



## Secure Perspective

Fred Robinson - [fdrobin@us.ibm.com](mailto:fdrobin@us.ibm.com)

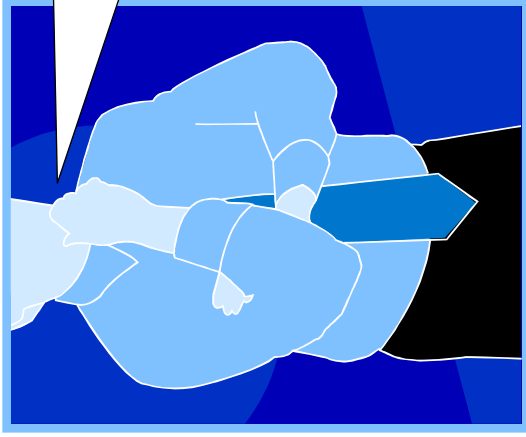
Dan Kolz - [kolz@us.ibm.com](mailto:kolz@us.ibm.com)

[http://ibm.com/systems/i/security/rethink\\_security\\_policy.html](http://ibm.com/systems/i/security/rethink_security_policy.html)

# The Problem

---

Auditor:



So ... why is  
CustUsgFile.dat  
secured as 753?

Administrator:

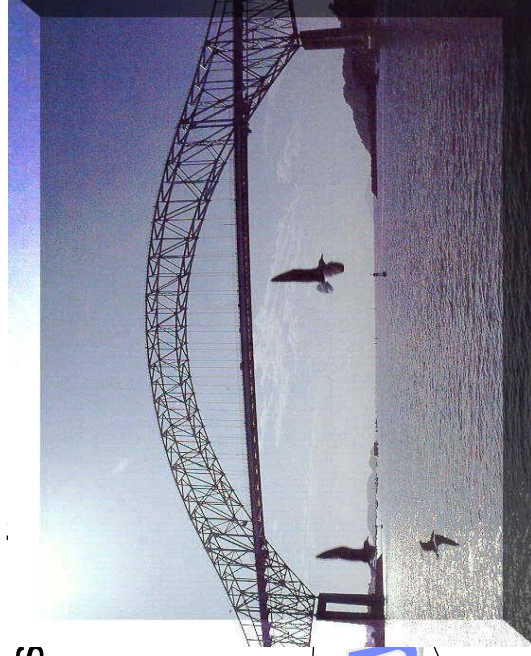


Well ... group mx52b  
needs to read it. I've  
got a note from  
bsmith@us.ibm.com  
right here that says he  
does.

# The Underlying Problem

---

- Security policy is currently driven by the IT staff
- Corporate officers are legally responsible for IT security
  - Business leaders must decide who is allowed access to digital assets
- Policy is the definition of s
  - No policy, no measurement
  - No policy, expensive audits



Policy

Implementation

Compliance with Security Audit Requirements is difficult to prove!

# IBM Secure Perspective

---

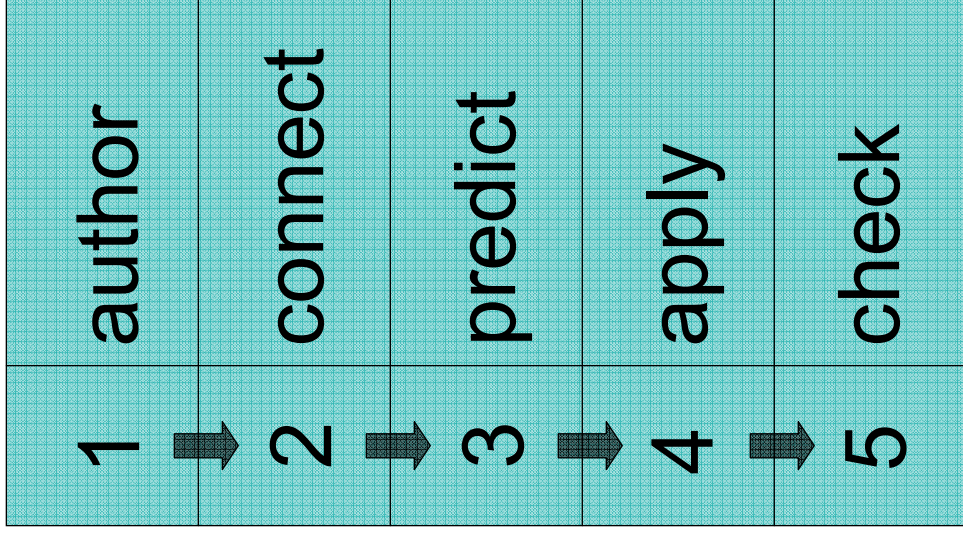
- Security Policy Implementation Facility
  - Based on Sparcle IBM Research Project
- Product – 5733-PS1
  - Hardware – System i
  - Operating System - i5/OS V5R3 V5R4 V6R1
- Availability May 2007 (English Only)
- Price
  - Per processor approx US\$1500 (one time charge)
- November 2007
  - Security Policy management of Windows, AIX, DB2 Servers
  - Windows in addition to i5/OS as a Managing System



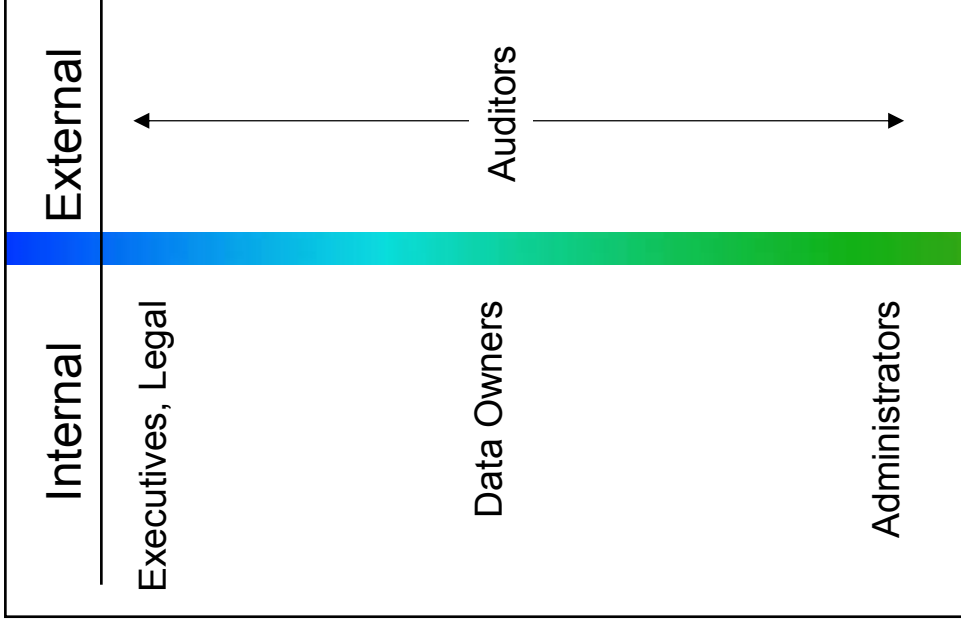
[http://www-03.ibm.com/systems/i/security/rethink\\_security\\_policy.html](http://www-03.ibm.com/systems/i/security/rethink_security_policy.html)

# The Solution - Secure Perspective

---



- Create meaningful policy
- connected to digital assets
- analyzed for problems
- Modifying systems
- checked for compliance



# Secure Perspective

---

- Author
  - Specify Policy Statement
  - Use
    - Actors, Resources, Actions, Purpose
- Connect
  - Map
    - Actors to user IDs
    - Resources to files, directories, and tables
    - Map Actions to system control mechanisms
- Predict
  - Problems with Policy implementation
- Apply
  - Change System
  - Report Changes
- Check
  - Compliancy validation – at anytime

## Benefits of Secure Perspective

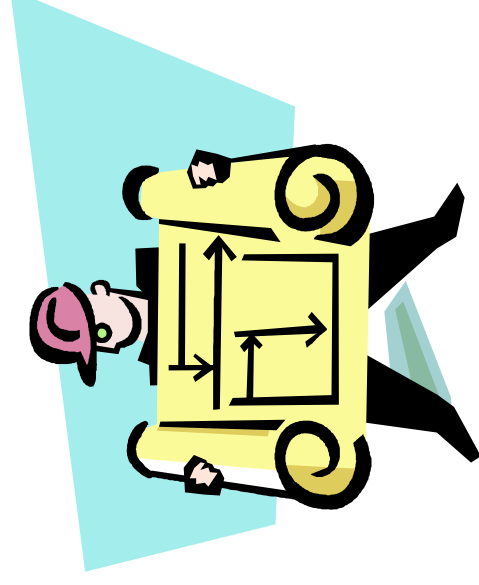
---

- Policies are written in natural language
- Mapped data is managed by the tool
- Easy Policy applications or compliance checks
- Reports saved
  - Policy application
  - Compliance checks
- Review effect of security policy on business processes

# Secure Perspective - Process

---

- Develop “Blueprint” of strategy
  - Know your objectives – What do you want to accomplish?
  - Know your scope – What/Who has to be covered?
  - Know your data – What is being secured?
- Follow a method
  - Repeatable process
  - Complete Security Policy
  - Reduce risk





# Author Security Policy

---

- Assemble stakeholders
  - Business leaders
  - Data owners
  - System administrators
  - Legal analysts
  - Internal auditors
- Consider legal/audit requirements
- Identify Key Assets/Resources to be managed
  - Enter Data Types
- Identify Roles/Responsibilities of Users (actors)
  - Enter Users identified in roles/responsibilities
- Enter Data Interactions
  - Enter Actions
- Establish Policy
  - Plain Language

# Connect

---

- Identify the Systems
  - Add to the System Configuration List
- Connect Policy terms to Business Assets

# Predict Problems

---

- Validate Result against Policy
  - Meets compliance standards?
- Make changes
  - Rerun compliance check
- Ensure Procedures are unaffected

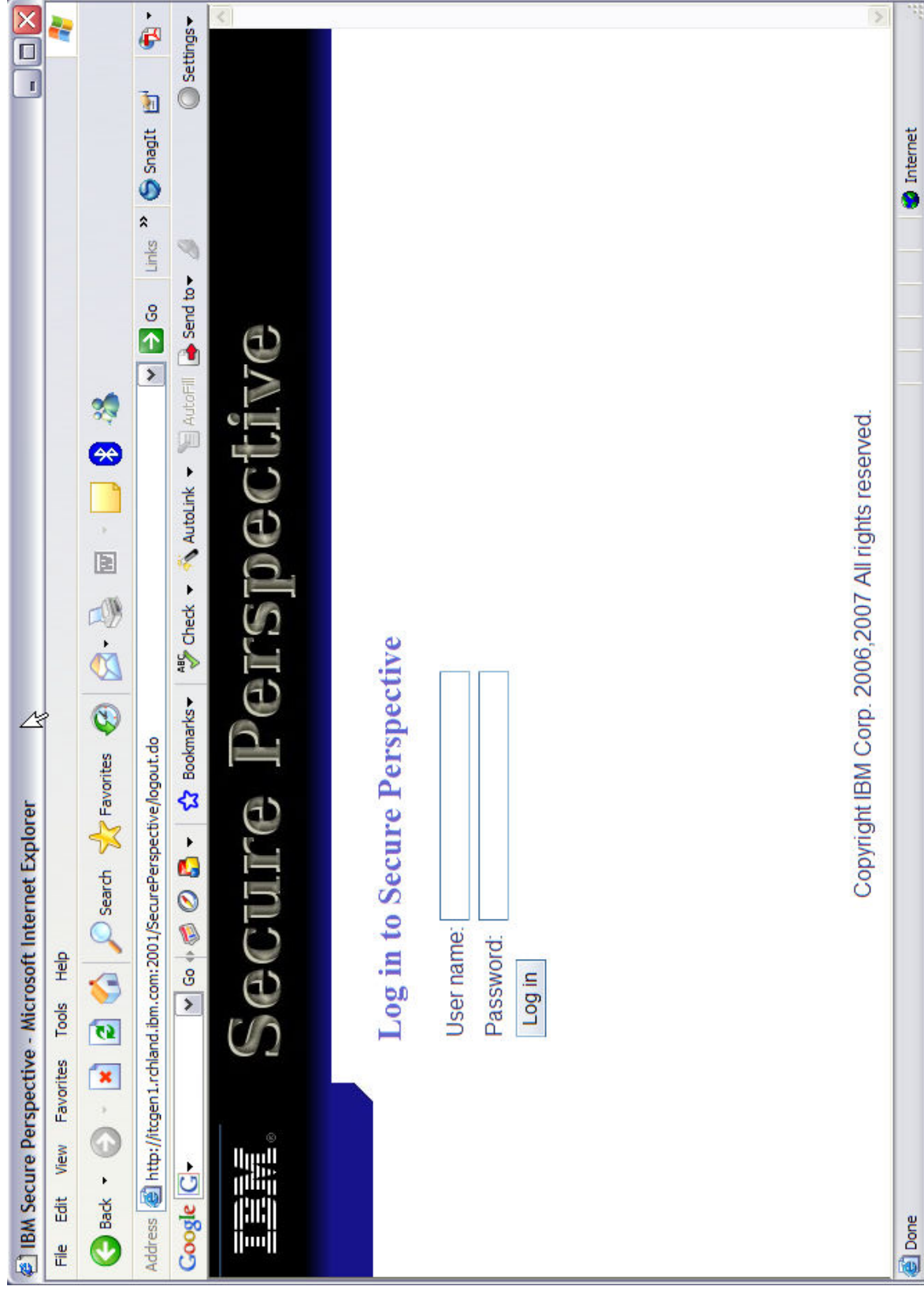
# Apply the Policy

---

- Only ONE Security Policy is CURRENT
- Modify the System
  - Create/Change
    - User profiles
    - Object authorities
- Optional “undo”
- Manage Policy
  - Routine compliance checks
  - Control Administration
    - Designate Policy Administrators
- Export the applied Policy
  - “Backup”
  - Maybe Imported
- Print Policy Summary
  - Future Review
  - Audit

