



Axel Buecker
Dinesh T. Jain
Aditya Joglekar
Nikhil Mayaskar

Identity Management for IBM Cognos 8 with IBM Tivoli Identity Manager

Introduction

This IBM® Redpaper™ publication describes how IBM Tivoli® Identity Manager can be used as a comprehensive identity management solution for IBM Cognos® 8. IBM Cognos 8 provides a security architecture that is flexible and compatible with existing security models. It can be integrated with authentication and cryptographic providers. Authentication in IBM Cognos 8 can be integrated with third-party authentication providers, such as IBM Tivoli Directory Server, Sun ONE Directory Server, Microsoft® Active Directory server, and so on. IBM Cognos 8 does not create or manage users as it is expected to be done by the authentication providers. On the other side, IBM Tivoli Identity Manager has excellent capabilities to do the job of identity management. Moreover, IBM Tivoli Identity Manager can provide an automated, policy-driven end-to-end user and group life cycle management solution for the Cognos infrastructure deployed in an organization. Leveraging IBM Tivoli Identity Manager for the identity management can deliver an ideal model working with Cognos security.

In this Redpaper, we provide technical illustrations, configurations, and design patterns for how Tivoli Identity Manager can be integrated with the Cognos 8 security model and its authentication provider (or providers), such as IBM Tivoli Directory Server.

This document is divided into several sections. For those readers who are not familiar with the IBM products covered in this paper, we provide a brief overview of Tivoli Identity Manager and IBM Cognos 8. We also provide a brief overview of how authentication and authorization is performed in Cognos 8. We cover the integration design patterns for Tivoli Identity Manager, IBM Cognos 8, and its authentication provider. We discuss the installation and configuration to implement the integration design. We then look deeper into the Tivoli Identity Manager features that can be leveraged to provide better security with Cognos 8. Finally, we document the conclusion for readers to extend this integration and provide links to various official documentation.

IBM Tivoli Identity Manager overview

IBM Tivoli Identity Manager provides a secure, automated and policy-based user life cycle management solution that can help effectively manage user accounts, access permissions, and passwords from creation to termination across the IT environment.

Tivoli Identity Manager can help you reduce the administrative costs and improve productivity through automation, user self-service, and other innovative capabilities for managing user accounts and access rights on various system resources. Figure 1 depicts the Tivoli Identity Manager system design.

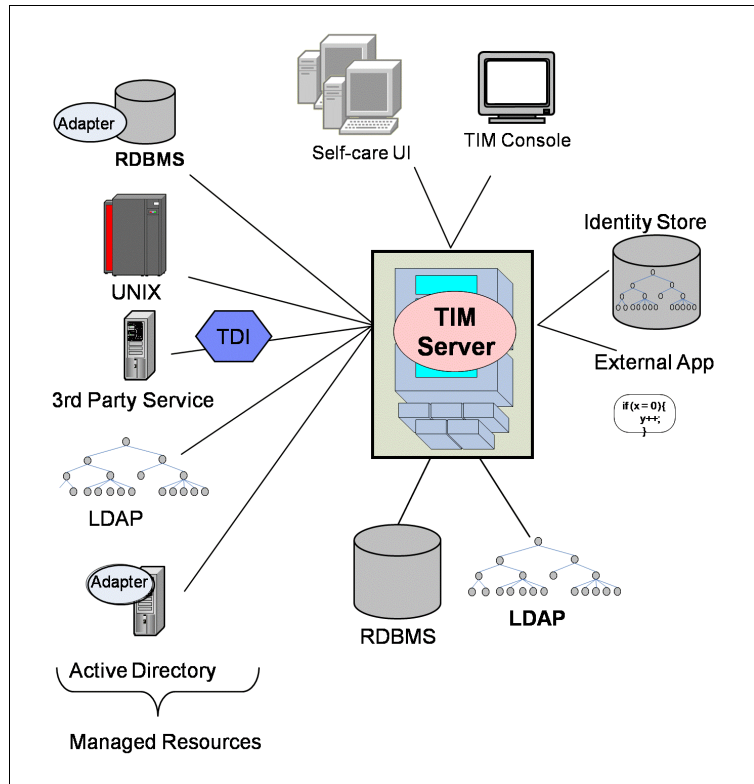


Figure 1 Tivoli Identity Manager (TIM) system design

We next look at several key components of the Tivoli Identity Manager architecture.

Tivoli Identity Manager server

Tivoli Identity Manager server provides core business logic and the provisioning platform for identity life cycle management. The Tivoli Identity Manager server contains information for various policies that determine how login IDs are created, how passwords are created, which users get access to various resources, which requests require use of approvals found in the workflow engine, and so on. The server is supported by the Lightweight Directory Access Protocol (LDAP) directory and database storage units

LDAP directory

The Tivoli Identity Manager system uses an LDAPv3 directory server as its primary repository for storing the current state of the enterprise it is managing. This state information includes the identities, accounts, roles, organization chart, policies, and workflow designs.

Database

A relational database is used to store all transactional, reporting, and schedule information. Typically, this information is temporary for the currently executing transactions, but there is also historical information that is stored indefinitely to provide an audit trail of all transactions that the system has executed.

Web-based user interface

Tivoli Identity Manager introduces a new dual-user interface that shows users only what they need to do their job. The interfaces are separate and users access them through separate Web addresses. Tivoli Identity Manager has two types of user interfaces, a self-care interface and an administrative console interface:

- ▶ Self-care user interface

This interface provides a simpler subset of personal tasks that apply only to the user.

- ▶ Administrative console user interface

This interface provides an advanced set of administrative tasks, and has new multitasking capabilities.

Managed resources and adapters

Any IT resource, such as operating system, database, file, directory, or mail server that Tivoli Identity Manager supports for user provisioning, is called a managed resource. Adapters serve as the links between the Tivoli Identity Manager server and the managed resources in an organization's computing system. An adapter is an interface that functions as a trusted virtual administrator, managing the user accounts on its assigned platform. Note that a separate adapter exists for each distinct type of managed resource supported by Tivoli Identity Manager. For a resource that is not supported by Tivoli Identity Manager, you may develop a custom adapter by using IBM Tivoli Directory Integrator technology.

See the IBM Redbooks® publication *Identity Management Design Guide with IBM Tivoli Identity Manager*, SG24-6996 and the IBM Tivoli Identity Manager 5.1 product documentation¹ to get more details about its architecture, components, and typical deployments.

IBM Cognos 8 overview

IBM Cognos 8 provides performance management and facilitates quick decision-making for business performance. It delivers the complete range of business intelligence (BI) capabilities including reporting, analysis, dashboards, and scorecards on a single, service-oriented architecture (SOA):

- ▶ Reporting

Reporting gives you access to a complete list of self-serve report types that are adaptable to any data source, and can operate from a single metadata layer for a variety of benefits such as multilingual reporting, ad hoc querying, and scheduling and bursting. You can author, share, and use reports that draw on data from all enterprise sources for better business decisions.

¹ The Tivoli Identity Manager Version 5.1 information center is located at:
<http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=/com.ibm.itim.doc/welcome.htm>

- ▶ **Analysis**
 Analysis enables the guided exploration of information that pertains to all dimensions of your business, regardless of where the data is stored. Analyze and report against online analytical processing (OLAP) and dimensionally aware relational sources.
- ▶ **Dashboards**
 Business dashboards communicate complex information quickly. They translate information from your various corporate systems and data into visually rich presentations using gauges, maps, charts, and other graphical elements to show multiple results together.
- ▶ **Scorecards**
 Scorecards help you align your teams and tactics with strategy, communicate goals consistently, and monitor performance against targets.

Figure 2 shows the IBM Cognos 8 product portfolio.

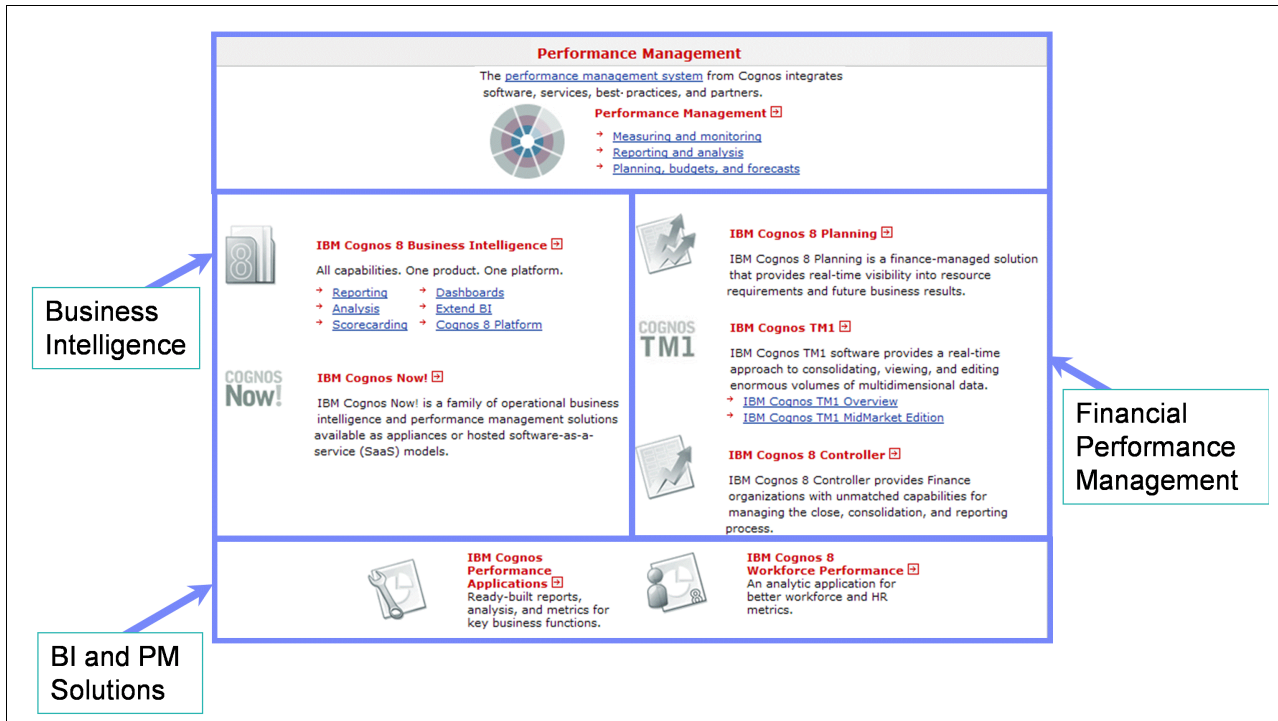


Figure 2 IBM Cognos portfolio

In addition to the BI capabilities, IBM Cognos 8 delivers a wide suite of financial performance management products. Several of these are:

- ▶ **IBM Cognos 8 Planning**
 This finance-managed solution provides real time visibility to the resource requirements and future business needs.
- ▶ **IBM Cognos TM1**
 This product provides a real-time approach to consolidating, viewing and editing enormous volumes of multidimensional data.

► IBM Cognos 8 Controller

This product provides finance organizations with unmatched capabilities for managing the closing, consolidation, and reporting process.

Figure 3 shows the IBM Cognos 8 Performance Management system.

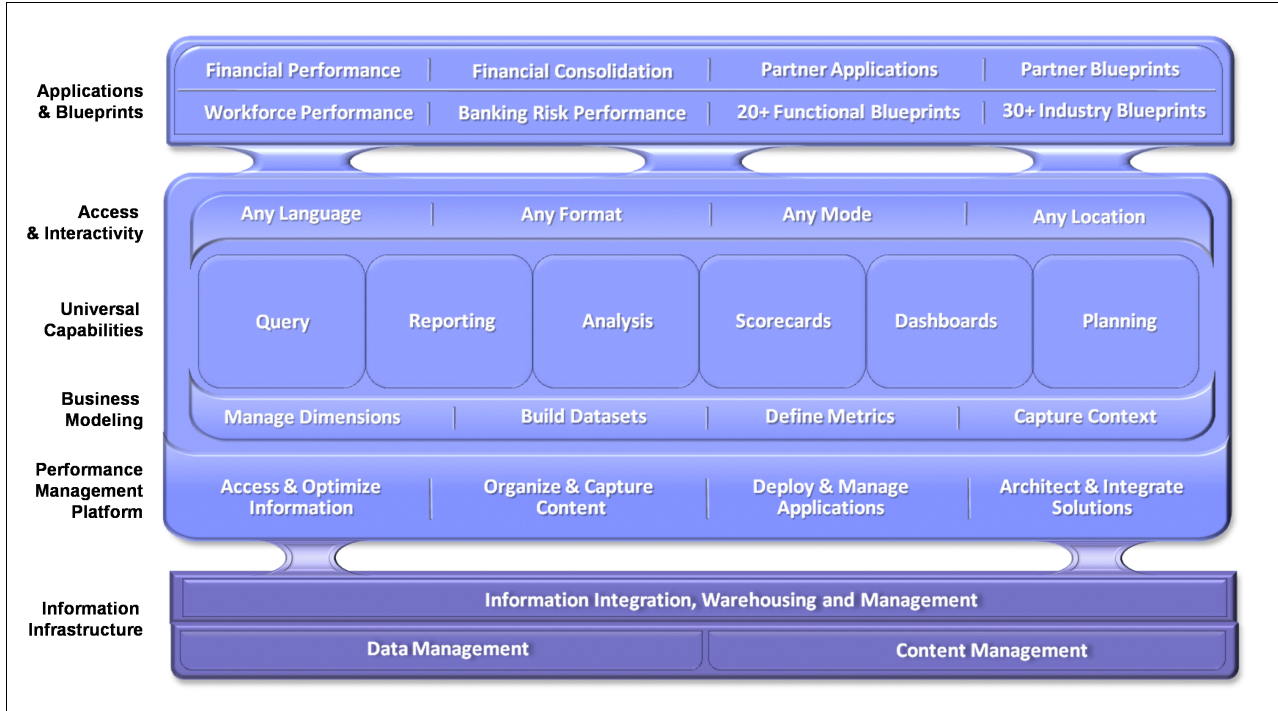


Figure 3 Cognos 8 Performance Management system

In short, IBM Cognos 8 can enable an organization to better understand and improve its business based on the following questions:

- How is the overall organization doing financially?
- Why is the situation the way it is?
- What can the organization do to improve?

