2AB, Inc. January 2006

Harmony

The 2AB Newsletter

2AB Announces Open Source Strategy

jLock Source available for Customers

Special points of interest:

- Open Source Strategy for jLock provides choice of GPL or Commercial Source licensing
- Using orb2's Identity Manager with CSIv2 GSSUP
- Sneak Preview of next release features in iLock Identity Management tools
- Governance-Based Access control
- Wide range of operating platforms

2AB has announced plans to Open Source the jLock product in 2006. jLock provides a scalable commercial implementation of the Java Authentication and Authorization Service (JAAS).

The source, which will be available for licensing under the GNU Public License (GPL), will include the JAAS implementation, the iLock Security Center Service and the standard edition of the jLock Administrative tools. This complete offering provides a scalable implementation of JAAS with graphical Identity Management of Users, Groups and Roles.

2AB will offer an alternative commercial source and binary license for customers who do not wish to open source derivative works. This dual-licensing model addresses the complex demands of the software community and has worked well for a number of companies. 2AB will continue to offer and support a commercial jLock Power Edition product.

jLock utilizes a Service Oriented Architecture and embeds 2AB's orb2 for remote communications. The open source version will use the Java ORB. Customers who require the performance, reliability and advanced features provided by orb2 may license the commercially supported binary version of jLock Power Edition or license orb2 independently.

jLock Power Edition will continue to embed orb2 and will provide value-added features such as advanced tooling in

(See OpenSource on page 5)

In this issue:

Developer's Corner

Using the orb2 Identity Manager

orb2 for Java version 4.2, released in June 2005, bundled Identity Management tools as part of the CSIv2 infrastructure to provide user, group and role based access control for securing the orb2 Naming Service. In this article we'll look at how you can leverage these tools to secure your orb2 CORBA applications.

CSIv2 is the OMG and JCP standard for secure interoperability. It leverages TLS for server authentication and provides a choice of mechanisms for client authentication. The most commonly used method of client authentication is the UserId and Password. In the CSIv2 standard, this is known as the GSSUP option. GSSUP can be used with or without TLS (that is, you may leverage GSSUP while still using TCP/IIOP as your transport protocol). This is useful in environments where you trust the server network infrastructure but still have a need to authenticate clients. You can, of course, use TLS for client authentication if you choose. TLS client authentication, however, will require a digital certificate for each user.

In this article, we will show

(See DevCorner on page 2)

(DevCorner Continued from page 1)

you how to integrate CSIv2's GSSUP client authentication into your CORBA applications. We will also provide a look at the Identity Management tools and Security services that ship with the orb2 for Java product.

orb2 includes security demonstration programs that use CSIv2. These demos (security and security_up) illustrate how a client and server can leverage CSIv2 with no code changes. While this level of transparency makes it very easy to secure existing applications, it requires that all the information needed by CSIv2 be placed in property files. In the case of GSSUP, this includes the UserId and Password for the client software. Obviously, this is not a very desirable solution! So we'll modify this Client demo to request a UserId and Password at runtime and then set CSIv2 parameters programmatically.

In Figure 1, we modify the Client.java provided (demos/security_up) to use a custom JDialog that requests a UserID and Password (shown in Figure 2). Figure 3 shows how to set the orb2 security properties programmatically. These properties are passed along with all the other orb properties in ORB_init(). The properties that tend to be static or that you wish to remain under the control of operations (such as debugging level or the location of the security center) may still be specified in property files. These properties are located in the Client.properties and Svc.properties files in the demonstration directory.

With these simple changes you have added CSIv2 GSSUP to your application without the need to hard-code a UserId and Password in a property file. Now let's look at how you use the Identity Manger to manage your UserIds and Passwords.