# Login

---



# Home Page

Secure Perspective Home

Secure Perspective allows the access to resources on a system to be controlled with a policy. Each policy is composed of a set of statements which specify which groups of users, called Actors, should be allowed to access a group of system objects, called Resources. The following flow chart provides an example of the tasks needed to be completed and a suggested order in which to complete these tasks in order to implement a meaningful and secure policy. \*click the images to work with the specific tasks

```
graph LR; TD[Term Dictionary] --> DC[Domain Configuration]; DC --> P[Policies]; P --> TM[Term Mappings]; TM --> PA[Policy Actions]
```

# Term Dictionary

## Term Dictionary

The Term Dictionary contains the building blocks of policies. The dictionary has a set of Actors, Resources, Actions, and Purposes. Each term may also have a set of synonyms that can be used in a policy.

### [View/Modify Dictionary Terms](#)

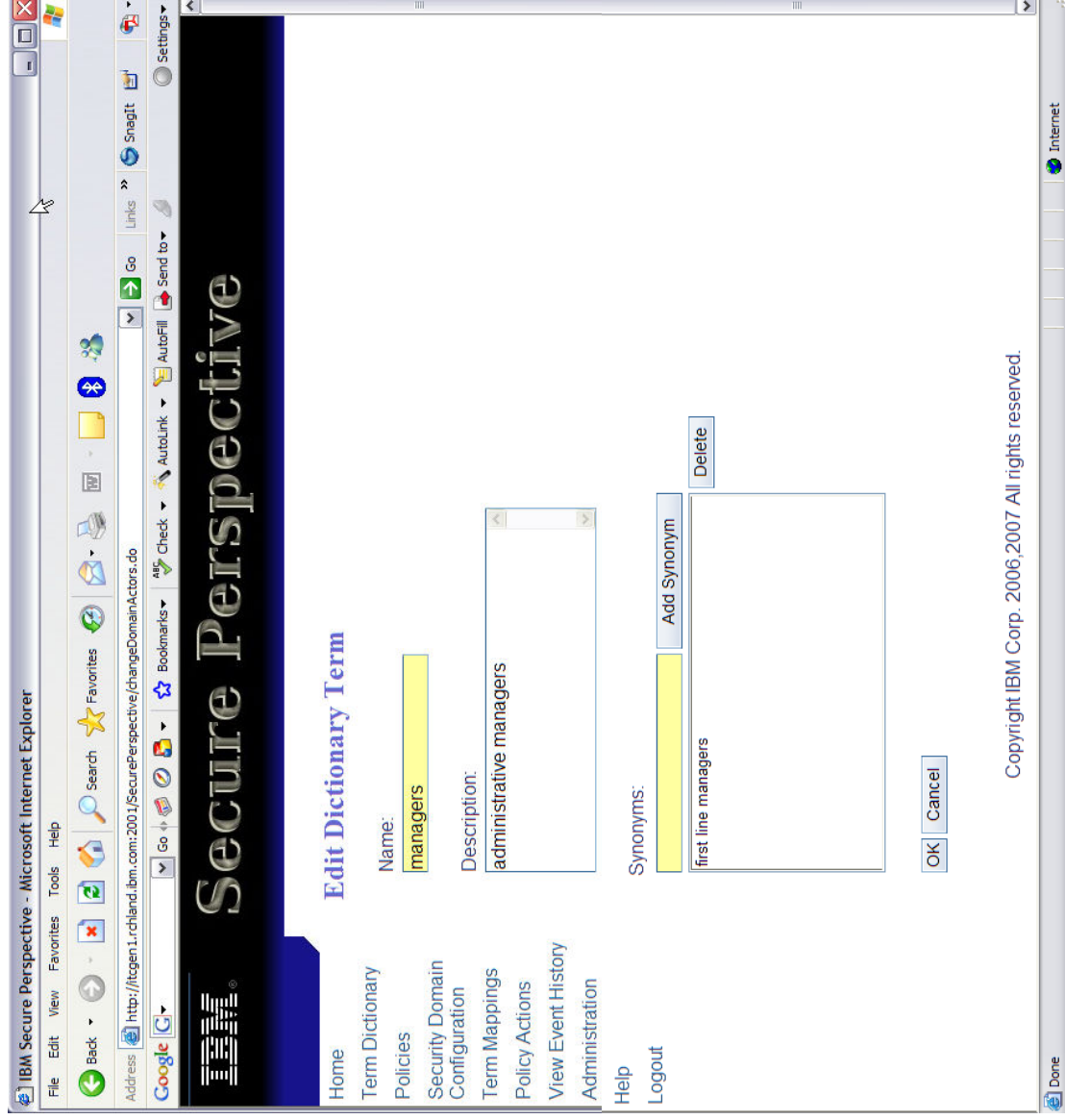
- Actors** Actors are groups of people that share a role or need for information within the organization.
- Actions** Actions specify ways in which an Actor can interact with a Resource.
- Resources** Resources are groups of data that should have the same access rules.
- Purposes** Purposes specify the reasons for which an Actor can interact with a Resource.

### [Import/Export Dictionary Terms](#)

- Import** Imports the term dictionary from an xml file.
- Export** Exports the term dictionary to an xml file.