See the IBM Cognos 8 product documentation² to learn more about the architecture and suite of products.

Cognos 8 authentication, authorization and access

IBM Cognos 8 does not authenticate users itself but rather relies on third-party authentication providers such as LDAP or Microsoft Active Directory to do so. This concept means that IBM Cognos 8 presents logon data (essentially credentials) entered by the user or obtained through single sign-on (SSO) mechanisms to the third-party authentication providers on behalf of the user. Then, when authenticated, IBM Cognos 8 must read the user's groups and roles from the authentication provider as well and make them available to the authorization functionality. This task is implemented by authentication providers.

² The IBM Cognos 8 v4 Business Intelligence information center is located at: <http://publib.boulder.ibm.com/infocenter/c8bi/v8r4m0/index.jsp>

After the users, groups, and roles are visible in the Cognos Connection, authorization policies can be created wherein a user can be assigned to a group or role depending on the business requirements.

The flow of an authentication request in Cognos 8

Let us look at a typical flow of an authentication request in Cognos 8, shown in Figure 4.

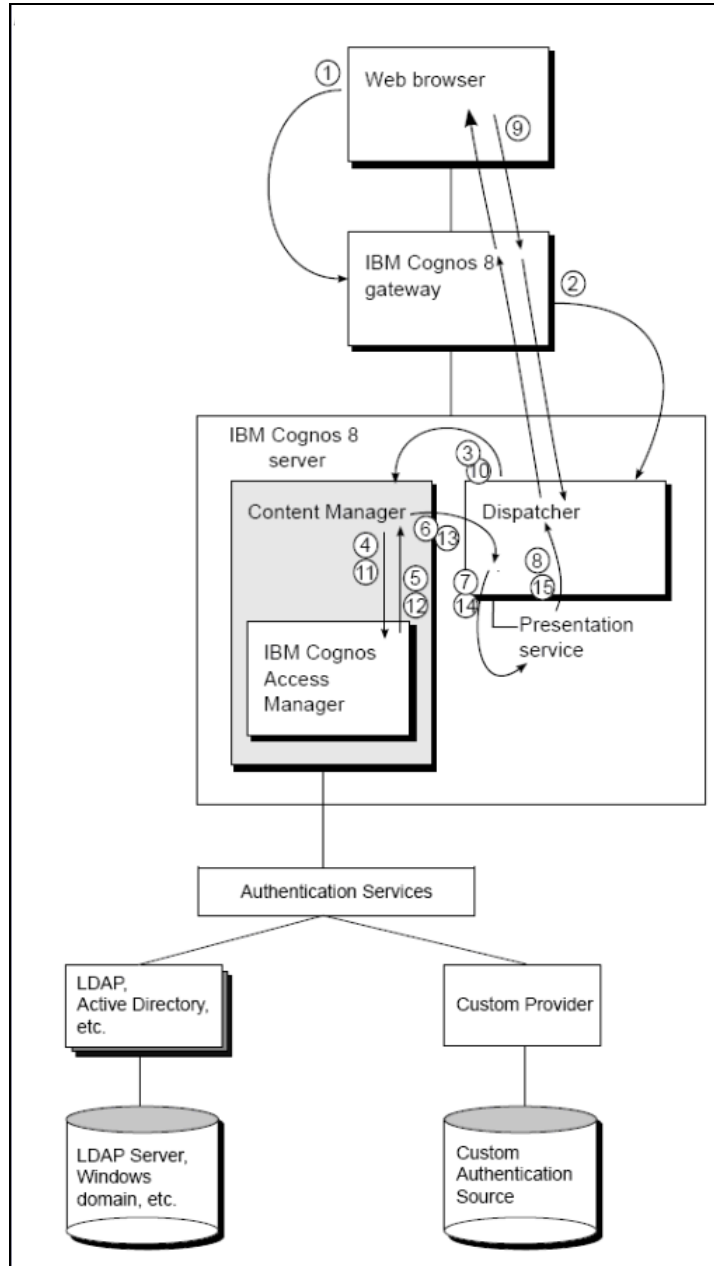


Figure 4 Flow of an authentication request in Cognos 8

When a user requests authenticated access to IBM Cognos 8, the flow is as follows:

1. The user clicks a report or analysis to view it, and the request goes through the gateway and the dispatcher to the presentation service.
2. The gateway accepts the request and sends it to a *dispatcher*.

3. The dispatcher notes that no *passport* is attached to the request, and sends the request to *Content Manager*.
4. Content Manager sends the request to *Access Manager*.
5. Anonymous access is disabled in this IBM Cognos 8 system, so Access Manager sends the request back to Content Manager with a fault attached. The fault contains information about what is needed to log on. For example, if multiple namespaces exist, the user will be required to select a *namespace*. If only one namespace exists, the user might be required to provide a user ID and password.
6. Content Manager returns the request with the attached fault to the dispatcher.
7. The dispatcher sends the request to the *presentation service*.
8. The presentation service creates the appropriate *logon page* for the user, and returns the page through the dispatcher and the gateway to the user.
9. The user enters the required information, such as a user ID and password. The information is attached to the original request and sent through the gateway to the dispatcher.
10. The dispatcher sends the request to Content Manager.
11. Content Manager sends the request to Access Manager.
12. Access Manager talks to the *authentication provider* through the *Authentication Service* to verify the supplied credentials. If all the required information is correct, Access Manager issues a *Passport ID*, attaches it in the HTTP header to the original request, and sends the request back to Content Manager. If the required information is incorrect or incomplete, the request faults back to step 9.
13. Content Manager sends the request to a dispatcher.
14. The dispatcher processes the request and sends it to the presentation service.
15. The presentation service sends the *Welcome page* back through the dispatcher and the gateway to the user.

Authorization and the CAMID

When a user is authenticated, the *passport* that is issued is the object that holds the *visas*. For each namespace, a visa is issued by the authentication provider after successful authentication has been established. In this case, the passport will hold a one-to-many numbers of visas. The Passport ID is the reference to the passport object, which is maintained, in memory, by the Content Manager component. The Passport ID is inserted in the *cam_passport cookie*, which is used to confirm that the user has successfully been authenticated in his or her current session before. Here, a user's identity is established, confirming access to the Cognos Portal content.

IBM Cognos 8 indicates which groups and roles the user is a member of, directly or indirectly, through inheritance (nested group memberships). This is true for groups and roles from the namespace for which the particular Passport ID has been issued, plus groups and roles from the Cognos namespace.

Authorization in IBM Cognos 8 applies to basically all objects that make up an IBM Cognos 8 application. All content (reports, analysis, folders, packages, and so on) and a wide range of functions and capabilities of systems can have permissions attached to them (for example, access to Studios). Permission defines *who*, a user, group or role, has *what* privileges on an object/capability/function.

The five privilege levels within IBM Cognos are:

- ▶ READ
- ▶ WRITE
- ▶ EXECUTE
- ▶ TRAVERSE
- ▶ SET POLICY

Internally, those privilege levels do not contain the names of users, groups, or roles, but instead contain an internal ID named *CAMID*³. The CAMID is constructed by the authentication provider for each object read in from an external authentication provider. This also applies to the internal authentication provider, so all the objects of the Cognos namespace have a CAMID assigned to them. By the user of this CAMID, IBM Cognos stores and verifies access to objects, when authorization is necessary. The CAMID of objects in the user's identity is compared to the permissions assigned to an object, and if they match, the privileges are granted or denied. Although the CAMID is built differently among authentication providers, they all use a common layout. The CAMID layout is a string, consisting of two fields that are concatenated:

```
CAMID:="CAMID(<NamespaceID>:<AuthProviderSpecificID>)"
```

The NamespaceID is the ID that is specified in Cognos configuration for the namespace. The AuthProviderSpecificID is an ID that is constructed internally by the authentication provider. Two examples are as follows:

- ▶ Example 1, User:

```
CAMID("LDAP:u:uid=admin,cn=admin,ou=support")
```

Where:

- LDAP is the NamespaceID
- uid=admin, is the user Relative Distinguished Name (RDN®)
- cn=admin, ou=support, is the Distinguished Name (DN)

- ▶ Example 2, Group:

```
CAMID("LDAP:g:cn=admin,ou=support")
```

Where:

- LDAP is the NamespaceID
- cn=admin, ou=support, is the Distinguished Name (DN)

Note: This ID is not officially documented because it is considered internal and subject to change without further notice. The layout documented here is current as of Cognos 8.4, however it might change in future versions without notice. Currently the AuthProviderSpecificID is composed from a type field, indicating the type of entry and some ID string. Type is one of: u for user, g for group, and f for folder. ID totally depends on the provider.

Leveraging Tivoli Identity Manager with Cognos 8

Cognos 8 supports various *authentication providers*, such as Microsoft Active Directory Server, LDAP, SAP, NT LAN Manager (NTLM), Cognos Series 7, and so on. These authentication providers store users, roles, and groups that can be used inside the Cognos environment while enabling the authentication mechanism. On the other side, the Tivoli Identity Manager supports most of such authentication providers as managed resources that

³ Cognos Access Manager ID

it can manage. Tivoli Identity Manager provides capabilities of provisioning users and groups on most of the managed resources that Cognos uses as authentication providers. The Microsoft Active Directory server, IBM Tivoli Directory Server, or Sun ONE Directory Server are examples of such authentication providers.

Leveraging Tivoli Identity Manager for managing users and groups on the authentication provider can deliver an ideal combination with the Cognos 8 security model. Further sections provide details about how Tivoli Identity Manager can be integrated with an authentication provider and leveraged with Cognos deployments.

Several key advantages for Cognos 8 when Tivoli Identity Manager is used with the Cognos authentication provider (or providers) are:

- ▶ Tivoli Identity Manager provides a centralized, policy-driven and automated end to end provisioning solution. Administrators can use the Tivoli Identity Manager Web-interface to manage users and groups on multiple authentication providers and performing administrative tasks on it rather than directly operating on the authentication providers' individual user interfaces.
- ▶ Tivoli Identity Manager allows provisioning policies that can be defined and customized as per the need. A provisioning policy can help to ensure an appropriate user getting provisioned with appropriate access rights.
- ▶ Approval workflows and e-mail notifications can be configured with all user provisioning activities, such as creating a user account on the authentication provider, user requesting an access to certain groups, and so on.
- ▶ Tivoli Identity Manager provides a self-care user interface that allows users to perform basic operations on their own without an administrator's involvement, such as resetting password, requesting access to groups, viewing and updating of personal information, and so on.
- ▶ Tivoli Identity Manager provides the ability to certify and validate a user's access to IT resources on a regular interval. An administrator can define a recertification policy that recertifies user accounts as well as access rights defined on the authentication provider.
- ▶ Auditing and reporting users and their access rights is one of the critical needs of most organizations. Tivoli Identity Manager's User and Access Reports can be leveraged to extend the existing Cognos auditing capabilities by providing auditing and reporting (traceability) of identity information of the authentication provider that accesses Cognos contents.
- ▶ Provisioning users on the authentication provider, based on the organizational roles that are defined in Tivoli Identity Manager (advanced scenario), can provide a role-based access control mechanism and the following benefits:
 - Role hierarchy helps to simplify and reduce the cost of user administration by enabling the use of an organizational role structure.
 - Separation of duties can strengthen security and compliance by creating, modifying, or deleting policies that exclude users from membership to multiple roles that may present a business conflict.

