
  - Redundant configurations harder for maintenance

Topics

- Goals & Overview
- Object-Level Security
- Row-Level Security
- Data-Value (Masking) Security
- Summary
- Q&A

Q&A

- Questions
  - Call Dunn Solutions Group at 1-800-486-3866 x 108

DunnSolutionsGroup