# Actors – Who?

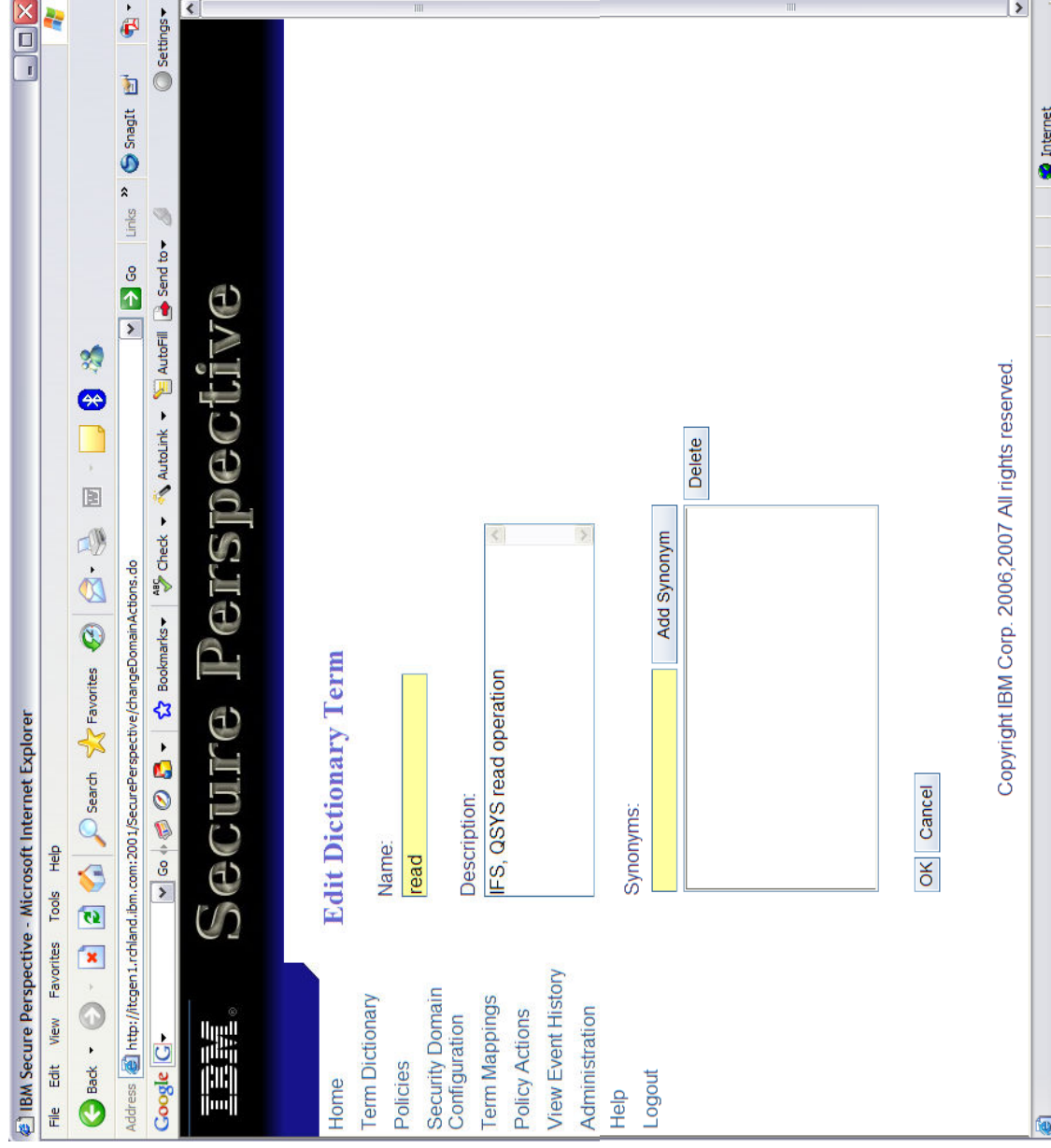
---



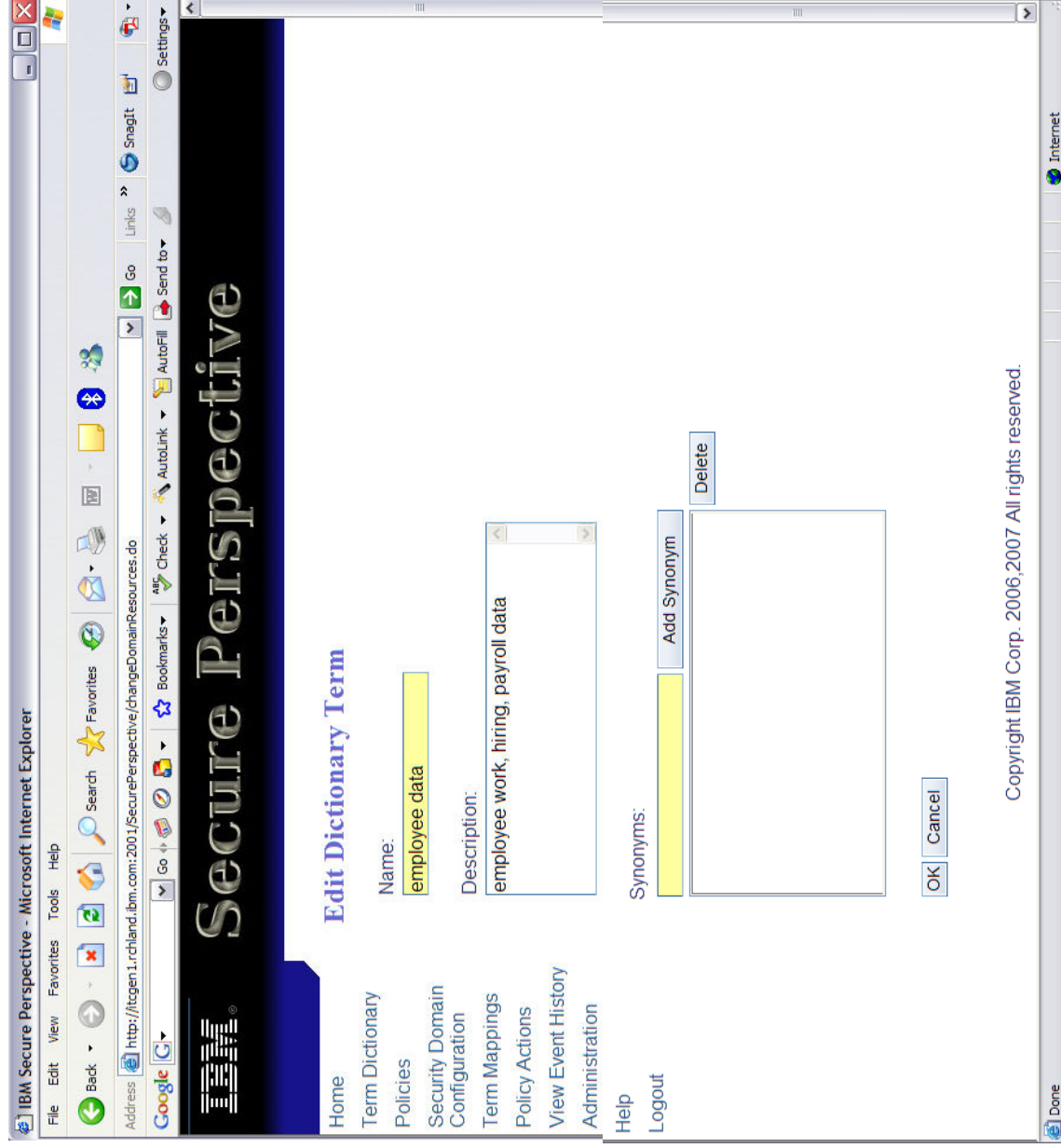


# Actions – How?

---



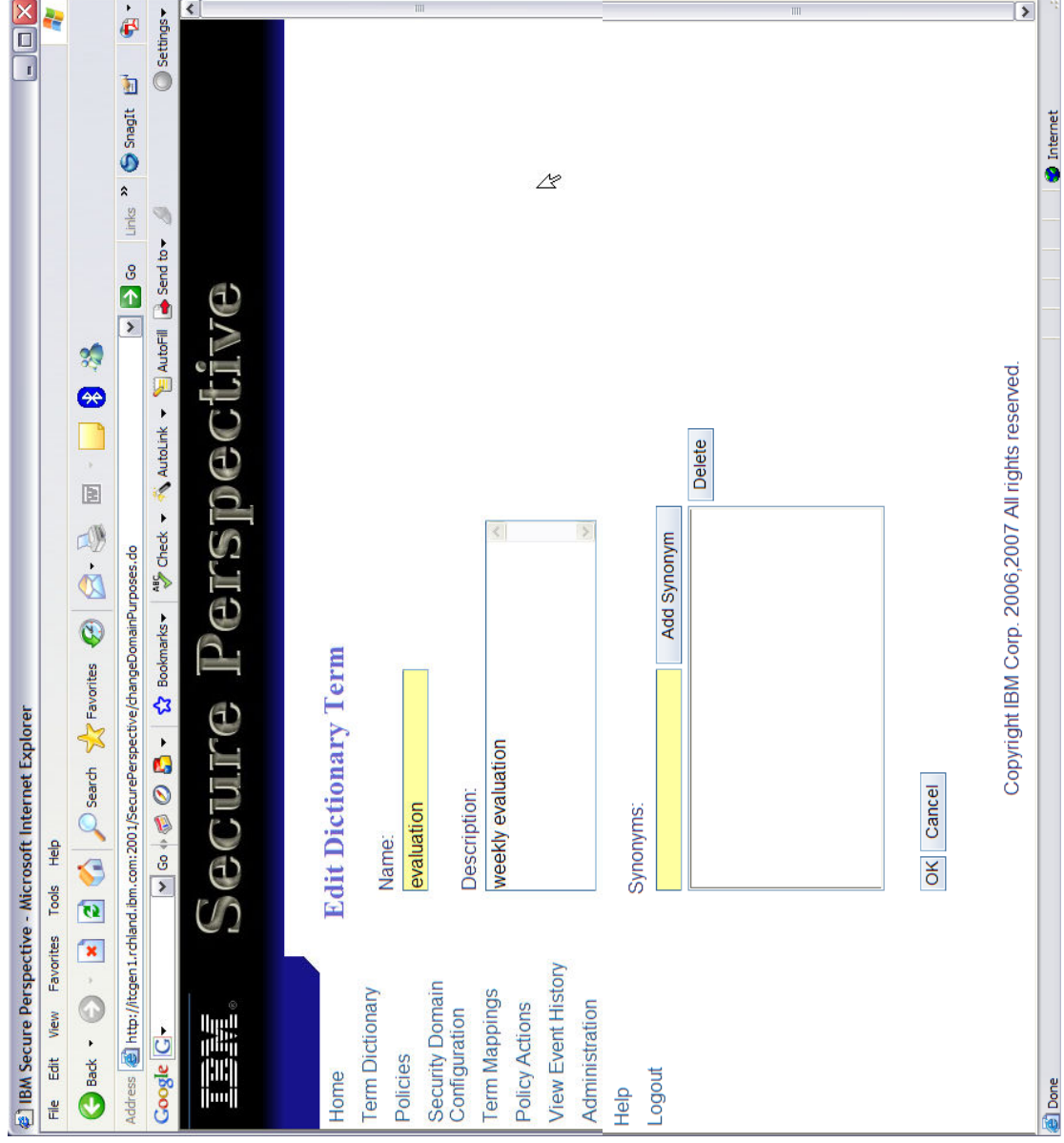
# Resources – What?



Copyright IBM Corp. 2006, 2007 All rights reserved.

# Purposes – Why?

---



# Policy Title

The screenshot shows a Microsoft Internet Explorer browser window displaying the IBM Secure Perspective web application. The browser's address bar shows the URL: <http://ftcgen1.rchland.ibm.com:2001/SecurePerspective/changePolicies.do>. The page features a large blue header with the IBM logo and the text "Secure Perspective". Below the header, the main content area is titled "Change Policy" and displays details for a policy named "Business Policy 1".

**Change Policy**

**Policy Attributes**

Name: Business Policy 1  
Description: Policy that restricts access to employee data  
Last Changed: Jul 5, 2007 9:41:05 AM  
[Edit Name and Description...](#)

**Policy Statement Types**

Resource Access   
[Edit Structured](#)  
[Edit Text](#)  
[View Policy Matrix](#)  
[Analyze](#)

Password Statements   
[Edit Structured](#)

**Navigation Links:** Home, Term Dictionary, Policies, Security Domain Configuration, Term Mappings, Policy Actions, View Event History, Administration, Help, Logout.

**Footer:** Copyright IBM Corp. 2006,2007 All rights reserved.

# Policy Structure

The screenshot shows a web browser window displaying the IBM Secure Perspective interface. The browser's address bar shows the URL: `http://tgen1.rchland.ibm.com:2001/SecurePerspective/changePolicy.do`. The page title is "Secure Perspective".

The main content area is titled "Resource Access Statements" and shows a policy named "Policy: Business Policy 1". The policy statement is: "Managers or hr staff can read employee data for the purpose of evaluation." Below the statement, there are three sections for configuration:

- Policy statements:** A list containing one statement: "Managers or hr staff can read employee data for the purpose of evaluation." It includes "Add", "Delete", and "Edit Text" buttons.
- Actors:** A list containing "hr staff" and "managers", both with checked checkboxes and "Edit..." buttons.
- Purposes:** A list containing "employee data" and "evaluation", both with checked checkboxes and "Edit..." buttons.

At the bottom of the configuration area, there are "Save", "OK", and "Cancel" buttons. The footer of the page contains the text: "Copyright IBM Corp. 2006,2007 All rights reserved."

IBM Secure Perspective - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

Go

Merriam-Webster Online Overview (Java 2 Pla...)

# Secure Perspective

## View Policy Matrix

Policy: Test Policy

X axis value:  Y axis Value:  Intersection value:

	managers	users
accounting data	modify	read
confidential material	modify	
payroll		write