Integration architecture

In this section, we describe how Tivoli Identity Manager can be integrated with the Cognos 8 security model. An integration architecture diagram is shown in Figure 5 on page 10.

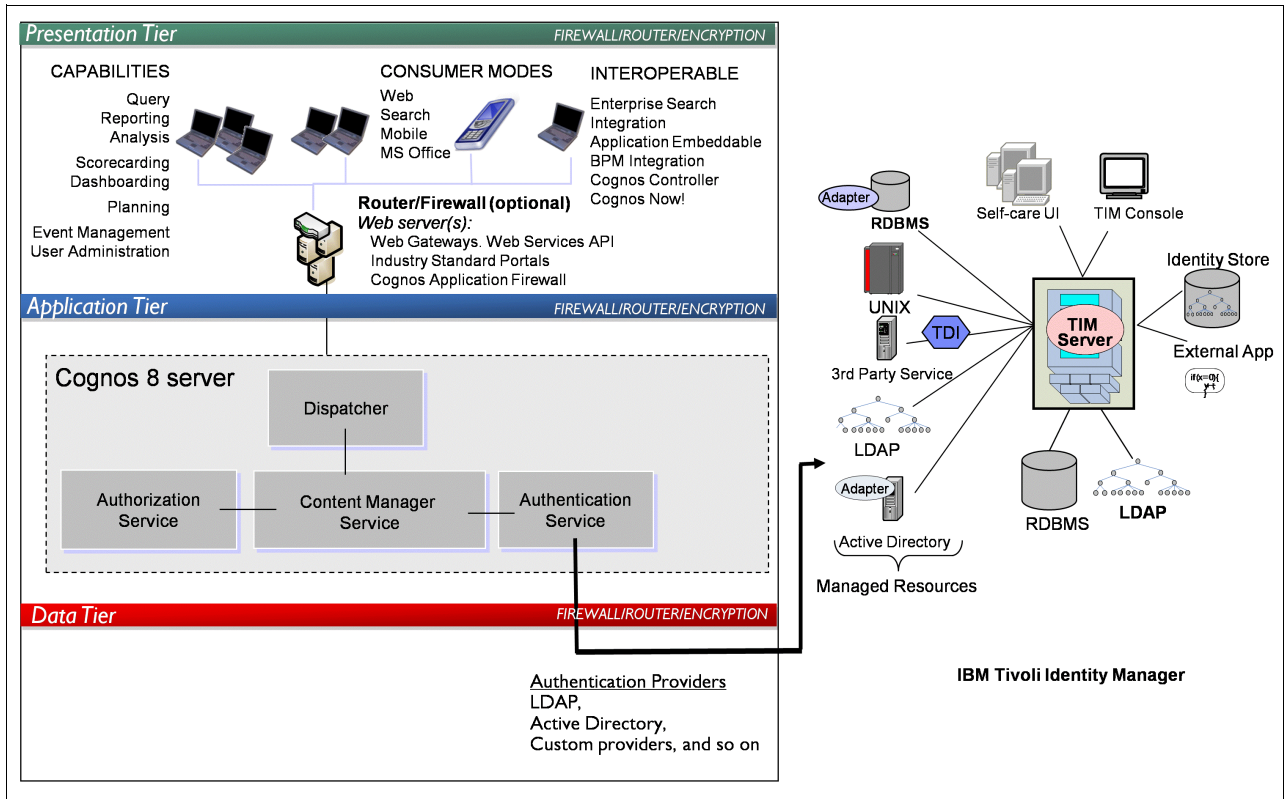


Figure 5 Integration architecture

As Figure 5 shows, Cognos 8 is enabled for one or more authentication providers. An authentication provider defines and maintains users, groups, and roles, and it also controls the authentication process. Each authentication provider known to IBM Cognos 8 is referred to as a namespace. User name, ID, password, regional settings, and personal preferences are several examples of information that is stored with the providers.

If authentication is set up for IBM Cognos 8, users must provide valid credentials, such as user ID and password, at login time. IBM Cognos 8 does not replicate the users, groups, and roles that are defined in the authentication provider. However, that information can be referenced in IBM Cognos 8 while setting up the access permissions to reports and other content. Users can also become members of Cognos groups and roles.

Tivoli Identity Manager manages users and groups on such authentication providers and can deliver an automated and policy-based user management solution throughout their life cycle. Tivoli Identity Manager provides centralized user access to disparate resources in an organization, using policies and features that streamline operations associated with user-resource access. In the following sections we provide more details about two sample approaches for utilizing Tivoli Identity Manager for managing the users from authentication providers.

Simple design approach

In this first design approach, we provide a simplified sample design of how Tivoli Identity Manager, an external authentication provider, and Cognos 8 security can be integrated together.

The approach discussed here does not use any of the default Cognos users or default Cognos groups. However, several of the existing built-in Cognos roles are used, rather than having to create new ones.

An important note is that this approach can be considered a *simple* approach because it does not involve defining roles in Tivoli Identity Manager.

The procedure is as follows:

1. Enable Cognos 8 security with an *authentication provider* configured for users and groups.
2. With Cognos 8, create Cognos groups, Cognos roles, or both, within the Cognos namespace to secure the content objects. Existing default Cognos roles can also be used rather than creating new ones.
3. Define an *HR feed* in Tivoli Identity Manager for creating *Person* entries along with their Tivoli Identity Manager accounts.
4. Configure Tivoli Identity Manager to manage the users and groups on the Cognos authentication provider by creating a *service* that supports the authentication provider as a *managed resource*.
5. Define or configure a *provisioning policy* in Tivoli Identity Manager that deals with the account creation on the managed resource (authentication provider for Cognos).
6. Optionally define an *adoption policy* in Tivoli Identity Manager that can associate user accounts from the authentication provider to their respective Person entries in Tivoli Identity Manager.
7. Define appropriate operations and policies on Tivoli Identity Manager as part of users and groups *provisioning*.
8. Perform user (accounts) and group management operations on the authentication provider from Tivoli Identity Manager.
9. In Cognos security, define *access permissions* and *capabilities* with Cognos groups and Cognos roles.
10. After objects are secured against the groups, roles, or both, in the Cognos namespace, add the authentication provider's groups and users to the appropriate Cognos groups and Cognos roles.

These steps are illustrated in n “Configuring the integration” on page 13, where we provide more practical insights about this approach.

Advanced design approach

In this second design approach, we provide an advanced sample on how Tivoli Identity Manager, an external authentication provider and Cognos 8 security can be integrated together. We use this approach to provide an overview of how *role based provisioning* can be performed with Tivoli Identity Manager.

Compared to “Simple design approach” on page 10, this approach defines roles in Tivoli Identity Manager and performs user account provisioning based on these roles. The users request access to Tivoli Identity Manager roles rather requesting access to the groups.

This approach does not use any of the default Cognos users or default Cognos groups. However, several of the existing default Cognos roles are used rather than creating new ones.

An important note is that roles defined in Cognos are different than roles defined in Tivoli Identity Manager. The procedure is as follows:

1. Enable Cognos 8 security with an *authentication provider* configured for users and groups.
2. With Cognos 8, create Cognos groups, Cognos roles, or both within the Cognos namespace to secure the content objects. Existing default Cognos roles can also be used rather than creating new ones.
3. Configure Tivoli Identity Manager to manage the users and groups on the Cognos authentication provider by creating a *service* that supports the authentication provider as a *managed resource*.
4. Using Tivoli Identity Manager, create groups on the authentication provider or run the *reconciliation operation* to import existing groups into the Tivoli Identity Manager repository.
5. Define *static roles* in Tivoli Identity Manager. For each group that exists in the authentication provider, ensure that at least one role is defined. As an example, for the *Authors* group that is created in the external authentication provider, create a static role *Authors* in Tivoli Identity Manager. Also ensure that *Common Access* is enabled for each of the role.
6. Define or configure *provisioning policies* in Tivoli Identity Manager that deal with account creation on the managed resource (authentication provider for Cognos). Ensure that for each role, a provisioning policy is created and that it also defines group membership parameters as part of its entitlements.

Perform the following steps with each of the provisioning policies to be created:

- a. Ensure that the policy has the *Membership Type* parameter selected as *Roles specified below*.
 - b. Select the appropriate role name that you created earlier. For example, in the case of the provisioning policy for the *Authors* role, ensure that *Authors* role is selected as the policy member.
 - c. With the *Entitlements* configuration, ensure that you have selected the group name as a parameter with the constant value selected as the group name from the authentication provider.
7. Define an *HR feed* in Tivoli Identity Manager for creating *Person* entries and their Tivoli Identity Manager *accounts*. Ensure that each user has at least a role associated with it.
 8. Optionally, define an *adoption policy* in Tivoli Identity Manager that can associate user accounts from the authentication provider to their respective *Person* entries in Tivoli Identity Manager.
 9. Define the appropriate operations and policies in Tivoli Identity Manager as part of user and group provisioning.
 10. Perform user (accounts) and group management operations on the authentication provider from Tivoli Identity Manager.
 11. In Cognos security, define *access permissions* and *capabilities* with Cognos groups and Cognos roles.
 12. After objects are secured against the groups, roles, or groups and roles, in the Cognos namespace, add the authentication provider's groups and users to the appropriate Cognos groups and Cognos roles.

Note that the advanced approach provided in this section is not discussed further in this paper. This approach is described here only to provide some direction toward how you can use role-based provisioning with IBM Tivoli Identity Manager.

Configuring the integration

In this section, we illustrate the design implementation of the approach listed in “Simple design approach” on page 10.

We show how Tivoli Identity Manager can be configured with an authentication provider that Cognos 8 uses for the authentication purposes. We illustrate various Tivoli Identity Manager features that can be used to manage users and groups for Cognos 8.

Our authentication provider is the IBM Tivoli Directory Server, and we refer to it as the LDAP server in this scenario. Users and groups are created on the LDAP server by using Tivoli Identity Manager. These users will access the Cognos 8 content. Several of the default Cognos roles are used in this integration scenario rather than creating new ones.

Prerequisites

Before configuring this integration scenario, an important task is to evaluate whether the authentication provider is supported by Cognos 8 as well as Tivoli Identity Manager. Before you configure the integration, see the respective product's support documentation.

Ensure that the following prerequisite software is installed and running properly:

- ▶ IBM Tivoli Identity Manager 5.1 is installed with the LDAP adapter service.
- ▶ IBM Cognos 8.4 is installed with sample content, that is, imported sample reports and packages in the public folder for the purpose of demonstrating the authorization and access process.
- ▶ IBM Tivoli Directory Server 6.2 is installed and configured with the suffix O=IBM,C=US. This LDAP server is used as an authentication provider with Cognos 8 security.

Configuration with Cognos security

The provider we demonstrate here is a full authentication provider that implements all the functionality required by Cognos 8 to communicate with an authentication provider, including:

- ▶ User authentication using external authentication providers
- ▶ Namespace searches

The searches can retrieve namespace objects and their properties, as required by IBM Cognos 8. The objects can be users, groups, and roles, which are then used for authorization purposes in the IBM Cognos namespace.

- ▶ Trusted Credentials Management
- ▶ Authentication provider configuration

Perform the following steps to configure Tivoli Directory Server as an authentication provider with Cognos 8:

1. Navigate to the **IBM Cognos Configuration** → **Security** → **Authentication** folder.
2. In the folder, right-click and select **Namespace resource** to add a new namespace resource to the Authentication folder.
3. Give the namespace a name such as TDS-LDAP and select a type of **LDAP** from the Type menu. Click **OK**.
4. Enter the required parameters, such as *server info*, and so on.

- Finally, test whether the namespace is properly configured by right-clicking on the newly created namespace and selecting **Test**.

The fully configured TDS-LDAP namespace is shown in Figure 6.

TDS-LDAP - Namespace - Resource Properties	
Name	Value
Type	LDAP
* Namespace ID	IBM
* Host and port	9.122.127.58:389
* Base Distinguished Name	O=IBM,C=US
User lookup	(cn=\${userID})
Use external identity?	False
External identity mapping	\${environment("REMOTE_USER")}
Bind user DN and password	*****
Size limit	-1
Time out in seconds	-1
Use bind credentials for search?	True
Allow empty password?	False
Unique identifier	cn
Data encoding	UTF-8
SSL certificate database	
Advanced properties	<click the edit button>
Folder mappings (Advanced)	
Object class	organization
Description	description
Name	o
Group mappings (Advanced)	
Object class	groupofnames
Description	
Member	member
Name	cn
Account mappings (Advanced)	
Account object class	organizationalperson
Business phone	telephonenumber
Content locale	preferredlanguage
Description	description
Email	mail
Fax/Phone	facsimiletelephonenumber
Given name	givenname
Home phone	homephone
Mobile phone	mobile
Name	cn
Pager phone	pager
Password	userPassword
Postal address	postaladdress
Product locale	preferredlanguage
Surname	sn
User name	cn
Custom properties	<click the edit button>

Figure 6 LDAP namespace configuration

6. Set the *Allow anonymous access* field under **Security** → **Authentication** → **Cognos** to **False** to enable the Cognos Connection to prompt for a namespace selection and login credentials, as shown in Figure 7.

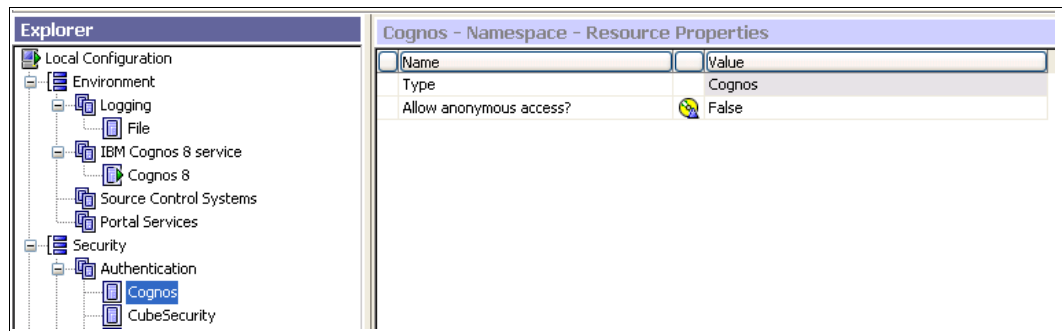


Figure 7 Disable anonymous access

Configuring Tivoli Identity Manager

In the following sections, we take you through the configuration for Tivoli Identity Manager.

- ▶ Define a service for the Cognos authentication provider
- ▶ Configuring a provisioning policy
- ▶ Defining approval workflows
- ▶ Defining the HR feed

Define a service for the Cognos authentication provider

In this section, we define a service in Tivoli Identity Manager for managing users and groups on the Cognos authentication provider, in our case the IBM Tivoli Directory Server.

Perform the following steps to define a service:

1. With Tivoli Identity Manager for managing the Cognos authentication provider as a managed resource, ensure that the respective service profile and the adapter are installed and configured properly. When IBM Tivoli Directory Server is a managed resource for Tivoli Identity Manager, ensure that the LDAP profile is present in the Tivoli Identity Manager server, and that the LDAP adapter (a Tivoli Directory Integrator based RMI adapter) is installed and running. See the adapter documentation for installation and configuration.
2. Log on to the Tivoli Identity Manager administrative console, for creating an LDAP service type.
3. From the Manage Services panel click the **Create** button to create an LDAP service to manage users and groups from Tivoli Directory Server.
4. Using the Service creation wizard, specify the required parameters, such as LDAP server location, administrator name, password, and so on.
5. With the LDAP service created (in step 4), ensure that the “Users and Groups” configuration is specified properly. This configuration should match the details provided with the authentication provider details from Cognos 8 security. Figure 8 on page 16 shows the Users and Groups configuration dialog with the appropriate LDAP service details.

Figure 8 Creating the LDAP service, Users and Groups configuration

6. Click **Test Connection** and make sure that the test is successful with the LDAP server details provided.
7. Click **Finish** to create the LDAP service.

An important note is that the group member user entry, specified in the Initial group member parameter, must exist with the LDAP server before accessing the Cognos contents after its security is enabled. This user can be created in the LDAP server using Tivoli Identity Manager as mentioned in “Creating LDAP accounts” on page 21.

Configuring a provisioning policy

As a result of the LDAP service creation, a provisioning policy is created automatically with certain default settings. Perform the following steps for correctly configuring this provisioning policy to provision LDAP accounts properly:

1. Log onto the Tivoli Identity Manager administrative console for updating the default provisioning policy created for LDAP service.
2. In the Manage Provisioning Policies panel click the **Search** button.
3. Click on the provisioning policy **Default Provisioning Policy for service LDAP Service**.
4. When the provisioning policy details wizard dialog opens, go to the Entitlements page.
5. Select the **LDAP Service** check box and click **Parameters**.
6. In the Entitlement Parameter page, click the **Create** button. Select the **Last name** attribute and click **Continue**. Repeat this step, using the attributes **Full name** and **User ID**. For each of these attributes, we assign the Parameter Type as JavaScript and Enforcement Type as Default. Specify the Value parameter for each of the attributes with the JavaScript code as shown in Figure 9 on page 17.

Manage Policies > Manage Provisioning Policies > Entitlement Parameter

Select one or more provisioning parameters that you want to change and click Change, or select Create to view a list to add a new attribute. To remove an attribute, select the attribute, and then click Delete.

<input type="checkbox"/> Select ^	Name ^	Template value ^	Enforcement... ^	Value Type ^
<input type="checkbox"/>	Last name	subject.getProperty("sn")[0];	Default	JavaScript
<input type="checkbox"/>	Full name	subject.getProperty("sn")[0];	Default	JavaScript
<input type="checkbox"/>	User ID	subject.getProperty("uid")[0];	Default	JavaScript

Page 1 of 1 Total: 3 Displayed: 3 Selected: 0

Figure 9 Provisioning policy configuration

7. Click **Continue** after all the parameters are created.
8. Click **Submit** to save the provisioning policy configuration changes.

Defining approval workflows

A workflow defines a sequence of activities that represent a business process. You can use Tivoli Identity Manager workflows to customize account and access provisioning, and life cycle management. For example, you can add approvals and information requests to account or access provisioning processes. See the Tivoli Identity Manager online documentation⁴ to learn more about workflows.

In this integration scenario, we define an *access request approval workflow*. When an existing Tivoli Identity Manager user (who has an LDAP account) requests access to certain groups in LDAP, an approval notification is sent to the workflow participant. If the request is approved, the user becomes a member of that LDAP group. If the workflow participant does not act on the request within a specified interval, the request is escalated to the Tivoli Identity Manager administrator for approval.

Perform the following steps to define the access request approval workflow:

1. Log on to the Tivoli Identity Manager administrative console.
2. Navigate to the **Manage Workflows** → **Design Access Request Workflows** panel, and click the **Create** button.
3. On the General tab, specify the Name for the workflow as Access Request Workflow for LDAP service.
4. Select the Service type as LDAP profile.
5. On the Activities tab, click the **Go** button that is associated with the “Create an approval activity” box. The Approval Activity dialog opens.
6. Specify a name for the “Activity name” parameter.
7. Specify Approver type as **Specified user**.
8. Choose the User name as one the existing users, for example, Betty Roberts; use the **Search** button.
9. Ensure that approval activity details are as shown in Figure 10 on page 18.

⁴ A good place to start learning more about workflows is at the following location:
http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.itim.doc/cpt/cpt_ic_wkflo_planning.html

Design Workflows > Manage Access Request Workflows > Approval Activity

Specify the activity name and escalation time for this approval activity, and specify the approver and escalation

*Activity name
Approval Activity

Approver type
Specified user

*User name
Betty Roberts Search...

Escalation time in days
1

Escalation participant type
Administrator

OK Cancel

Figure 10 Approval Activity

10. Click **OK** to continue.
11. Click the **OK** button one more time to complete the access request approval workflow configuration.

Defining the HR feed

As administrator, you must perform a number of initial steps to seed employee data from one or more human resources (HR) repositories and populate the Tivoli Identity Manager registry with an equivalent set of users. Tivoli Identity Manager allows you to add a number of users to the system by reading a data source, such as a user repository, directory, file, or custom source. The process of adding users based on a user data repository is called an *identity feed*, or *HR feed*. You need to anticipate the effect of missing information in the user record. For example, if the record that you feed into Tivoli Identity Manager has no e-mail address for the user, the user will not be able to receive a password for a new account in an e-mail, and must call the help desk, or contact the manager. You can use several source formats to load identity records into the Tivoli Identity Manager user registry.

Tivoli Identity Manager supplies the following service types to handle several of the most common sources for identity feeds:

- ▶ Comma-separated value (CSV) identity feed
- ▶ DSML identity feed
- ▶ AD OrganizationalPerson identity feed (Microsoft Windows® Active Directory)
- ▶ iNetOrgPerson (LDAP) identity feed
- ▶ IDI data feed (based on Tivoli Directory Integrator)

You can populate initial content and subsequent changes to the content of the people registry from these sources. As an example, we use a CSV identity feed to populate the Tivoli Identity Manager registry.

In Example 1 we display sample HR feed input data (`sample.csv`) that is used with our integration scenario.

Example 1 HR feed sample CSV file content (sample.csv)

```
uid,sn,cn,givenname,mail
bstintson,Stintson,Barney,Barney Stintson,bstintson@tuvwxyz.com
brobberts,Roberts,Betty,Betty Roberts,brobberts@tuvwxyz.com
djain,jain,Dinesh,Dinesh jain,djain@tuvwxyz.com
hspellman,Spellman,Hilda,Hilda Spellman,hspellman@tuvwxyz.com
jroddick,Roddick,James,James Roddick,jroddick@tuvwxyz.com
jsmith,Smith,James,James Smith,jsmith@tuvwxyz.com
nkapoor,Kapoor,Neeta,Neeta Kapoor,nkapoor@tuvwxyz.com
nmayaskar,Mayaskar,Nikhil,Nikhil Mayaskar,nmayaskar@tuvwxyz.com
rverma,Verma,Rhea,Rhea Verma,rverma@tuvwxyz.com
```

Perform the following steps to populate the Tivoli Identity Manager registry with Person data.

1. Copy the file `sample.csv` to the machine where your Tivoli Identity Manager server is installed.
2. Log on to the Tivoli Identity Manager administrative console to create a service of type *CSV Identity Feed*.
3. In the Manage Services panel, click **Create** and select the service type as **CSV Identity Feed**.
4. Specify the complete file path for `sample.csv` file.
5. Select the **Use workflow** option.
6. Click **Test Connection** and ensure that the operation returns success.
7. Click **Finish** to save the service profile and return back to the Manage Services panel.
8. From the newly created service's context menu, select the **Reconcile Now** option.

Performing the above steps successfully shows the Person entries that are created in Tivoli Identity Manager, and located under the Manage Users panel (Figure 11 on page 20).

Manage Users

Manage Users > Select a User

To locate a user that you want to manage, type information about the user in the field, select a filter, and then click Search. The match your criteria are displayed in the table below. By default, clicking Search will search the system based on the beginning letter of the item you are searching for. To search for a textual pattern in the middle of an item, use the "*" symbol on the keyboard to indicate a wildcard. (For example, typing "b*" will find "abc".)

Search information: Search by: Last Name [v] [Search] [Advanced...]

Users

To perform a particular task for a user, click the icon next to the name of the user, and then select the task that you want to perform.

10 results found for: *

Include accounts when suspending, restoring, or deleting users

<input type="button" value="Create"/> <input type="button" value="Change"/> <input type="button" value="Delete"/> <input type="button" value="Suspend"/> <input type="button" value="Restore"/> <input type="button" value="Transfer"/> <input type="button" value="Refresh"/>						
<input type="checkbox"/> Select	Name	E-mail Ad...	Last Name	Business ...	Status	
<input type="checkbox"/>	Barney	bstintson@xy...	Stintson	IBM Corporation	Active	
<input type="checkbox"/>	Betty	brobberts@xy...	Roberts	IBM Corporation	Active	
<input type="checkbox"/>	Dinesh	djain@xyz.com	jain	IBM Corporation	Active	
<input type="checkbox"/>	Hilda	hspellman@x...	Spellman	IBM Corporation	Active	
<input type="checkbox"/>	James	jsmith@xyz.c...	Smith	IBM Corporation	Active	
<input type="checkbox"/>	James	jroddick@xyz...	Roddick	IBM Corporation	Active	
<input type="checkbox"/>	Neeta	nkapoor@xyz...	Kapoor	IBM Corporation	Active	
<input type="checkbox"/>	Nikhil	nmayaskar@x...	Mayaskar	IBM Corporation	Active	
<input type="checkbox"/>	Rhea	rverma@xyz.c...	Verma	IBM Corporation	Active	
<input type="checkbox"/>	System Administrator		Administrator	IBM Corporation	Active	

Page 1 of 1 Total: 10 Displayed: 10 Selected: 0

Figure 11 Manage Users: Successful import from a CSV file

By default, a Tivoli Identity Manager account is generated for each person that is created in Tivoli Identity Manager. In the above example, each person receives an e-mail notification about their Tivoli Identity Manager account and password.

The following sections use several accounts that we have already created.

Identity management for Cognos using Tivoli Identity Manager

In the previous sections, we configured Cognos 8 with an authentication provider. Then, we created a new service in Tivoli Identity Manager to recognize the Authentication Provider as a managed resource. In this section, we illustrate how Tivoli identity Manager can be leveraged as an identity management solution for managing users and groups on the authentication provider that can enable better security within the Cognos infrastructure.