Home

Term Dictionary

Policies

Security Domain Configuration

Term Mappings

Policy Actions

View Event History

Administration

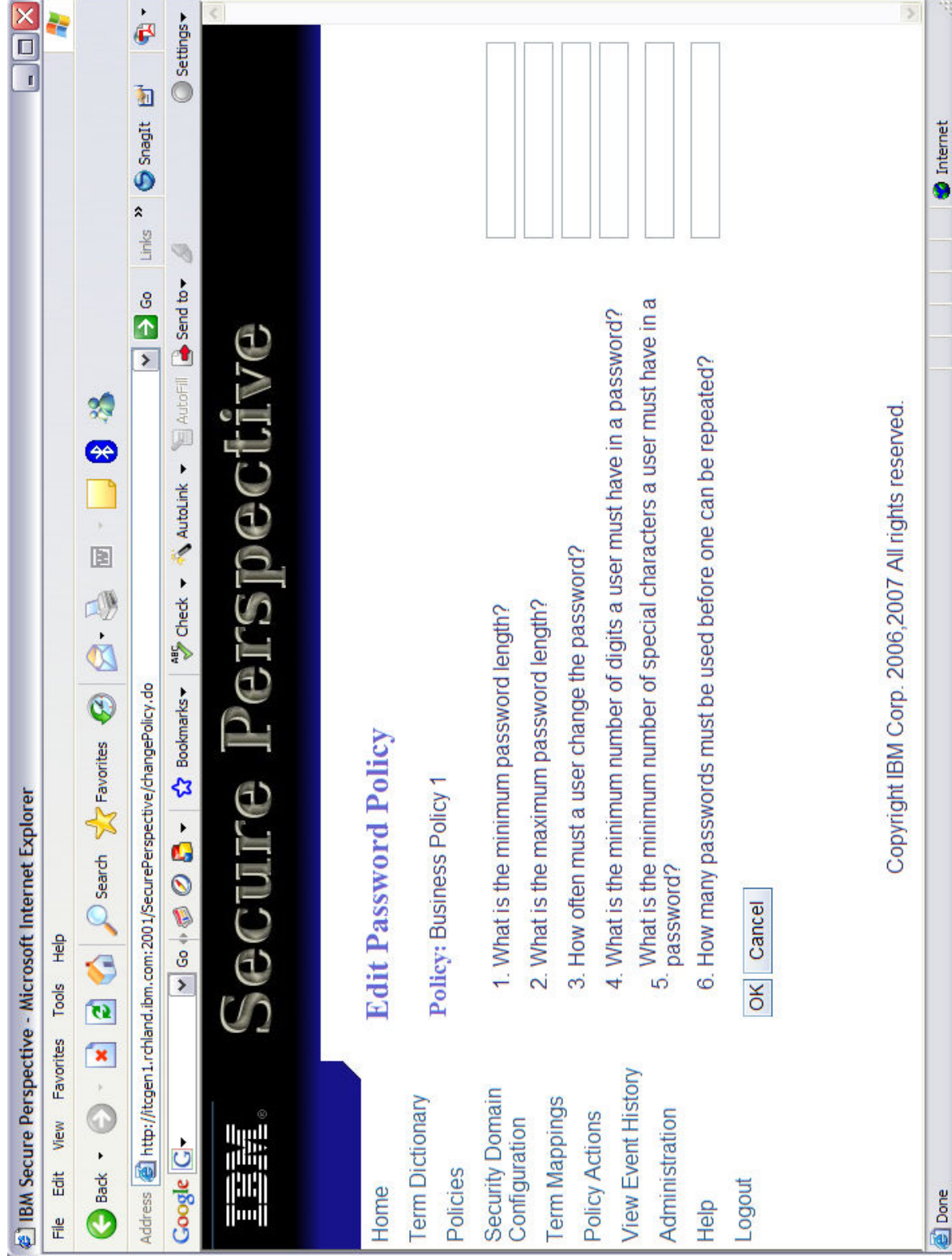
Help

Logout

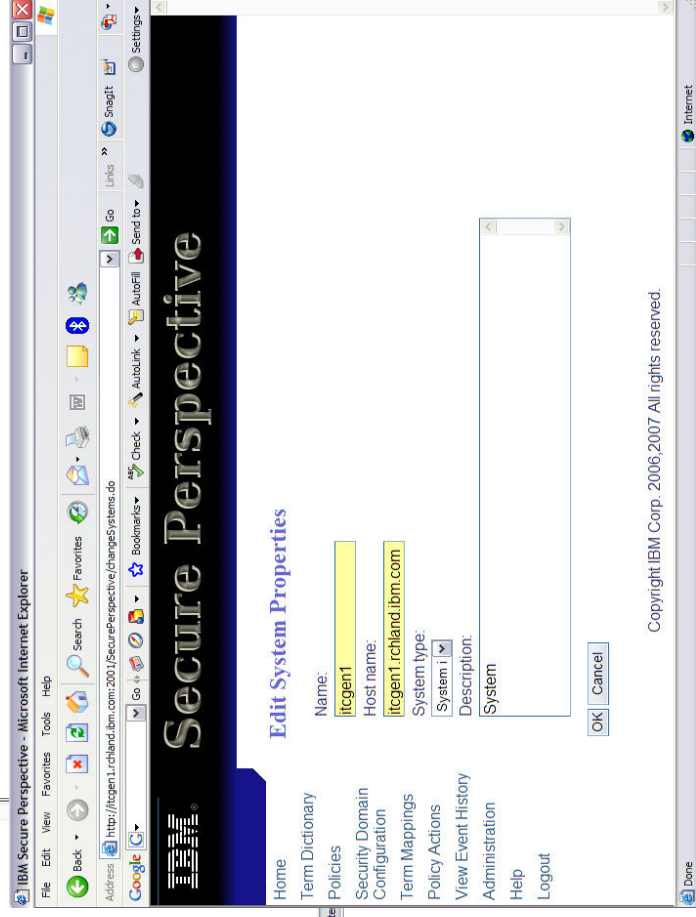
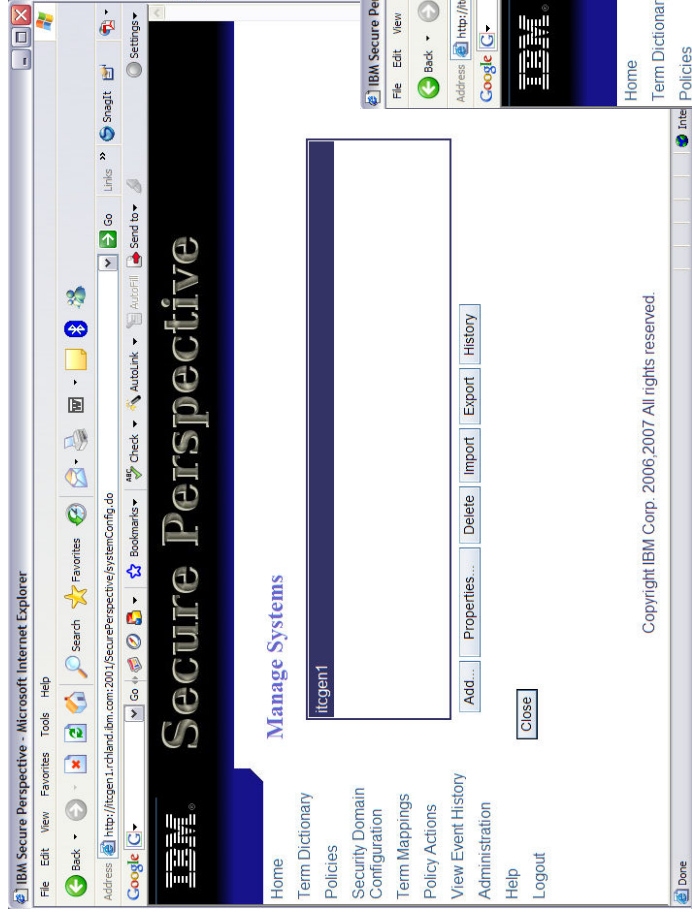
Done

Copyright IBM Corp. 2006,2007 All rights reserved.

# Password Policy



# Security Domain





# Term Mapping-Actors

The screenshot shows the 'Edit Term Mappings' dialog box in the IBM Secure Perspective application. The dialog is titled 'Edit Term Mappings' and includes a 'Printable Summary' link. It is for 'System: itcgen1'. The 'Actors' tab is selected, showing a list of actors: 'hr staff' and 'managers'. The 'Unmapped Profiles' list contains: AS024GRP, DB2XML, DICK, DOUGA, FDROBIN, GJAMES, GREATGUY, KOLZ, LPTEST, NRAUT, PROFILE6, QANZAGENT, QAUTPROF, QBRWS, and QCLUMGT. The 'Mapped Profiles' list contains: LLOYD and SPKOLZ. There are 'Add -->' and '<-- Remove' buttons between the lists. At the bottom are 'OK' and 'Cancel' buttons. The background shows the application menu with options like Home, Term Dictionary, Policies, Security Domain Configuration, Term Mappings, Policy Actions, View Event History, Administration, Help, and Logout.

Copyright IBM Corp. 2006, 2007 All rights reserved.

# Term Mapping-Actions

The screenshot shows a Microsoft Internet Explorer browser window displaying the IBM Secure Perspective web application. The browser's address bar shows the URL: `http://itcgen1.rchland.ibm.com:2001/SecurePerspective/modifyTermMappingsForSystem.do`. The page title is "IBM Secure Perspective".

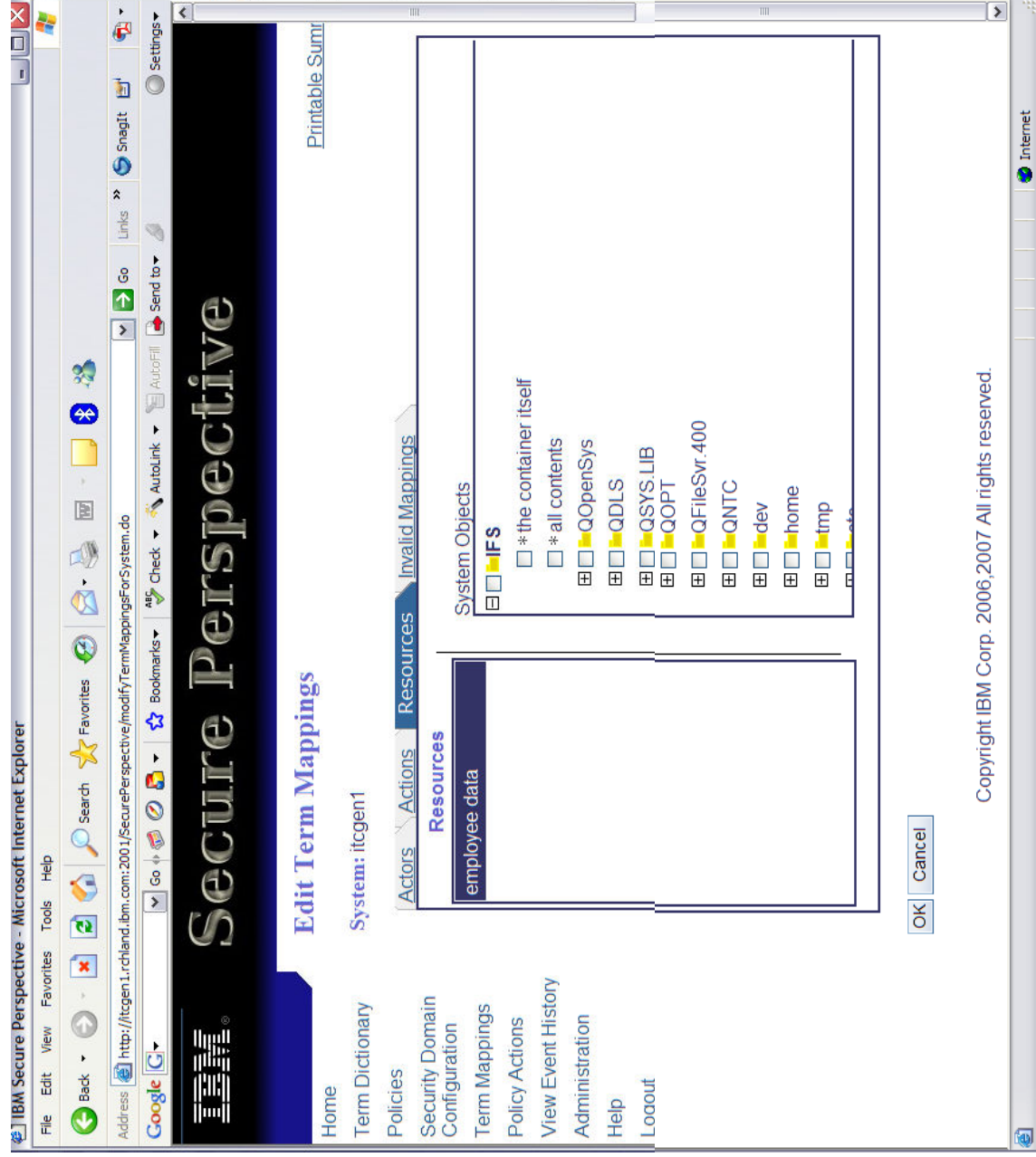
The main content area features a navigation menu on the left with the following items: Home, Term Dictionary, Policies, Security Domain Configuration, Term Mappings, Policy Actions, View Event History, Administration, Help, and Logout. The "Term Mappings" section is active, showing "System: itcgen1".

The "Edit Term Mappings" dialog box is open, displaying the "Actions" tab. The "read" action is selected in a list box. To the right, there are two columns of permissions, each with a list of actions and a corresponding checkbox:

Integrated File System:	QSYS:
read <input checked="" type="checkbox"/>	read <input checked="" type="checkbox"/>
write <input type="checkbox"/>	write <input type="checkbox"/>
execute <input type="checkbox"/>	execute <input type="checkbox"/>
opr <input checked="" type="checkbox"/>	opr <input checked="" type="checkbox"/>
exist <input checked="" type="checkbox"/>	exist <input checked="" type="checkbox"/>
mgt <input checked="" type="checkbox"/>	mgt <input checked="" type="checkbox"/>
alter <input checked="" type="checkbox"/>	alter <input checked="" type="checkbox"/>
ref <input checked="" type="checkbox"/>	ref <input checked="" type="checkbox"/>

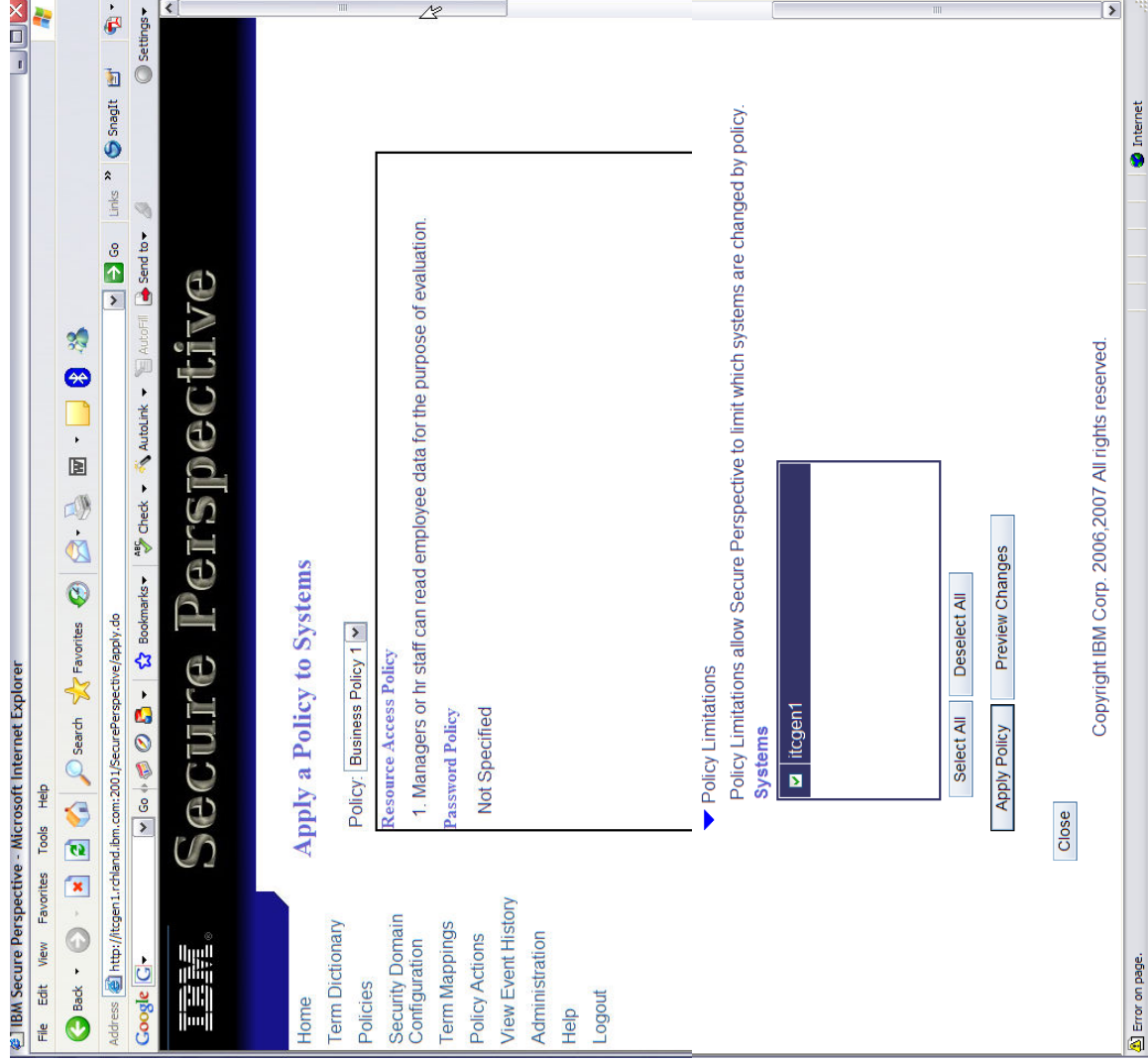
At the bottom of the dialog box, there are "OK" and "Cancel" buttons. The footer of the browser window contains the text: "Copyright IBM Corp. 2006,2007 All rights reserved."