Managing authentication provider's users and groups

After Tivoli Identity Manager is populated with users (Persons having their Tivoli Identity Manager accounts) and a managed resource like LDAP, we can request new LDAP accounts for these users. Tivoli Identity Manager also provides capabilities of managing groups on an LDAP server.

Tivoli Identity Manager, in combination with the LDAP Adapter, can be used to automate the following administrative tasks:

- ▶ Creating new users (LDAP accounts) on the directory server
- ▶ Modifying user attributes on the directory server
- ▶ Changing user account passwords on the directory server
- ▶ Suspending, restoring, and deleting user accounts on the directory server
- ▶ Reconciling user accounts and groups on the directory server
- ▶ Creating, modifying, and deleting groups on the directory server

If users and groups already exist on your LDAP server, a reconciliation operation can be performed on the LDAP service configured with Tivoli Identity Manager. See the online documentation⁵ to learn more about the *reconciliation operation* and *adoption policies*.

Creating LDAP accounts

In this section, we create LDAP accounts for the Tivoli Identity Manager users (Persons) that were created during the HR feed operation in “Defining the HR feed” on page 18.

Perform the following steps from the Tivoli Identity Manager administrative console, to create LDAP accounts:

1. Log on to the Tivoli Identity Manager administrative console.
2. In the Manage Users panel, click **Search** to see the list of users.
3. Right-click the user Barney Stintson to access the context menu for that user. Click the **Request Accounts** option.
4. Search and select the Service as **LDAP service**.
5. Click **Continue**.
6. In the Account Request panel, provide the required details for creating the LDAP account for the user Barney Stintson. By default, the required information is already provided.
7. Click **Submit**.
8. Go back to the Manage Users panel.
9. Right-click the user Barney Stintson to access the context menu for that user. Click option **Accounts**.
10. Click **Search**.

You see the LDAP account created for Barney Stintson, as shown in Figure 12 on page 22.

⁵ The online Tivoli Identity Manager Version 5.1 information center is located at:
<http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=/com.ibm.itim.doc/welcome.htm>

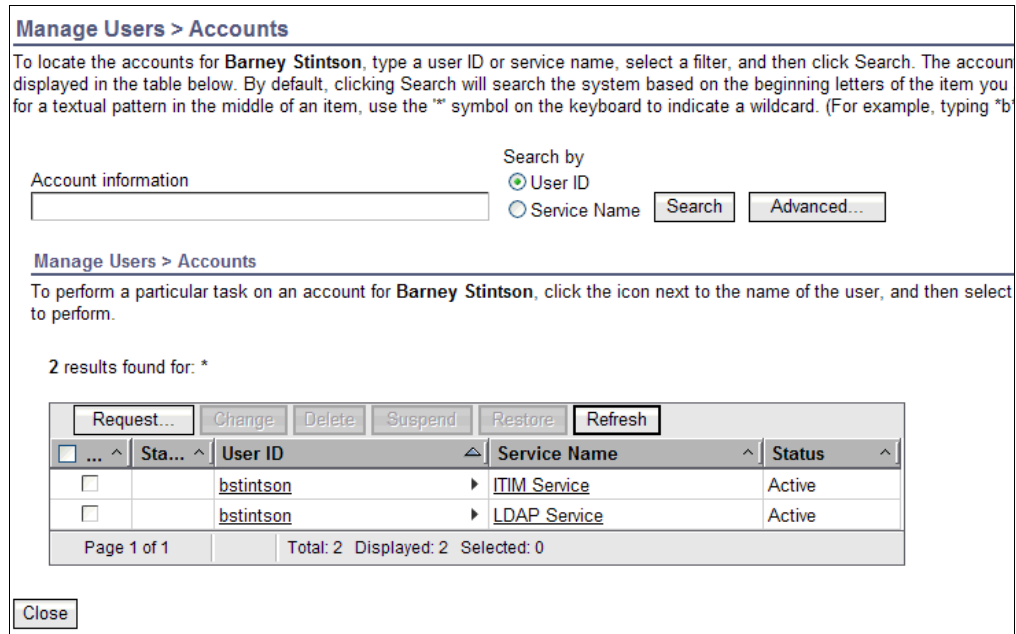


Figure 12 User accounts for Barney Stintson

11. Perform similar steps with all the remaining users to create LDAP accounts.

An important point to note is that with these steps, we created LDAP accounts manually for each user. This activity can also be done by setting the *Provisioning Policy* for the LDAP service to *automatic*. In that case, each user is provisioned with an LDAP account automatically because of the provisioning policy's enforcement.

Creating LDAP groups

Perform the following steps to create LDAP groups and associate LDAP users to the groups.

1. Log on to the Tivoli Identity Manager administrative console.
2. In the Manage Services panel, click **Search** to display the LDAP service in the Services table.
3. Right-click the LDAP Service and select **Manage Groups** from the pop-up menu.
4. Click **Search**. If you have already created any groups, they are shown with the Groups table as a result of the search operation.
5. Click **Create** to start the Group Creation wizard.
6. Specify the Group Name, Analysis group, and other details on the General Information page.
7. Click **Next**.
8. On the Access Information tab, specify the access details as shown in Figure 13 on page 23.

Manage Groups > Create Group > Access Information	
<ul style="list-style-type: none"> ✓ General Information ∞ Access Information Group Membership 	<p>Select the Define an Access check box to activate the access fields. Specify the access information and owner. Additionally, you can choose to enable access requests by users and specify when the Common Access list. If the Define an Access check box is subsequently unchecked, the information operation is completed.</p> <p><input checked="" type="checkbox"/> Define an Access</p> <p>Access status</p> <p><input type="radio"/> Enable Access</p> <p><input checked="" type="radio"/> Enable Common Access</p> <p><input type="radio"/> Disable Access</p> <p>*Access name</p> <p>Analysis</p> <p>Access type</p> <p>Application</p> <p>Access description</p> <p>This access is for Analysis group.</p> <p>Access owner</p> <p>Search... Clear</p> <p>Approval workflow</p> <p>Access Request Workflow for LDAP service</p> <p><input checked="" type="checkbox"/> Notify users when access is provisioned and available for use</p> <p><input checked="" type="checkbox"/> Notify users when access is de-provisioned</p>
<p>< Back Next > Finish Cancel</p>	

Figure 13 Group access information

9. Note that the access request approval workflow defined in earlier sections is specified here with the Approval workflow parameter.
10. Click **Finish** to complete the Group Creation wizard.

You have now successfully created the LDAP *Analysis group*. If an access request to this LDAP group is executed by using Tivoli Identity Manager, any LDAP user can become a member of this group if the user Betty Roberts approves their requests. Perform these steps to create a few more LDAP groups and enable their access details. Each group can have a different access request approval workflow and its workflow participants as per the requirement.

Figure 14 on page 24 shows several LDAP groups that were created on the LDAP service.

Manage Groups > Select Group

To locate a group on LDAP Service service, type information about the group name or description in the field, and then click Search. The groups that match the criteria are displayed in the table below. By default, clicking Search will search the system based on the beginning letters of the item you are searching for. For a textual pattern in the middle of an item, use the "*" symbol on the keyboard to indicate a wildcard. (For example, typing "b*" will find "abc".)

Search information: Search by: Group name or description Access name Group Type: All

Groups

You can add, change, or delete groups. Select the group in the table, and then click the appropriate button.

6 results found for: *

<input type="checkbox"/> Sel...	Group Name	Description	Group Type	Access Name	Access Status	Access Type
<input type="checkbox"/>	Analysis group		LDAP groups	Analysis	Enable Common Access	Application
<input type="checkbox"/>	Authors	This group is for report authors	LDAP groups	Authors	Disable Access	Application
<input type="checkbox"/>	Consumers	This is Consumers group	LDAP groups	Consumers	Disable Access	Application
<input type="checkbox"/>	Metrics Authors	This group is for Metrics Authors	LDAP groups		Disable Access	
<input type="checkbox"/>	Query Users Group		LDAP groups	Query Users Group	Disable Access	Application
<input type="checkbox"/>	Readers		LDAP groups	Readers	Disable Access	Application

Page 1 of 1 Total: 6 Displayed: 6 Selected: 0

Figure 14 LDAP groups

Defining authorization and access permissions with Cognos

In this section, we define authorization and access permissions with Cognos.

Setting up authorization in Cognos

By default, Cognos 8 BI contains a built-in namespace called *Cognos*, which is configured for anonymous (or guest) access. The namespace is pre-populated with several groups and roles that can be used to define *authorizations*. Administrators can extend this namespace by creating new groups and roles to their liking. However, creating users is not possible. The best practice is to create users and groups by using a third-party authentication provider and assign them roles by using the Cognos namespace.

The steps in this section outline the procedure for setting up authorizations for various users and groups that are created in the Tivoli Directory Server LDAP.

The user *jsmith*, created in the TDS-LDAP namespace (based on our Tivoli Directory Server), is assigned administrator privileges. This user will then assign authorization capabilities to the other users and groups, created in TDS-LDAP, to grant access to all the objects in the Cognos connection.

The *Analysis group* in TDS-LDAP is then added to the *Analysis users* role present in the *Cognos* namespace, and the users in this group are granted access only to the Analysis Studio and the reports in the public folders.

Perform the following steps to set up authorization:

1. Navigate to the **IBM Cognos Administration** → **Security** → **Cognos** namespace as shown in Figure 15.

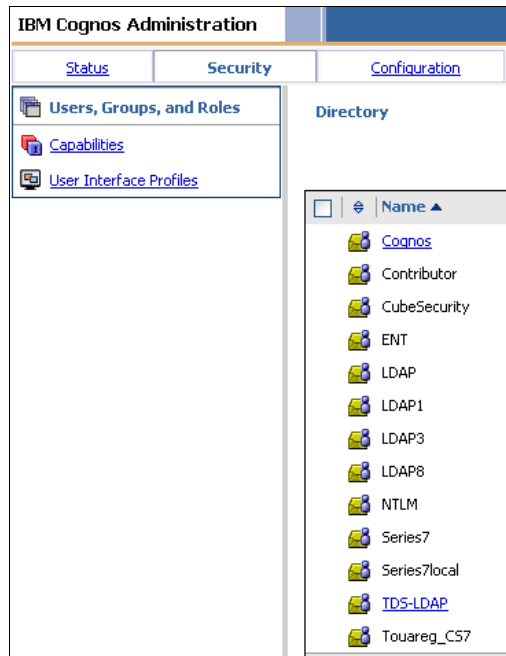


Figure 15 Cognos security configuration

2. Remove the group **Everyone**, which is present under the System Administrators role in the Cognos namespace, shown in Figure 16, and add the user jsmith to it, shown in Figure 17 on page 26. This LDAP user has been created in Tivoli Directory server using Tivoli Identity Manager (for more details, see “Creating LDAP accounts” on page 21).

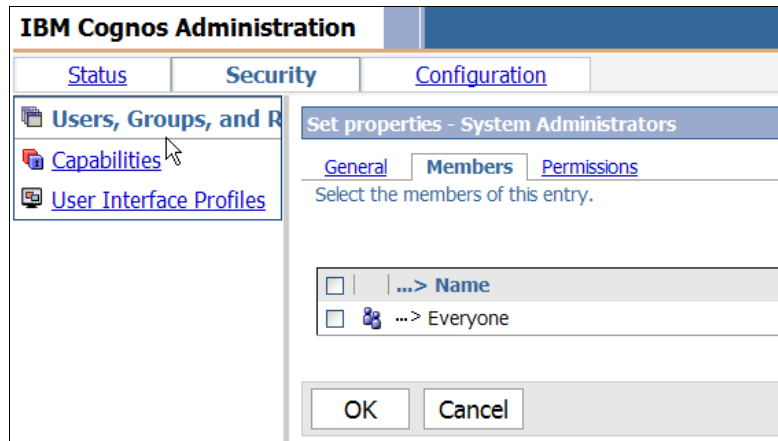


Figure 16 Group Everyone present under the System Administrators role

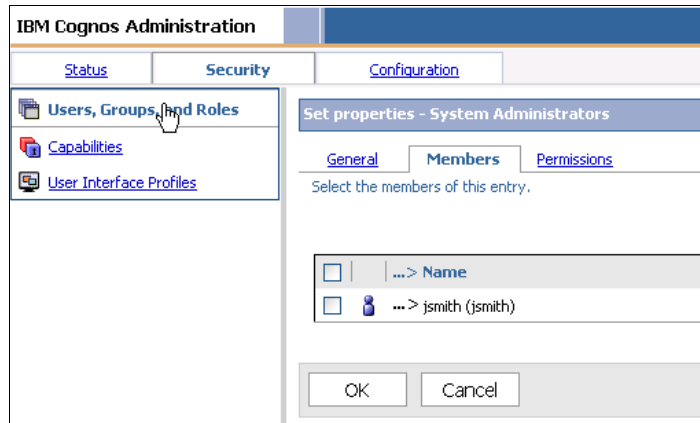


Figure 17 User jsmith added under the System Administrators role

3. Navigate to **IBM Cognos Administration** → **Security** → **Capabilities** → **Analysis Studio** → **Set properties**, as shown in Figure 18.

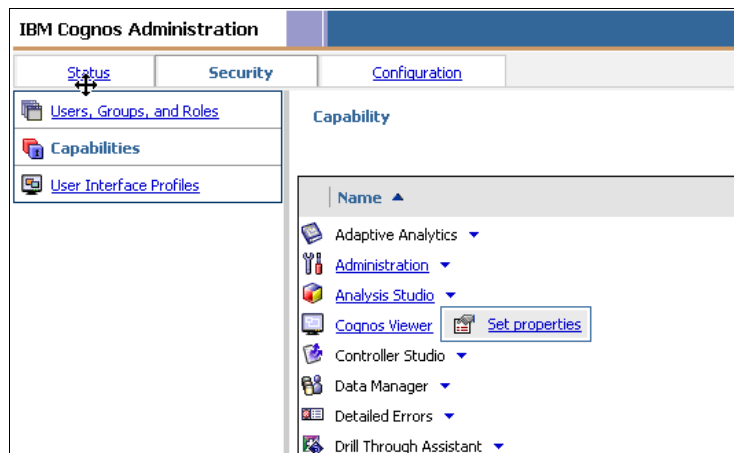


Figure 18 Analysis Studio properties

4. On the Permissions tab, grant **Execute** and **Traverse** permissions to the Analysis Users role, as shown in Figure 19.

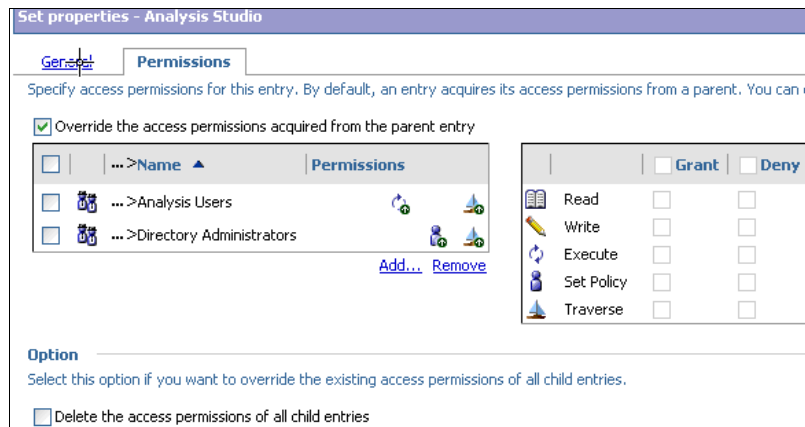


Figure 19 Analysis Studio permissions

5. Go to **IBM Cognos Administration** → **Security** → **Capabilities** → **Query Studio** → **Set properties**.
6. On the Permissions tab, add the Analysis Users role from the Cognos namespace and deny it *all* permissions. See Figure 20. Similar settings can be made for the remaining Studios for which access is needed or denied and for each of the roles as per the requirements.

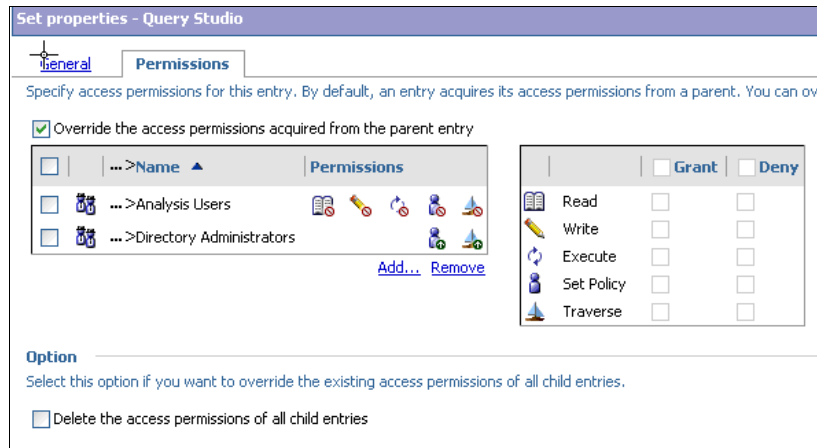


Figure 20 Query Studio permissions

7. Navigate to **IBM Cognos Administration** → **Security** → **Users, Groups, and Roles** → **Cognos** → **Analysis Users**, as shown in Figure 21.

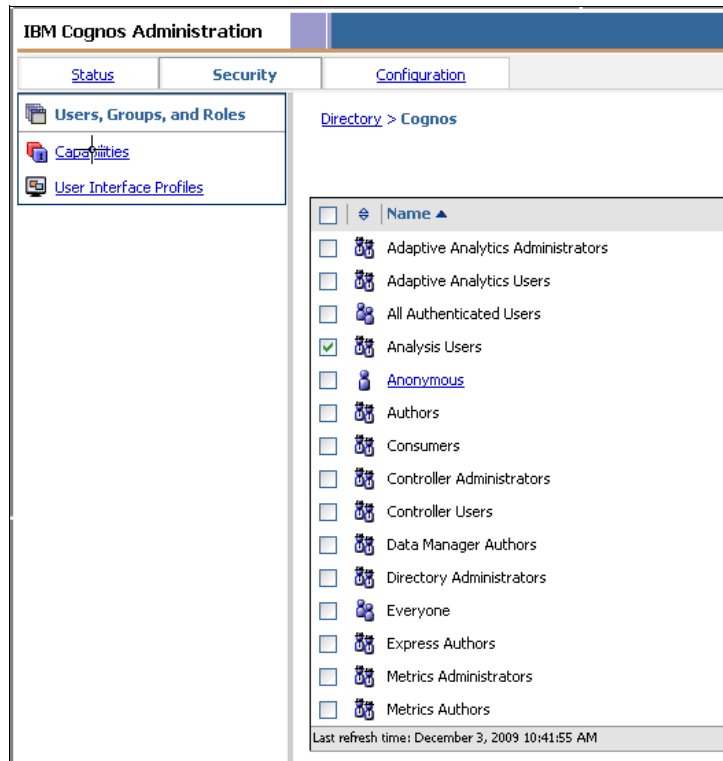


Figure 21 Cognos Users, Groups, and Roles

8. On the Members tab add the **Analysis group** as a member from the TDS-LDAP namespace, as shown in Figure 22.

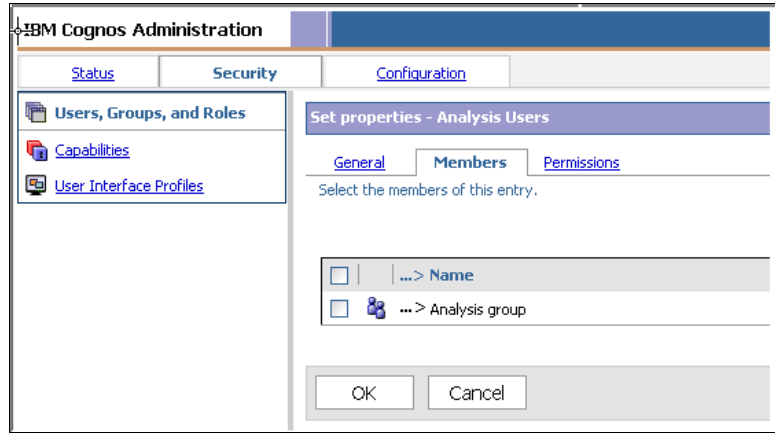


Figure 22 Adding Analysis group as a member

Now, the members of the Analysis group can access all the report objects and they can only use Analysis Studio. Similarly, permissions for other groups or roles can be configured in the Cognos connection.

Accessing Tivoli Identity Manager’s self-care user interface

In previous sections, we added person data (employee data) in Tivoli Identity Manager by using the HR feed mechanism. Each person that is added through this mechanism is being automatically assigned a Tivoli Identity Manager account. We also created LDAP accounts for these users. Using their Tivoli Identity Manager accounts, the users can access the Tivoli Identity Manager self-care user interface. The self-care user interface provides a central interface for users to perform a variety of simple, intuitive tasks that cover updating of their personal information and passwords, viewing requests, completing and delegating activities, and requesting and managing their own accounts and accesses.

Figure 23 shows a view of the Tivoli Identity Manager self-care interface from Barney Stintson.

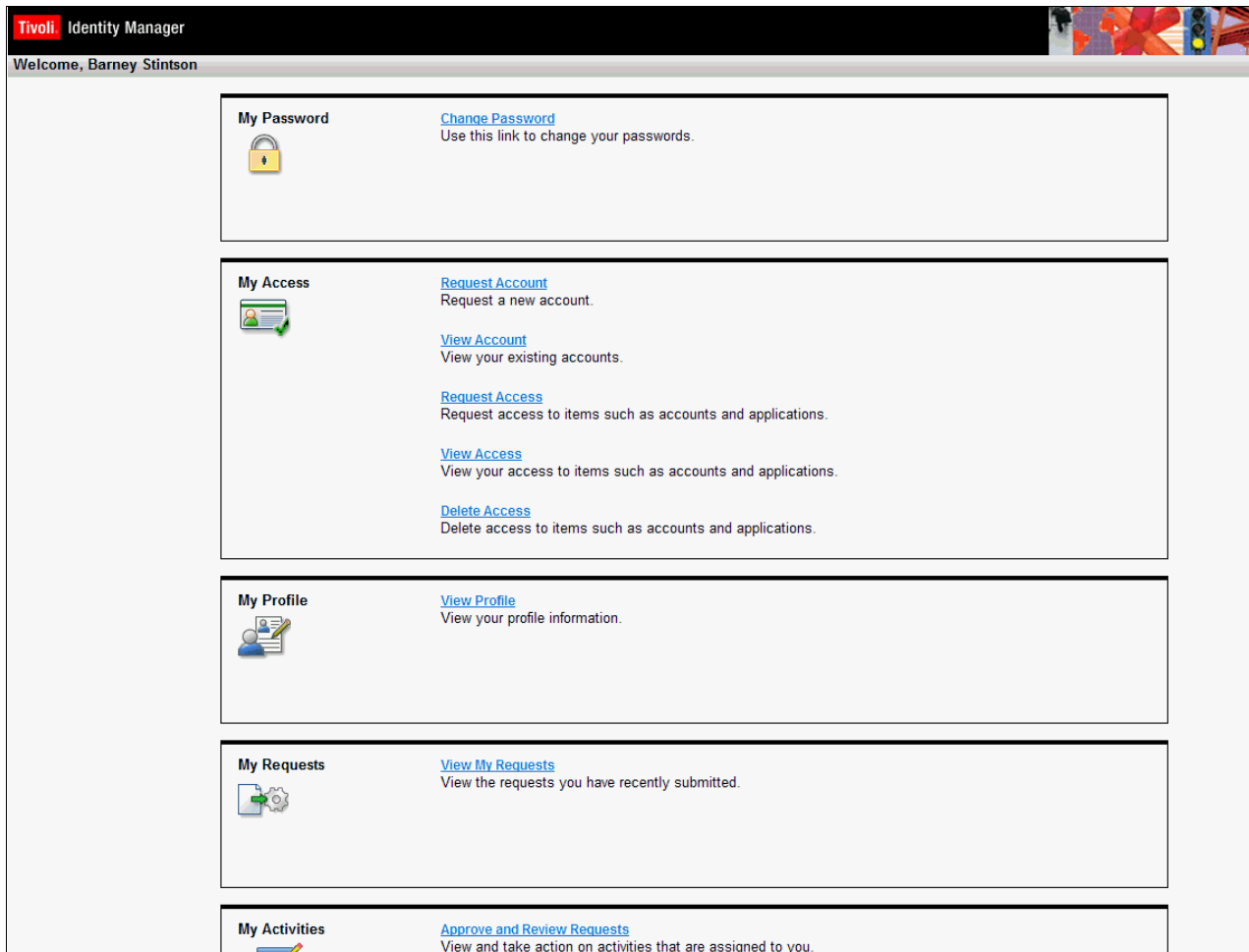


Figure 23 Tivoli Identity Manager self-care user interface

In the following sections, we illustrate several useful self-care capabilities that are often needed.

Resetting a password

With Tivoli Identity Manager in place for managing user accounts, users can log into the self-care user interface to perform basic account operations without any involvement of an administrator. Users can view their account information and perform password resets on the accounts.

Perform the following steps for the user Barney Stintson (having a Tivoli Identity Manager account ID as bstintson) to reset the account password.