# Term Mapping-Resources



Copyright IBM Corp. 2006,2007 All rights reserved.

# Apply Policy



# i5/OS Security Policy Commands

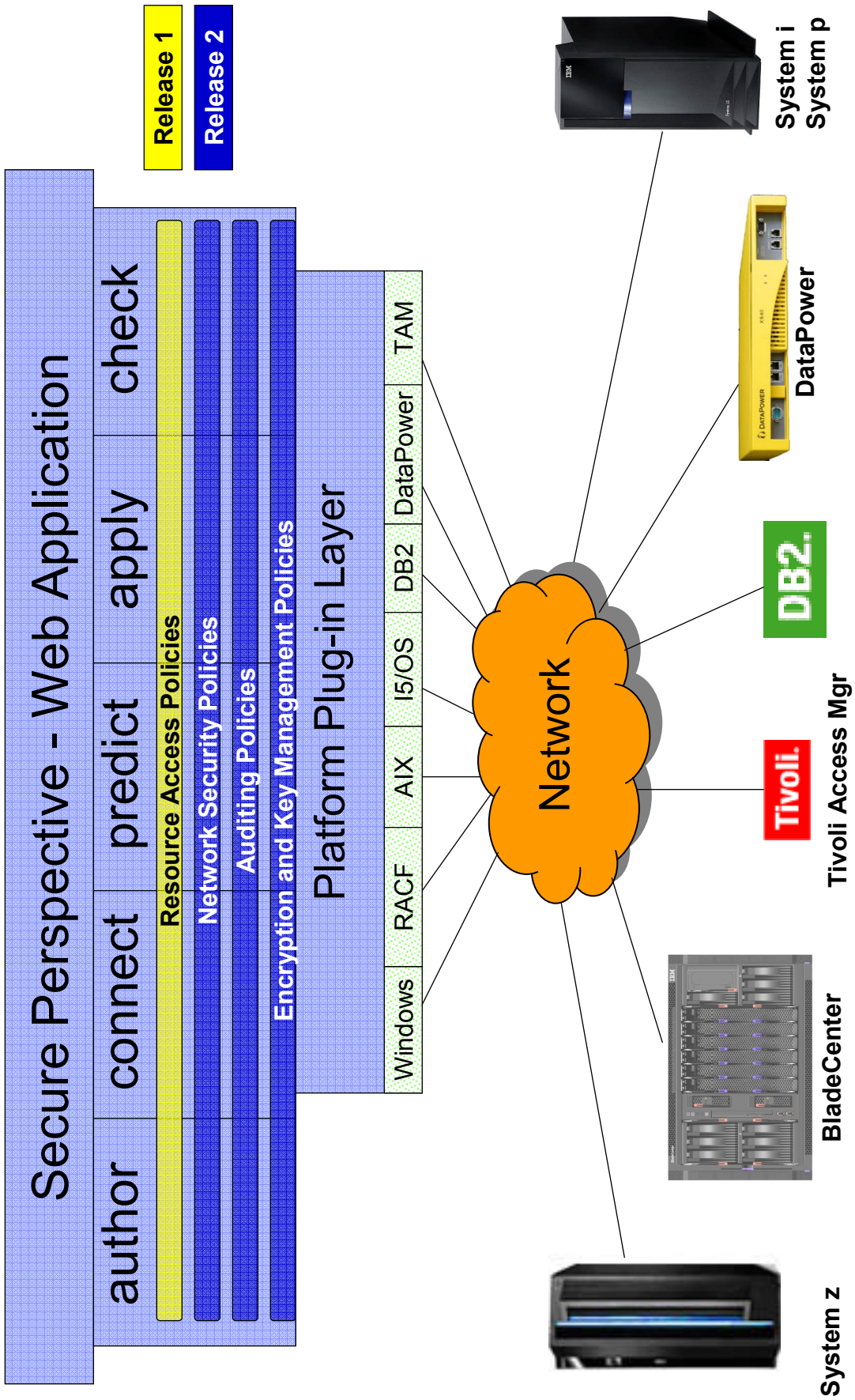
---

▼ Change statements for system: Business System 1

**Status**   **Statement**

success	CHGAUT OBJ('/Education/Labs/test1.txt') USER('PUBLIC) DTAAUT('EXCLUDE) OBJAUT('NONE)
success	CHGAUT OBJ('/Education/Labs/test1.txt') USER('KSHIM) DTAAUT('NONE) OBJAUT('NONE)
success	CHGAUT OBJ('/Education/Labs/test2.txt') USER('PUBLIC) DTAAUT('EXCLUDE) OBJAUT('NONE)
success	CHGAUT OBJ('/Education/Labs/test2.txt') USER('KSHIM) DTAAUT('NONE) OBJAUT('NONE)
success	CHGAUT OBJ('/Education/Labs/test1.txt') USER('PUBLIC) DTAAUT('EXCLUDE) OBJAUT('NONE) SUBTREE('ALL)
success	CHGAUT OBJ('/Education/Labs/test1.txt') AUTL('NONE) SUBTREE('ALL)
success	CHGAUT OBJ('/Education/Labs/test2.txt') USER('PUBLIC) DTAAUT('EXCLUDE) OBJAUT('NONE) SUBTREE('ALL)
success	CHGAUT OBJ('/Education/Labs/test2.txt') AUTL('NONE) SUBTREE('ALL)
success	CRTAUTL AUTL(QSY1000002) TEXT('employee data') AUT('EXCLUDE)
success	CHGAUT OBJ('/Education/Labs/test1.txt') AUTL(QSY1000002) SUBTREE('ALL)
success	CHGAUT OBJ('/Education/Labs/test2.txt') AUTL(QSY1000002) SUBTREE('ALL)
success	ADDAUTLE AUTL(QSY1000002) USER(SPJOHN) AUT('READ )
success	ADDAUTLE AUTL(QSY1000002) USER(SPJANE) AUT('READ )

# Secure Perspective Architecture



# New/Improved GUI features – November 2007

---

- Homepage
- Menu bar
- Term mappings
  - List / tree views
  - Filterable
- General look & feel
- Improved event history
- Help

# New Wildcard Mapping

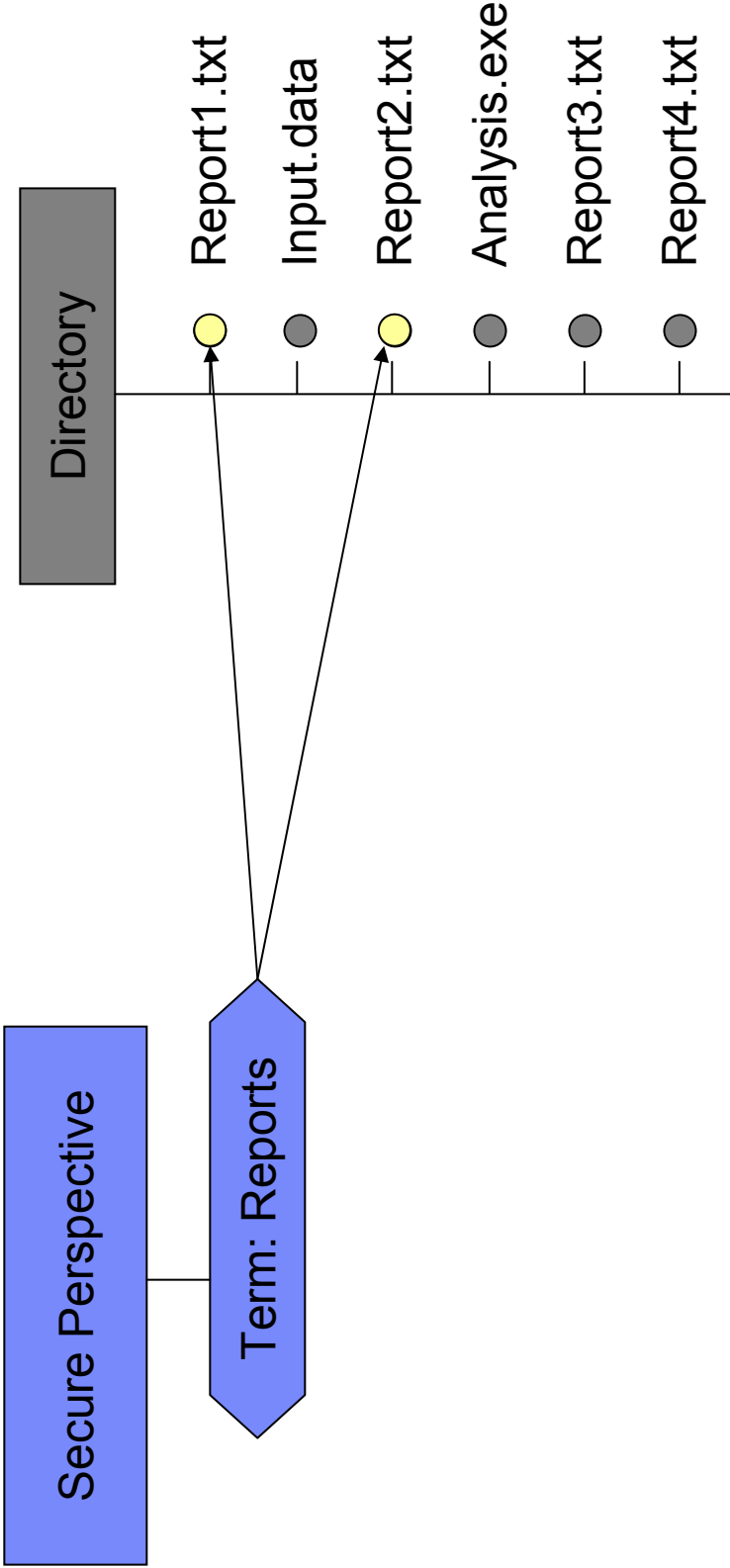
---

- Example problem
  - You need to map several shell scripts in a directory to the same resource
  - These scripts change frequently and may not be the same at apply time as they were at map time
- Solution: Create a wildcard filter
  - Create filename-based filters (e.g., `*.sh` or `*account*`)
  - Map the filters to resource terms just as you would files
  - Apply policy—files matching the filter are automatically mapped to that term (if not explicitly mapped to another term)



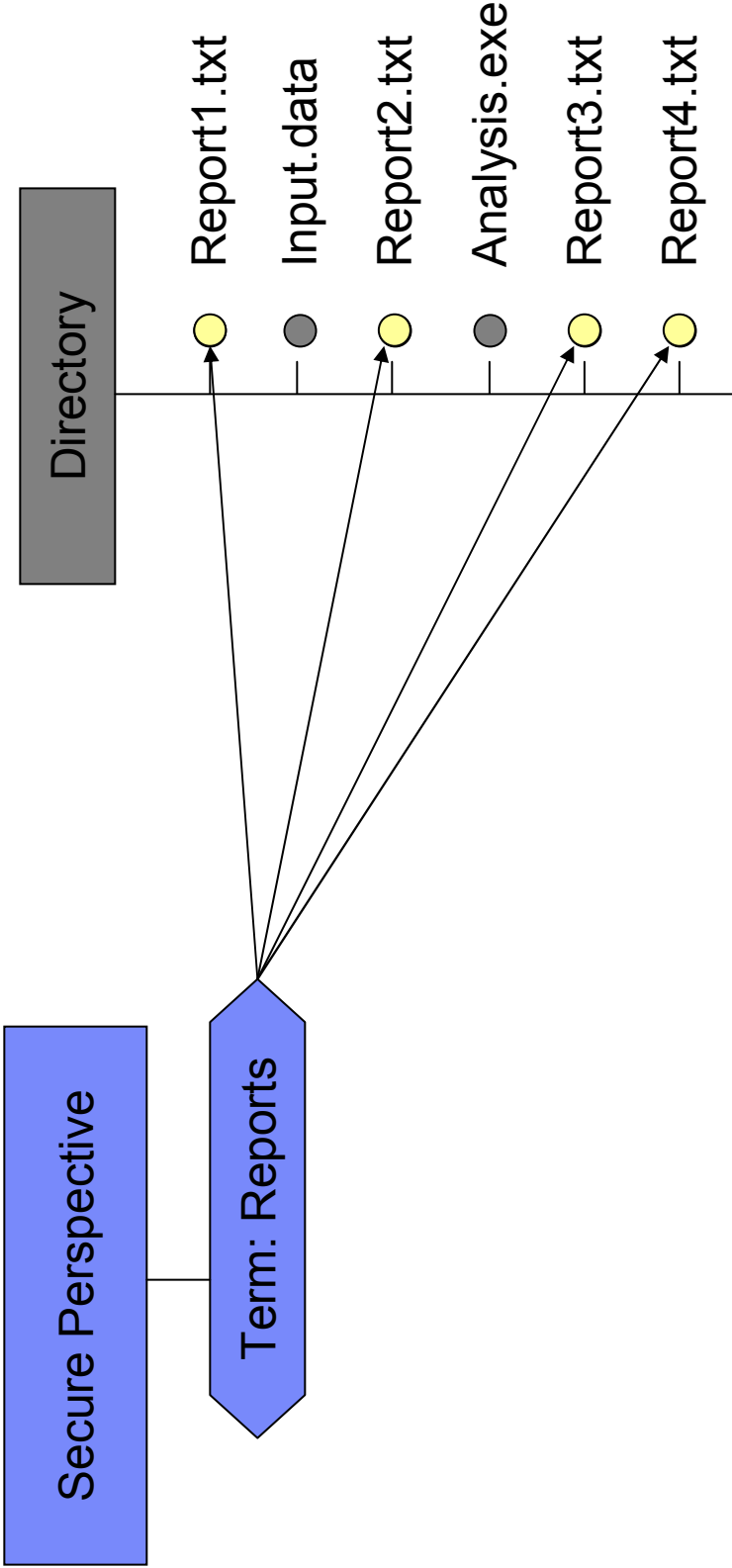
# Wildcard Mapping Example

---



# Wildcard Mapping Example (2)

---



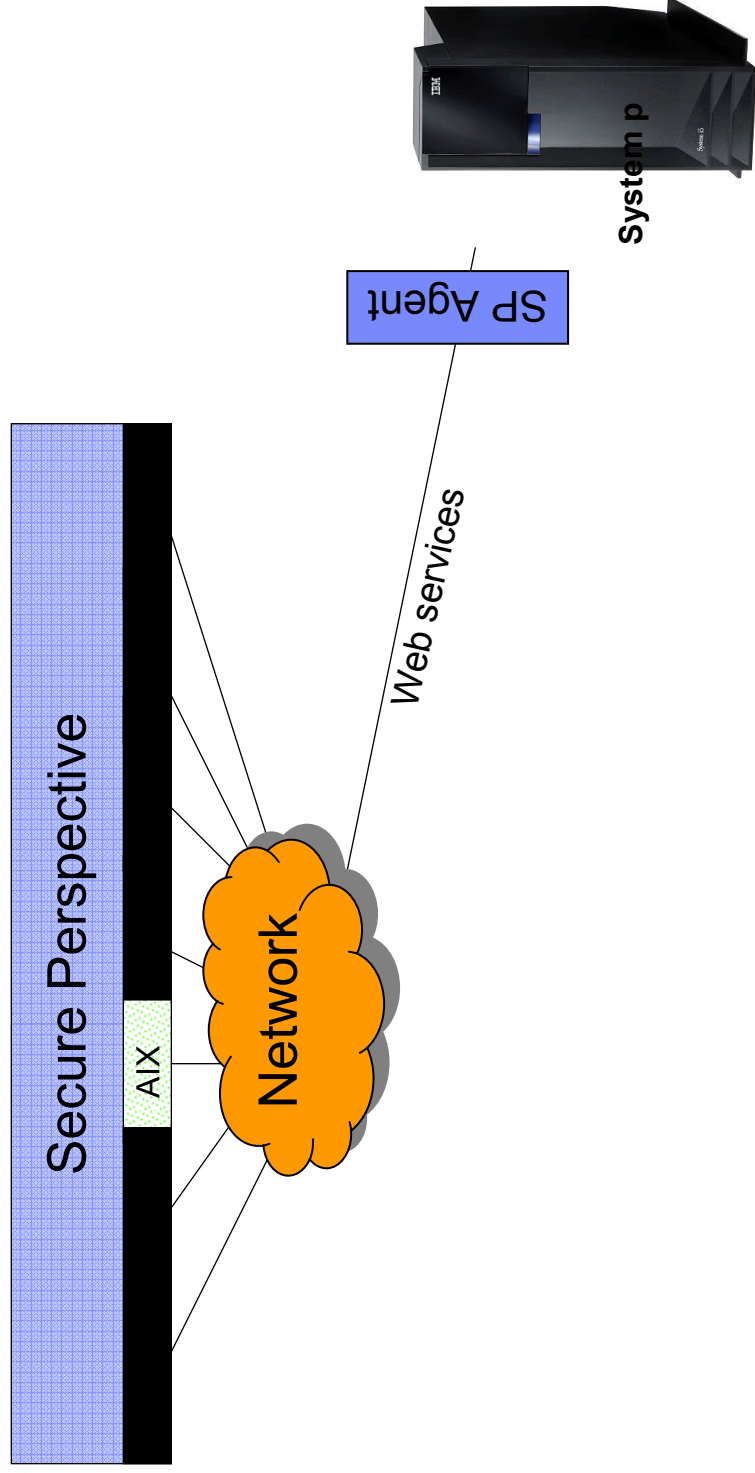
# Cross-platform Capabilities

---

- i5/OS
- AIX (New)
- Windows (New)
- DB2 (New)

# AIX Capability Architecture

---



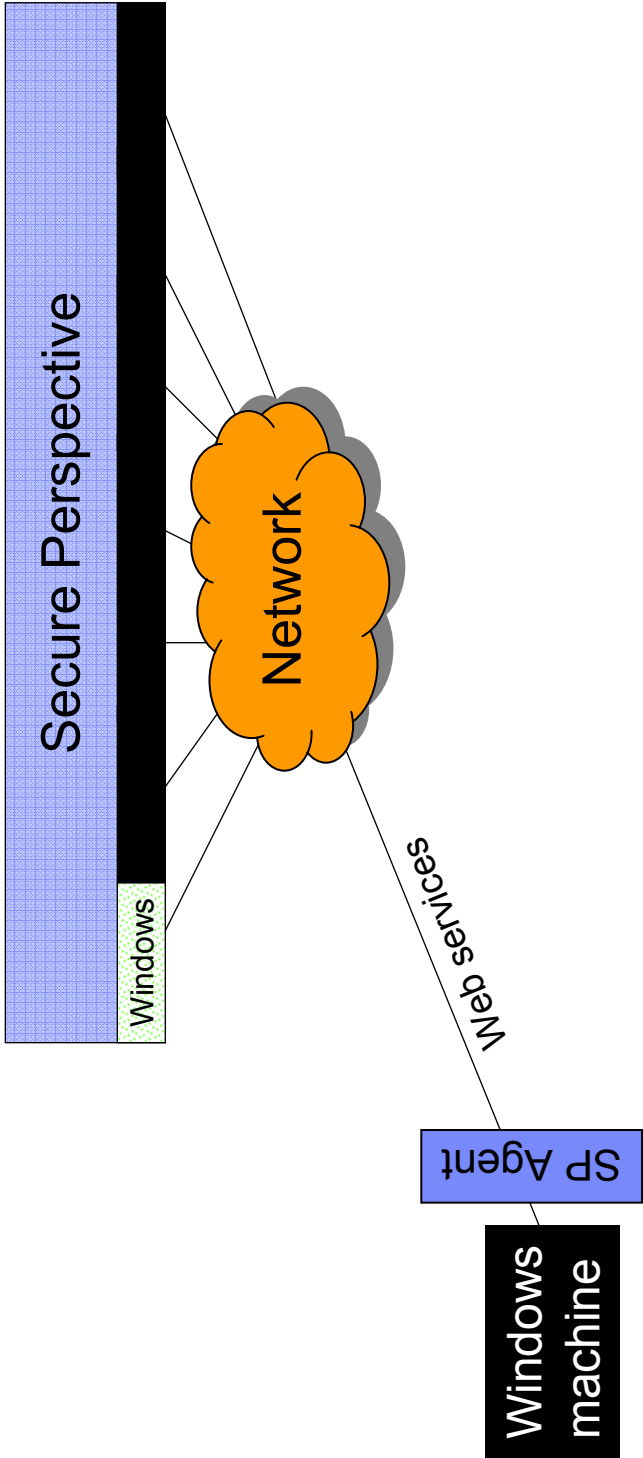
# AIX Access Rights

---

- Controlled using NFS4 access control lists on the JFS2 version 2 file system
- Controls the following access rights:
  - Read
  - Write
  - Execute
  - Append
  - Delete
  - Read attributes
  - Write attributes
  - Read named attributes
  - Write named attributes

# Windows Capability Architecture

---



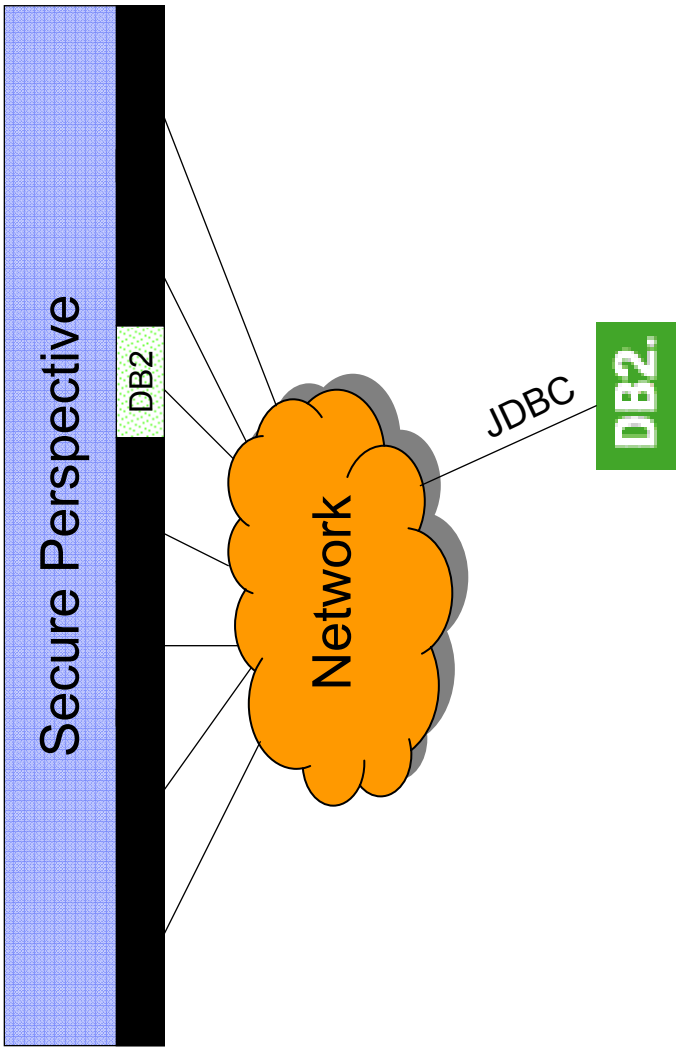
# Windows Access Rights

---

Files	Directories
Read Data	List Directory
Write Data	Add File
Append Data	Add Subdirectory
Execute	Traverse
	Read EA
	Write EA
	Delete Child
	Read Attributes
	Write Attributes
	Delete
	Read Control
	Write DAC
	Write Owner
	Synchronize
	Generic – All
	Generic – Execute
	Generic – Write
	Generic – Read

# DB2 Capability Architecture

---





# DB2 Plug-in dpk1

---

- Controls DB2 databases on Windows, Linux, and AIX
- Controls database-level authorities (database administrator, connect, etc.)
- Controls all privileges on
  - Schemas
  - Tables
  - Views
  - Columns
  - Indexes
  - Packages

**Slide 41**

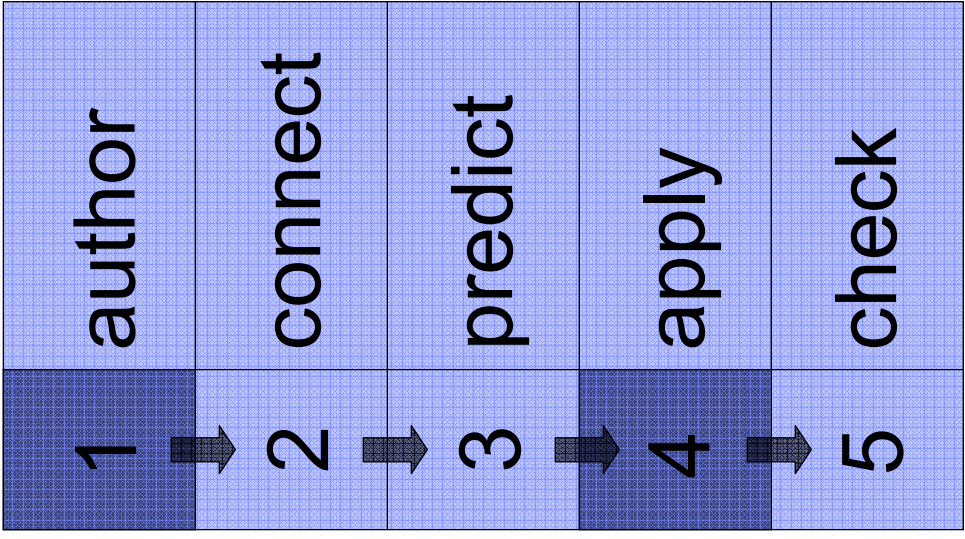
---

**dpk1**

**Remove Plug-in**  
Daniel Kolz, 9/25/2007

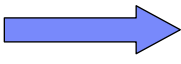
# Transformation from Abstract to Concrete Statements