1. Log on to the Tivoli Identity Manager self-care user interface: Use the existing user ID bstintson.
2. From the home page, click the **Change Password** hyperlink.
3. On the Change Password details page, provide details such as the old password and new password.

- Review the account information that is affected by this password change, as shown in Figure 24.

Tivoli Identity Manager

Welcome, Barney Stintson

[Home](#) > [Change password](#)

Change Password

View the accounts to be affected by the password change and review the criteria for the new password. Then, specify a new password.

▼ **1. View my accounts that will be affected by this password change.**

Account Type	User ID	Description
ITIM Service	bstintson	
LDAP Service	bstintson	

Page 1 of 1 Total: 2 Displayed: 2

2. For security purposes, enter your current Tivoli Identity Manager password.

Current Tivoli Identity Manager password:

▼ **3. Review the criteria for my new password:**

- There is no restriction for the new password.

4. Change my password.

New password:

New password (confirm):

Figure 24 Change Password details

- Click **OK** to submit the password change for the listed accounts.
- Click the **View My Requests** link to verify that the password change operation succeeded.

Requesting LDAP group access

With the Tivoli Identity Manager self-care user interface, users can manage their access information, for example, membership for various groups. Users can also request new access or remove existing accesses.

Let us look at how user Barney Stintson requests access to the *Analysis Group*.

An important point to note is that, in “Defining approval workflows” on page 17, we defined an *access request approval workflow* for the LDAP profile, and it is associated with the access request of the LDAP group *Analysis Group*. When the user Barney Stintson requests access to this group, an approval notification is sent to the approver, that is, Betty Roberts.

Perform the following steps for the user Barney Stintson to request access to the *Analysis Group*, and for the user Betty Roberts to approve the access request:

- Log on to the Tivoli Identity Manager self-care user interface with user ID `bstintson`.
- On the home page, click the **Request Access** hyperlink.
- Click the **Analysis** Access Name hyperlink.

4. Click **Request Access**. An access request is submitted, as shown in Figure 25.

The screenshot shows a web page titled "Request Submitted: New Access". At the top, it says "Welcome, Barney Stintson" and has a breadcrumb trail: "Home > Request access > Request submitted". The main heading is "Request Submitted: New Access". Below this, a message states: "You have submitted a request. Below is the information available to you at this time." There is a section titled "Request Detail" with the following information: Request ID: 6447972490214660085, Date submitted: December 29, 2009 1:39:48 PM, Request type: Access Add, Account/Access: bstintson on Analysis, Access type: Application, and Description: This access is for Analysis group. Below this is a "Related Tasks" section with three bullet points: "To check on the status of your request, refer to the View Requests page.", "To request another access, click on Request Access to search for another access.", and "To perform other tasks go to the Tivoli Identity Manager Home page."

Figure 25 Access request details

5. Click on the **View Requests** page hyperlink.
6. In the Requests table, click the **Access Add** hyperlink. Details about the request information is displayed, as shown in Figure 26.

The screenshot shows a web page titled "Request Information". At the top, it says "Welcome, Barney Stintson" and has a breadcrumb trail: "Home > View my requests > Request information". The main heading is "Request Information". Below this is a section titled "Request Detail" with the following information: Request ID: 6447972490214660085, Date submitted: December 29, 2009 1:39:46 PM, Request type: Access Add, and Account/Access: bstintson on Analysis. Below this is a section titled "Status Detail: Pending approval" with the following information: Due date: December 30, 2009 1:39:48 PM and Approvers: Betty Roberts. Below the approver information is a table with one row: "Full Name" with a dropdown arrow, "Betty Roberts", and "Page 1 of 1 Total: 1 Displayed: 1". At the bottom of the page is a link: "Go to View My Requests".

Figure 26 View request information

Submitting this access request initiates an approval workflow for the user Betty Roberts to take action.

7. Log out from the Tivoli Identity Manager self-care user interface.

8. Log on to the Tivoli Identity Manager self-care user interface using the user ID broberts. This user is the approver for the access request workflow that we have just defined.
- When Betty Roberts logs in, an approval activity is automatically shown in the to-do list, labeled *Action Needed* (Figure 27 on page 32).

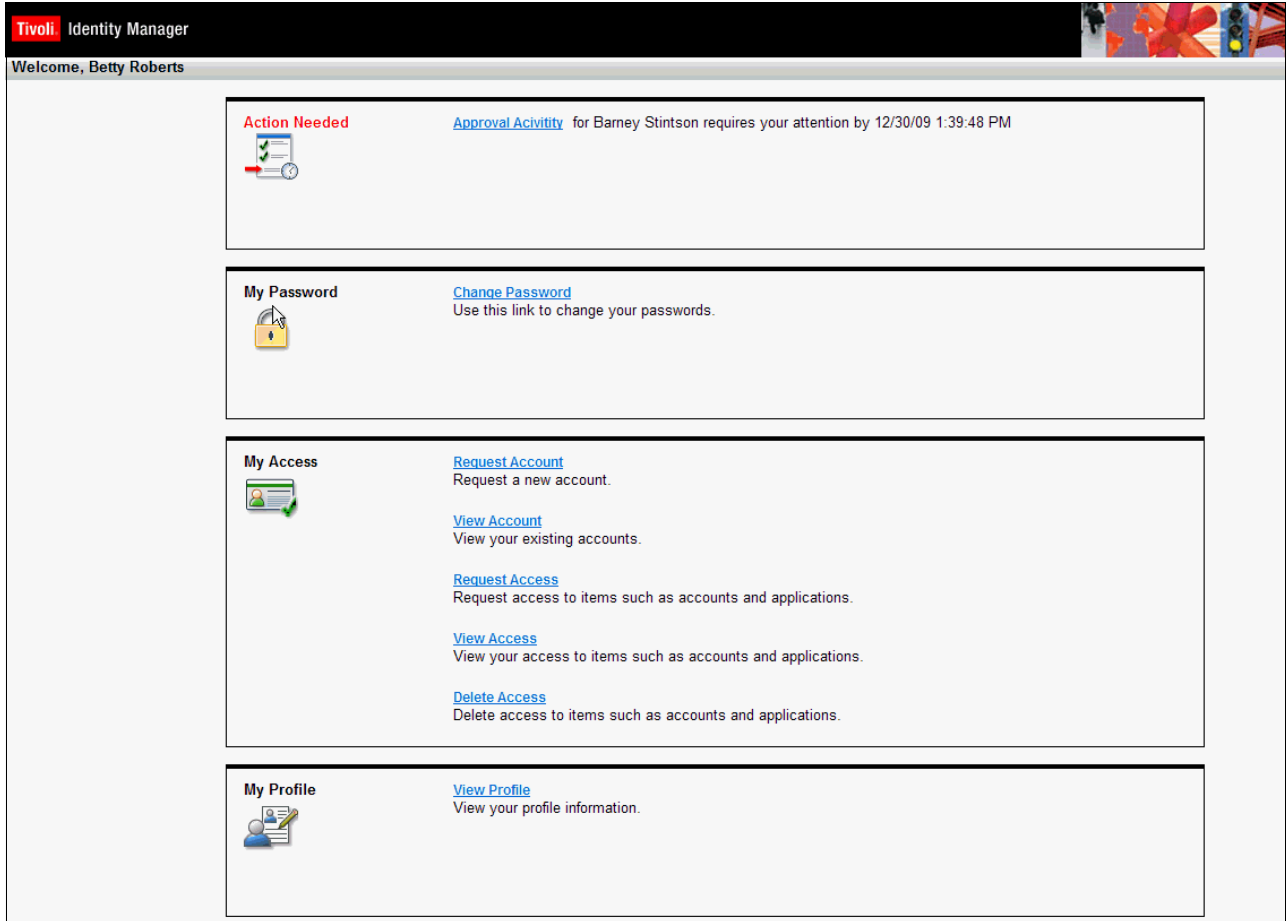


Figure 27 Self-care user interface for the workflow approver

9. Click the **Approval Activity** hyperlink.
- The review (approval) page opens. It offers various details and an approval action to be taken, as shown in Figure 28 on page 33.

Review Request

Review the details of this request. To complete this activity, select the appropriate action, enter information in the comments field, and click OK. If you do not want to approve or reject the request at this time, click Cancel.

Request Detail

Date submitted: December 29, 2009 1:39:47 PM
 Request type: Access Add
 Requested for: Barney Stintson
 Requested by: Barney Stintson
 Account/Access: bstintson on Analysis
 Due date: December 30, 2009 1:39:48 PM
 Instruction summary: Approve/Reject the Request

Instruction Detail

The following request has been submitted for your approval
 View Changes: <http://9.122.127.58:9080/itim/self/ReviewActivities.do?activity=6447976464219223321>
 Description:
 Requestee: Barney Stintson
 Subject: bstintson
 Access Name: Analysis
 Request Initiated: Dec 29, 2009 01:39:47 IST
 Process Reference: 6447974602776489668

Requested by process:
 Process ID: 6447972490214660085
 Process Name: Access Add
 Description: Access Add Process
 Requester: Barney Stintson
 Requestee: Barney Stintson
 Subject: bstintson

Reviewer Action

Select the appropriate action:

Approve
 Reject

Reviewer Comments

Enter comments:

I approve this request since Barney Stintson is on assignment of designing analytics reports for the next few months.

Figure 28 Review request

10. As shown in Figure 28, select **Approve** and provide reviewer comments.

11. Click **OK** to finish the approval activity.

Performing these steps sends an access notification to Barney Stintson, granting the user access to the *Analysis Group*. When Barney now logs in to Cognos, he will be able to use Analytics Studio capabilities, access all the report objects, and use Analysis Studio.

Figure 29 on page 34 shows the Cognos 8 page after Barney has successfully logged in.

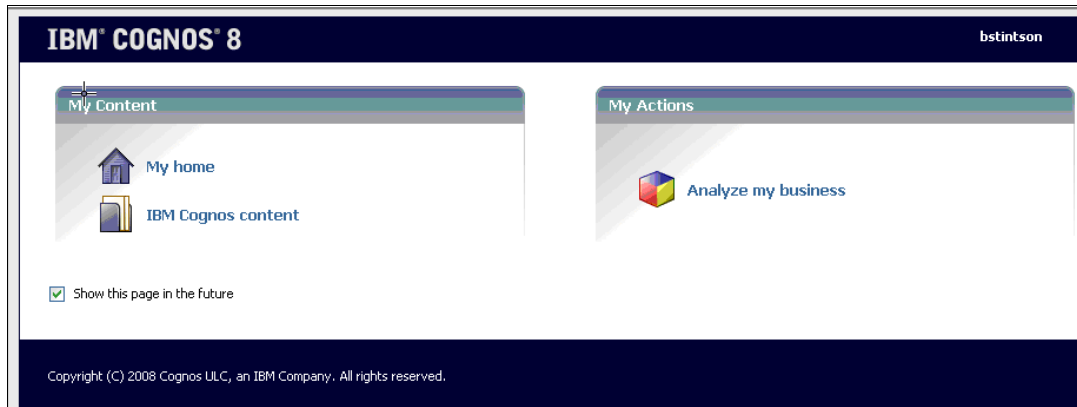


Figure 29 User bstintson accessing Cognos content

8.4 User recertification

Tivoli Identity Manager provides the ability to certify and validate a user's access to IT resources on a regular interval. User *recertification* is a type of certification process that combines recertification of a user's accounts, group memberships of accounts, and role memberships into a single activity. User recertification activities are completed by a specified participant, such as a manager or application owner. Each user recertification activity lists accounts, group memberships, and role memberships owned by a user. Groups that are enabled as access are displayed within the activity using the access information rather than the group information. The participant can individually approve or reject whether the user still requires each account, group membership, and role membership. Several actions can be taken when a resource or membership is rejected, including suspension of the resource or removal of the membership.

Setting up a user recertification policy

Perform the following steps to set up the recertification process for LDAP accounts and access (groups) entitlements in our IBM Cognos integration scenario:

1. Log on to the Tivoli Identity Manager Administrative console.
2. Go to the **Manage Policies** → **Manage Recertification Policies** panel and click **Create** to create a new Recertification policy.
3. On the Recertification Policy wizard's General page, provide the policy name Recertification Policy for all users.
4. Click **Next**.
5. Select Policy recertifies as **Users**.
6. Click **Next**.
7. With the default settings selected, click **Next** again.
8. On the Resource Targets page, select options **None**, **Accounts on specified services**, and **All groups on specified services** respectively for the options Roles, Accounts, and Groups.
9. Click **Next**.
10. Click **Add** to add the account target as *LDAP Service*, which we created earlier.
11. Click **Next**.
12. Select the recertification schedule options as needed. In our example, we select Evaluation frequency as **Weekly**.