---



## Statements

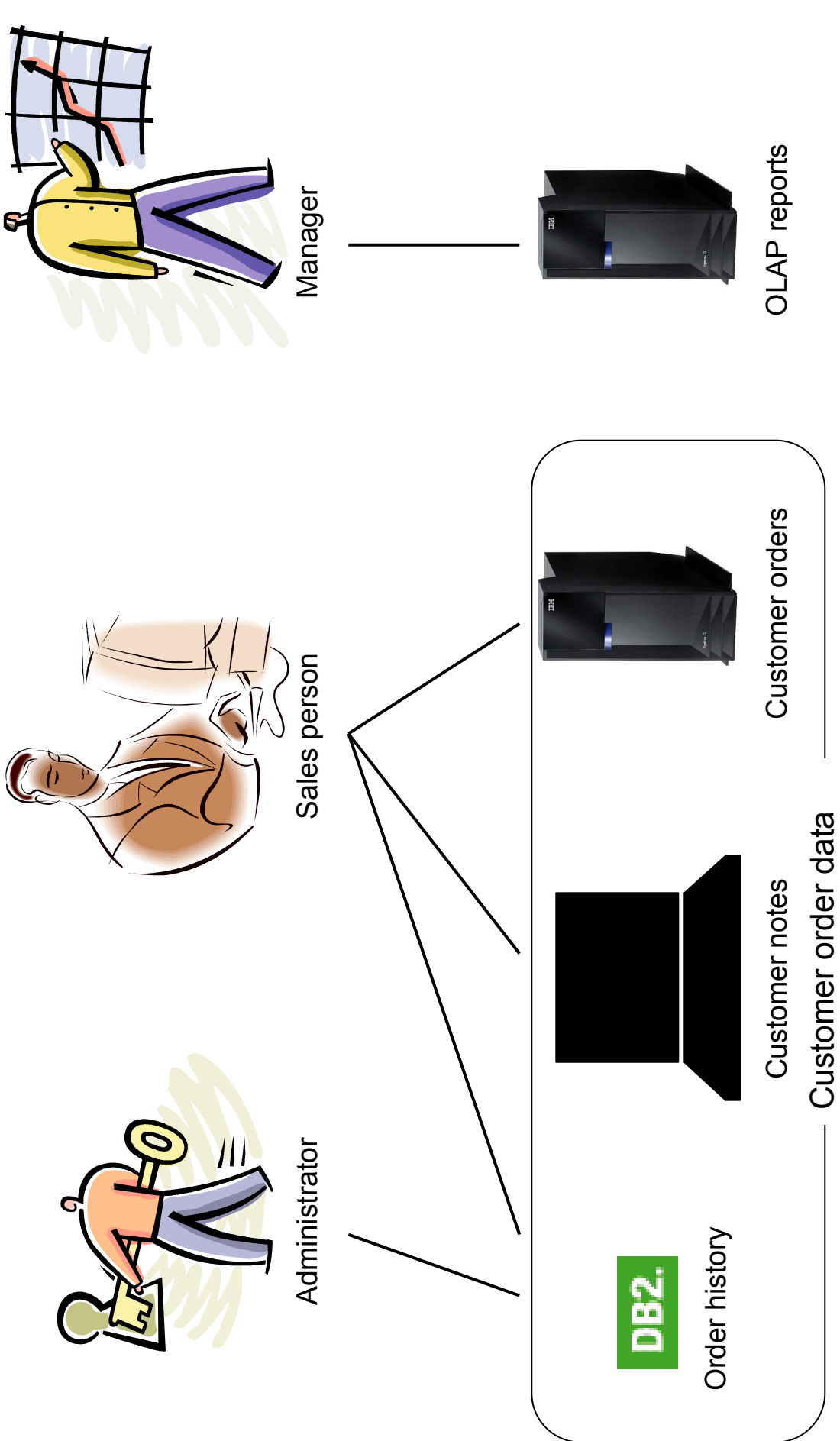
Accountants can change accounting data.



```
chmod dkolz +rw /data/ledger  
chmod sullivan +rw /data/ledger  
...
```

# Basic Use Scenario

---



# Sample Policy

---

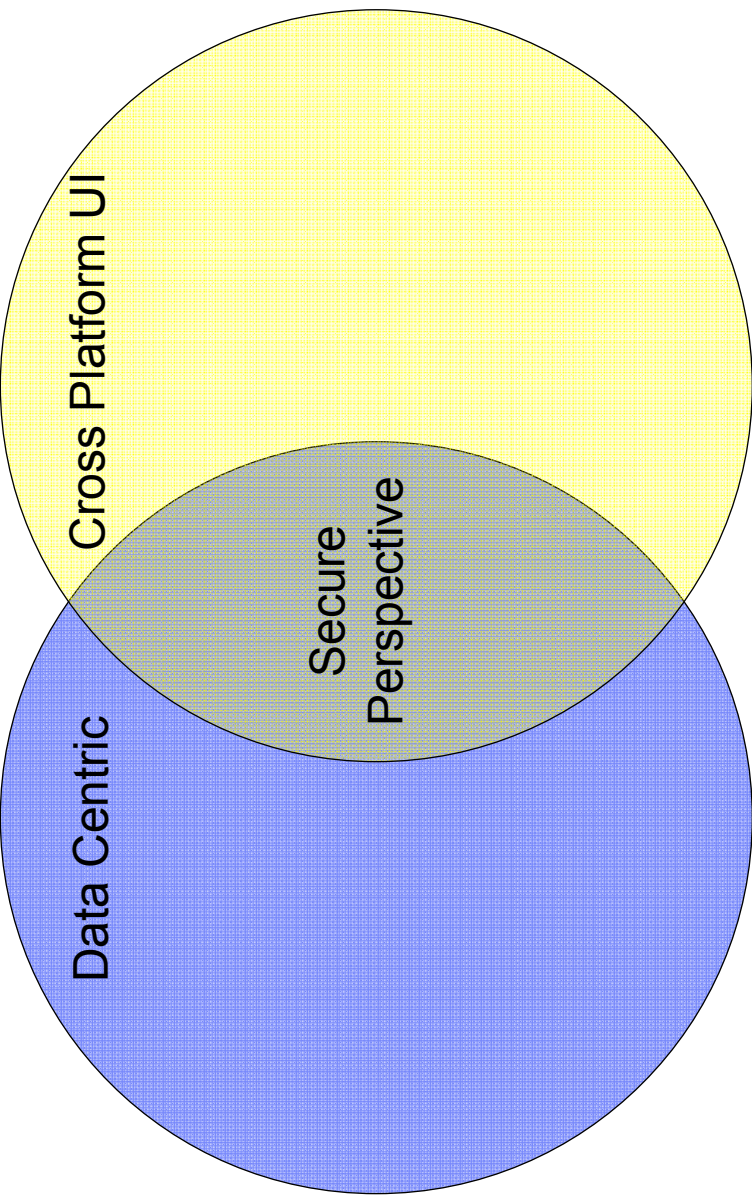
1. Sales people can change customer order data.
2. Managers can read OLAP reports.
3. Administrators can administrate customer order data.

---

- DEMO

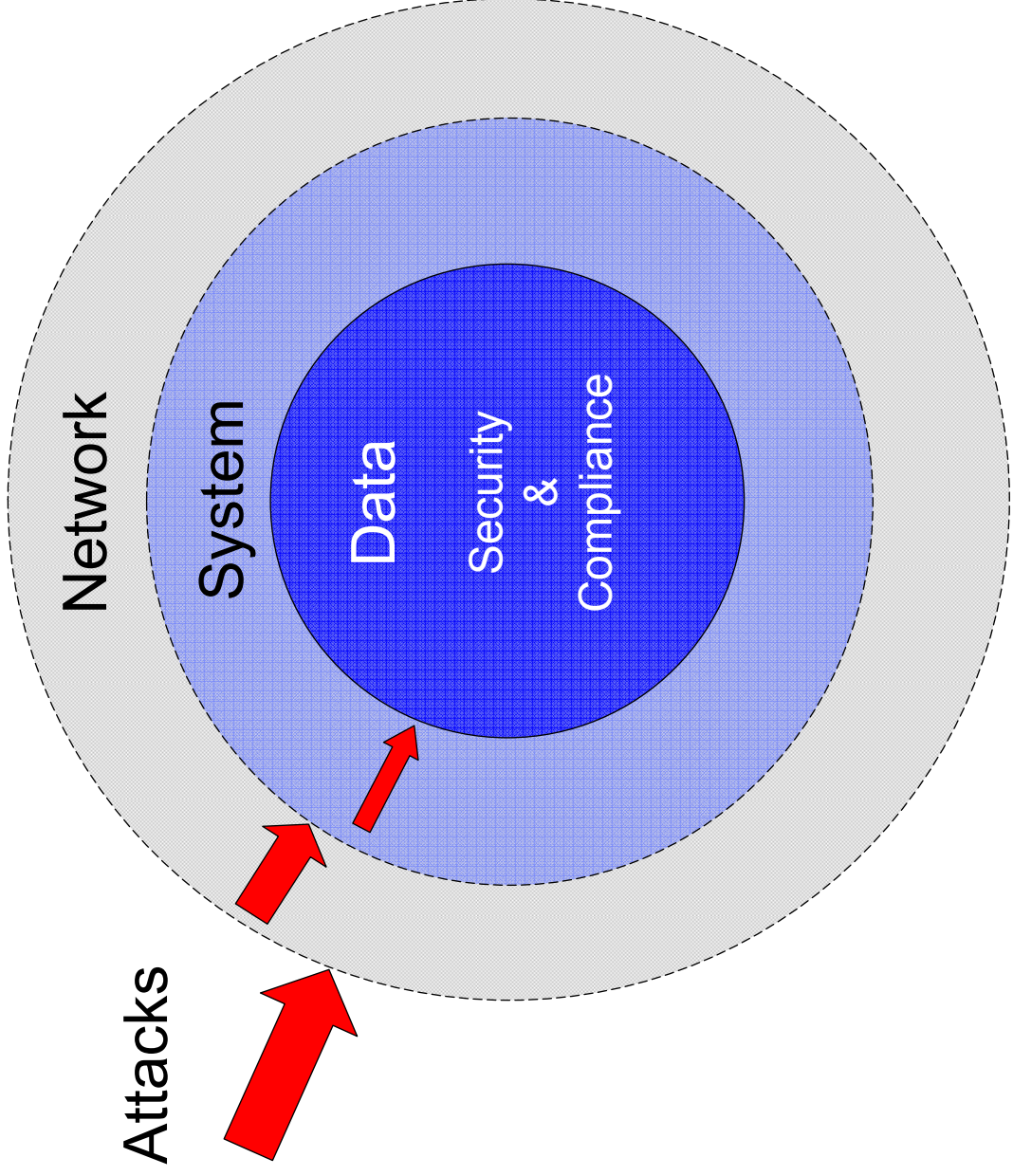
# Vision of Secure Perspective

---



# Data-Centric Model

---





# Data Centric Policy

---

- Resource Access Control (Released)
- Password Policy (Released)
- High Availability (Possible future work)
- Performance (Possible future work)
- Process (Possible future work)
- Backup Network (Possible future work)
- **Auditing (Possible future work)**
- **Encryption (Possible future work)**

# Cross Platform UI

---

- Platforms:
  - System i (Released)
  - DB2 (Coming soon)
  - AIX (Coming soon)
  - Windows (Coming soon)
  - RACF (Possible future work)
  - Linux (Possible future work)
  - Data Power (Possible future work)
- ONE user interface

# Ordering/pricing

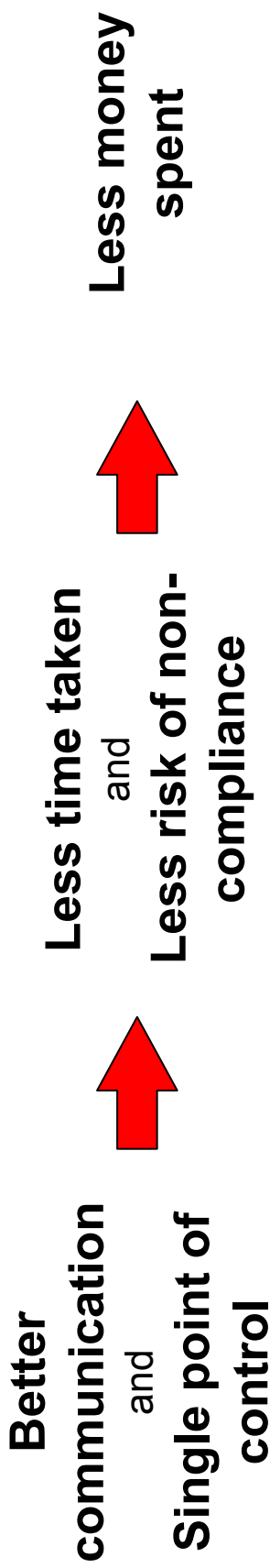
---

- Web application available for i5/OS and Windows
- \$1500/processor controlled
  - i5/OS
  - Windows
  - AIX
  - DB2

# Benefits

---

- Improved involvement in policy authoring from the business side of the house
- Accelerated deployment and checking of policy
- Reduced chance of problems (due to problem prediction)
- Consolidated point of control for many platforms/boxes

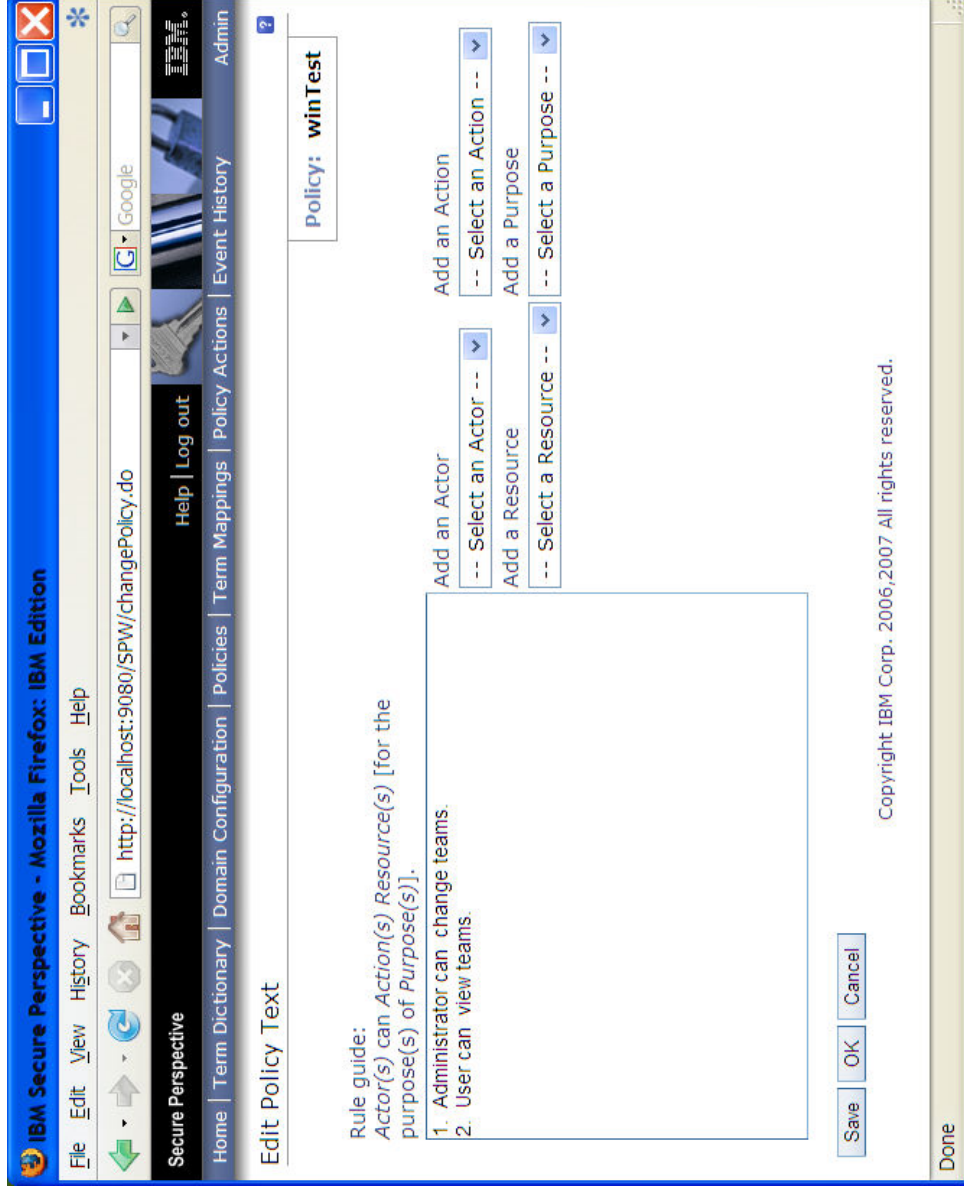




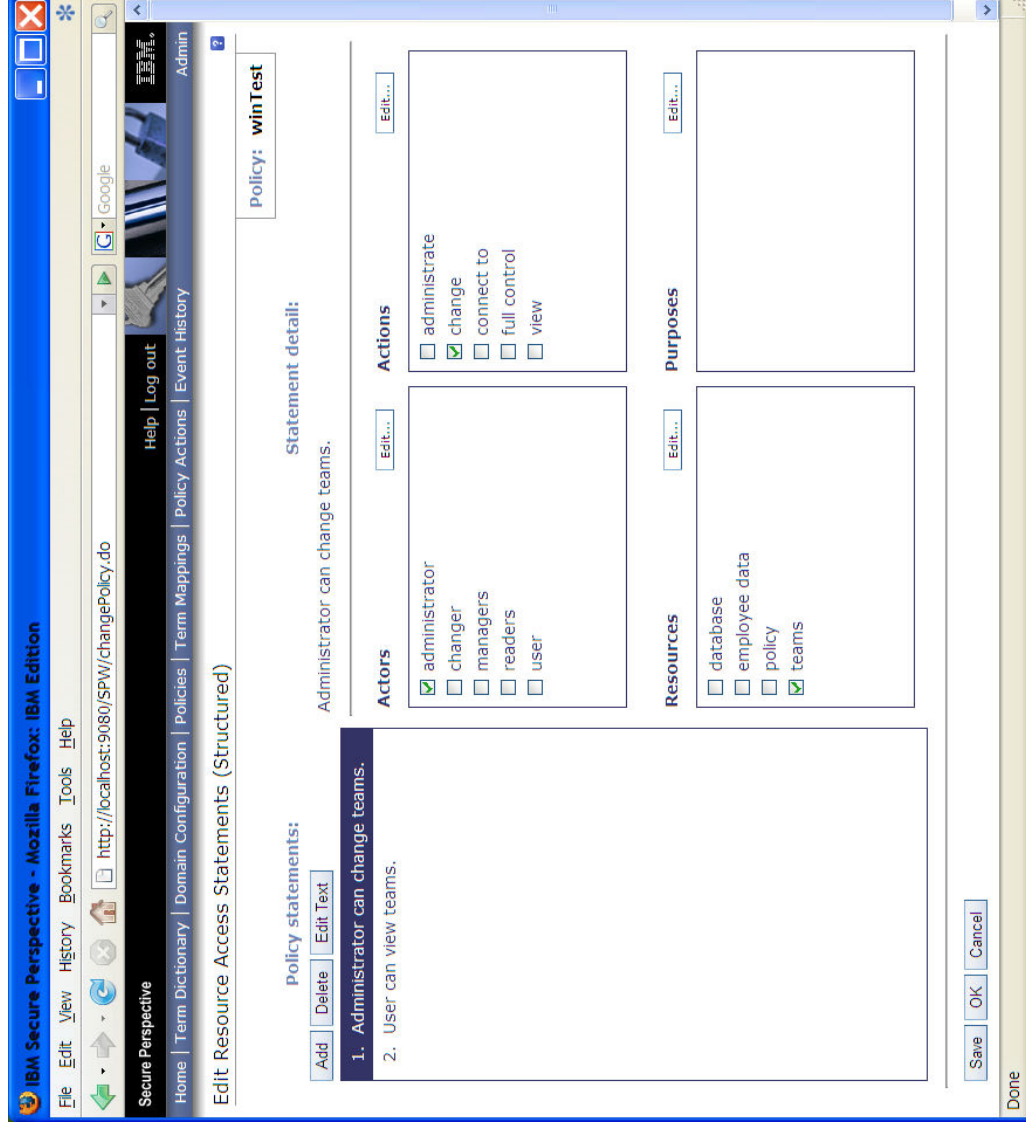
[http://www-03.ibm.com/systems/i/security/rethink\\_security\\_policy.html](http://www-03.ibm.com/systems/i/security/rethink_security_policy.html)

# Policy Authoring – Text Edit Mode

---

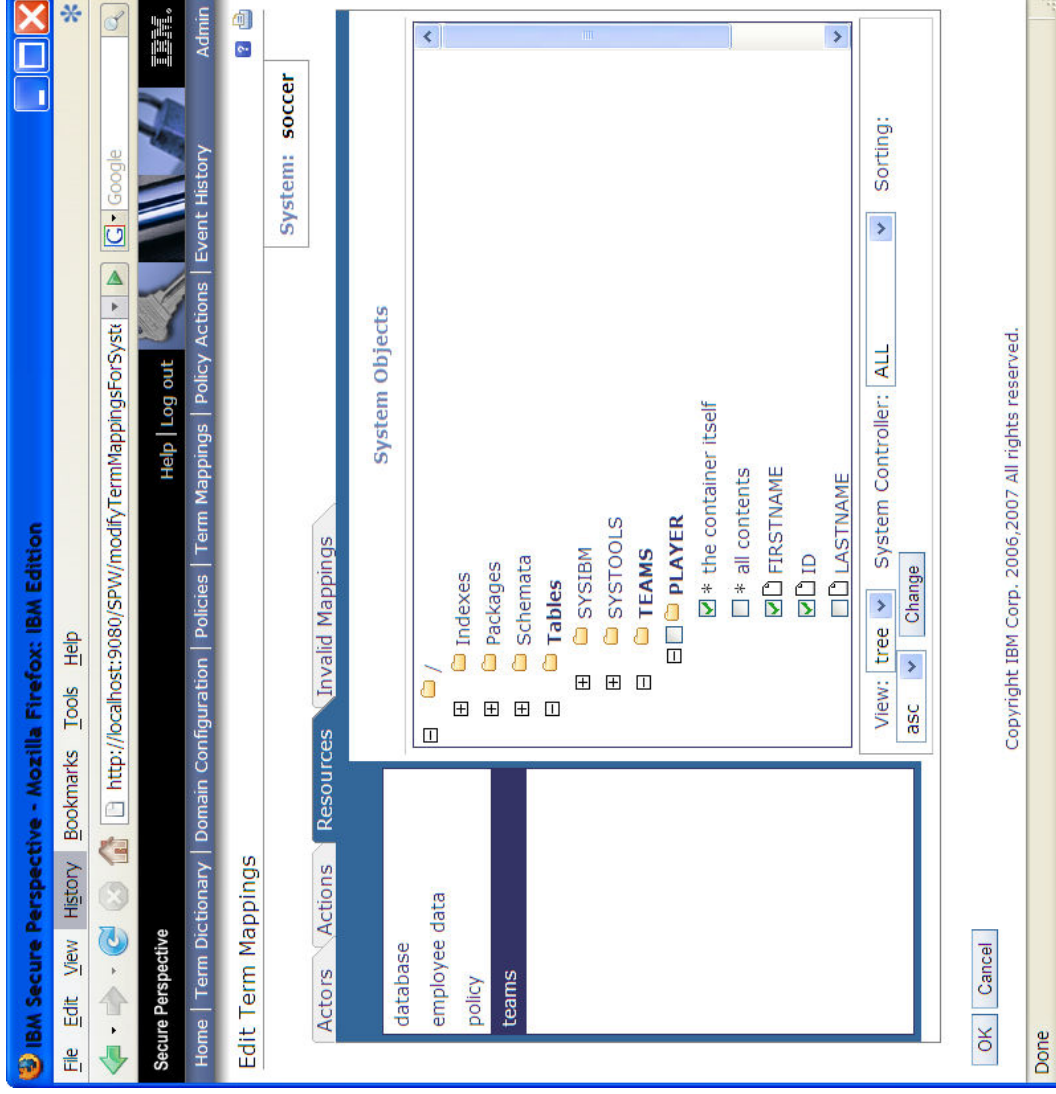


# Policy Authoring – Structured Edit Mode



[Authoring Statements](#)  
[Creating Statements](#)

# Mapping (Tree View)





# Mapping (List View)