13. Click **Next**.

14. On the Policy page choose **Specified user** for the option “Who approves recertification.”

15. Select the user Betty Roberts as the recertification approver.

16. With the remaining settings set to the defaults, click **Finish**.

Performing these steps creates a user recertification policy with a weekly execution schedule and with Betty Roberts being the approver.

Recertifying users

Now that the user recertification policy is configured and scheduled for weekly execution, Betty Roberts receives recertification notifications every week, and she must recertify (approve or reject) LDAP accounts as well as LDAP group memberships.

The following steps show how Betty Roberts recertifies accounts and group memberships for the LDAP service:

1. Logs on to the Tivoli Identity Manager self-care user interface as broberts.

The home page, shown in Figure 30, shows the various recertification approvals pending as the very first task.

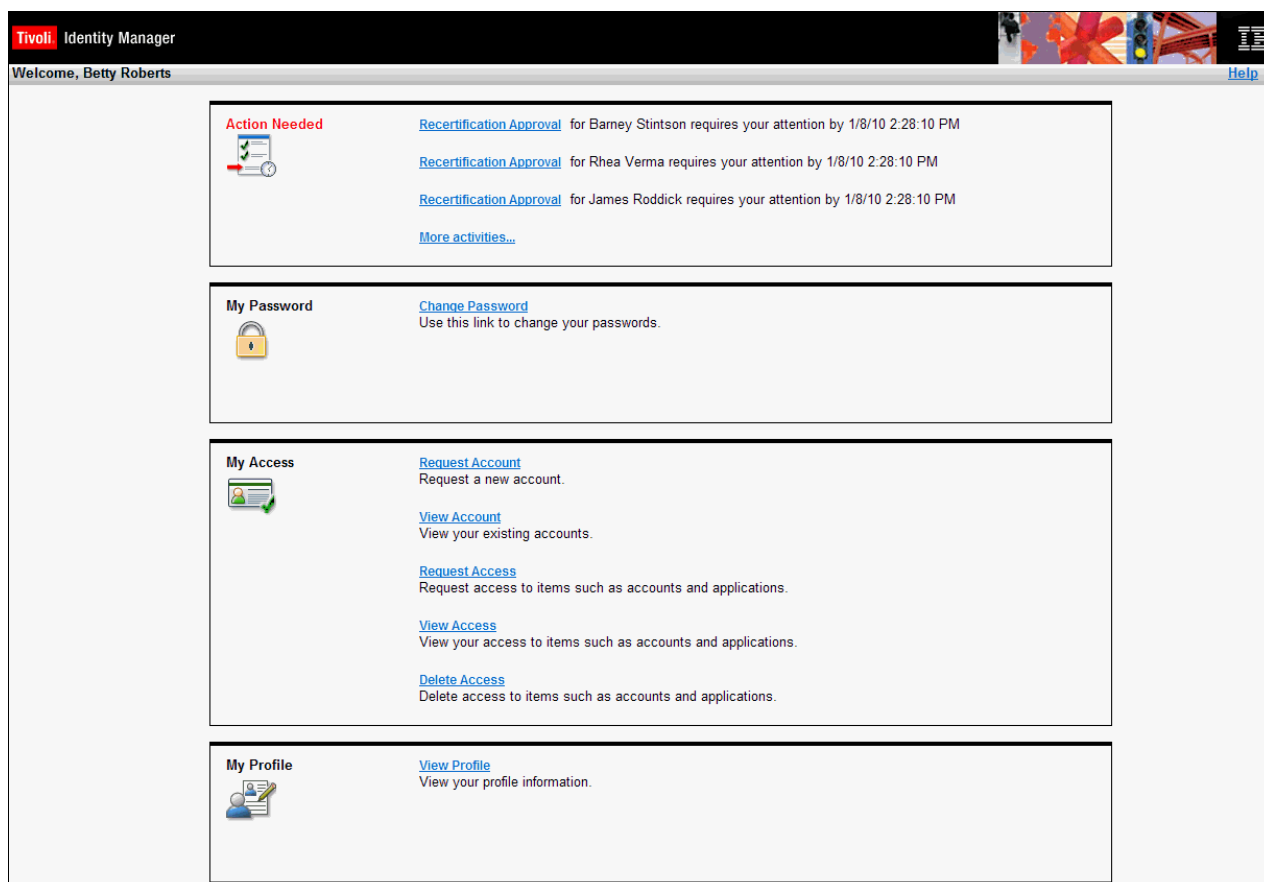


Figure 30 User recertification requests

2. Clicks the **Recertification Approval** hyperlink for the user Barney Stintson.

- Performs the approve action by selecting **Yes** for Barney's LDAP account as well as the *Analysis group*, shown in Figure 31.

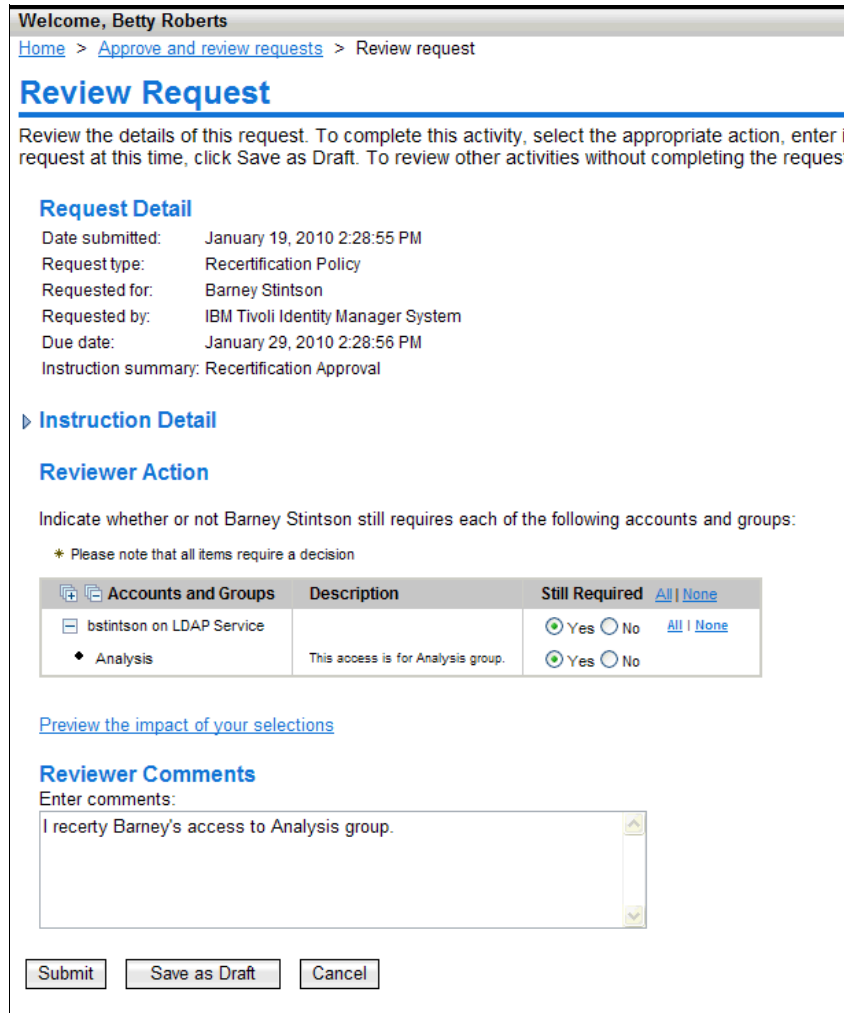


Figure 31 Review Request

- Clicks **Submit** to complete the recertification activity.

Reporting

Many organizations require detailed auditing and reporting that can show exactly who accessed what, how and when they accessed it, and who approved or granted user access. Tivoli Identity Manager provides centralized auditing and reporting that can reduce the time spent on audit trails on disparate systems. An authorized user can use the Tivoli Identity Manager report system to create reports based on the criteria you select. Tivoli Identity Manager allows authorized users to generate various types of reports.

In our integration setup, where we are managing LDAP accounts and groups by using Tivoli Identity Manager, the following reports can be useful for auditing purposes:

Requests Reports that provide workflow process data, such as account operations, approvals, and rejections.

- User and Accounts** Reports that provide user and accounts data, such as individual access and accounts, pending recertification's, and suspended individuals.
- Services** Reports that provide service data, such as reconciliation statistics, list of services, and summary of accounts on a service.

Refer to the IBM Tivoli Identity Manager online documentation to learn more about the reporting capabilities.

Conclusion

In this paper, we have demonstrated the added value that IBM Tivoli Identity Manager can deliver as an identity life cycle management solution when integrated with IBM Cognos 8 security. We also discussed v sample design approaches and illustrated the integration between Tivoli Identity Manager, the Cognos authentication provider, and Cognos 8 security features. Finally, we have shown several key features of Tivoli Identity Manager that can help to provide better security with users and their access rights in a Cognos environment.

References

The publications listed in this section are considered particularly suitable for a more detailed discussion of the topics covered in this paper.

- ▶ The Tivoli Identity Manager version 5.1 information center:
<http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=/com.ibm.itim.doc/welcome.htm>
- ▶ IBM Cognos 8 v4 Business Intelligence information center:
<http://publib.boulder.ibm.com/infocenter/c8bi/v8r4m0/index.jsp>
- ▶ Cognos proven practices Web site:
<http://www.ibm.com/developerworks/data/library/cognos/cognosprovenpractices.html>

The team who wrote this IBM Redpaper

This paper was produced by a team of specialists from around the world working at the International Technical Support Organization (ITSO).



Axel Buecker is a Certified Consulting Software IT Specialist at the International Technical Support Organization, Austin Center. He writes extensively and teaches IBM classes worldwide on areas of Software Security Architecture and Network Computing Technologies. He holds a degree in Computer Science from the University of Bremen, Germany. He has 23 years of experience in a variety of areas related to Workstation and Systems Management, Network Computing, and e-business Solutions. Before joining the ITSO in March 2000, Axel worked for IBM in Germany as a Senior IT Specialist in Software Security Architecture.



Dinesh T. Jain is a Senior Staff Software Engineer in the IBM India Software Lab. He has been part of the Tivoli Security product development team for the past 6 years. In his current role, Dinesh is part of the Tivoli Identity Manager Development team, based in Pune, India. Dinesh has been an author of several articles and IBM Redbooks publications, and an innovator of several solutions published on IBM developerWorks®, and the Tivoli OPAL site. As a Tivoli Lab Advocate, Dinesh has worked closely with several key clients to promote Tivoli Security products and to improve existing deployments of Tivoli security products. Dinesh holds a Masters degree in Computer Science from the University of Pune, India.



Aditya Joglekar is an Associate Software Engineer in the IBM India Software Lab. He is part of the Tivoli Identity Manager team. As part of his job role, he is responsible for improving the quality of the product. He also has been involved with Tivoli Directory Integrator on an internship as a project trainee before he joined IBM. Aditya holds a Masters of Computer Application degree from the Vishwakarma Institute of Technology, India.



Nikhil Mayaskar works on the IBM Cognos System Quality team in the IBM India Software Lab in Pune for the past 2 years. In his role, Nikhil has been involved in analysis, design, development, and enhancement of the test framework for testing the Cognos suite of products. His areas of experience are Java™, J2EE, and Web technologies in finance and business intelligence domains. Nikhil holds a B-Tech degree in Electrical Engineering from IT-BHU, India.

Thanks to the following people for their contributions to this project:

Diane Sherman
International Technical Support Organization, Austin Center

Dave Bachmann, Oliver Bergmann, Aditi Bhattacharya, Antonio Marziano, Manoj Patil,
Sameer Wakude
IBM

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing, IBM Corporation, North Castle Drive, Armonk, NY 10504-1785 U.S.A.

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs.

This document REDP-4643-00 was created or updated on February 9, 2010.



Send us your comments in one of the following ways:

- ▶ Use the online **Contact us** review Redbooks form found at:
ibm.com/redbooks
- ▶ Send your comments in an email to:
redbooks@us.ibm.com
- ▶ Mail your comments to:
IBM Corporation, International Technical Support Organization
Dept. HYTD Mail Station P099
2455 South Road
Poughkeepsie, NY 12601-5400 U.S.A.




Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. These and other IBM trademarked terms are marked on their first occurrence in this information with the appropriate symbol (® or ™), indicating US registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at <http://www.ibm.com/legal/copytrade.shtml>

The following terms are trademarks of the International Business Machines Corporation in the United States, other countries, or both:

Cognos®
developerWorks®
IBM®

RDN®
Redbooks®
Redpaper™

Redbooks (logo) ®
Tivoli®

The following terms are trademarks of other companies:

SAP, and SAP logos are trademarks or registered trademarks of SAP AG in Germany and in several other countries.

Java, and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Microsoft, Windows, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Other company, product, or service names may be trademarks or service marks of others.