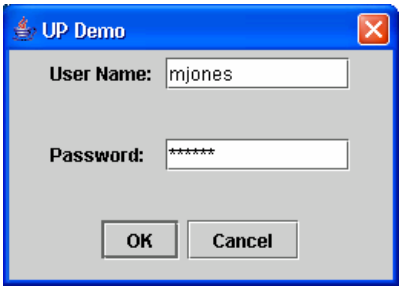
The Identity Manager (and your CSIv2 GSSUP) uses a sharable Security Service. Like all Service Oriented solutions, this enables remote administration as well as sharing of services between multiple applications and users. Figure 4 shows the User View in the Administrative Tool.

For more information and/or the modified demo source, contact info@2ab.com.

```
import com.twoab.orb2.util.*;
        ...
JFrame frame = new JFrame();
UserPwdDialog logind =
        new UserPwdDialog(frame, "UP Demo",true );
        String [] user = logind.getData();
        ...
```

Figure 1: Request UserID & Password via dialog

Figure 2: The UserPwdDialog




```
Properties props = new Properties();
…
props.setProperty(
        "com.twoab.orb2.security.user", user[0]);
props.setProperty(
        "com.twoab.orb2.security.password", user[1]);
…
try  {
 // initialize ORB
 orb = ORB.init(args, props);
 …
```

Figure 3: Set the user and password properties

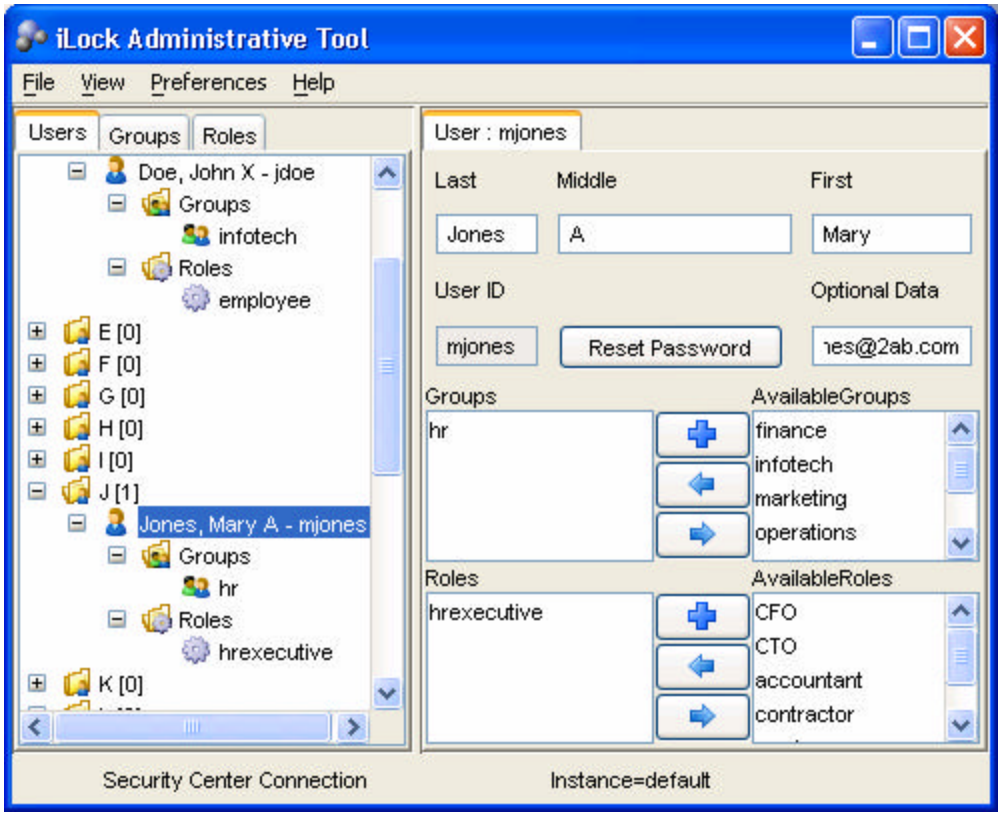


Figure 4: The orb2 Identity Manager User View

Sneak Preview

Governance-Based Access Control

CGI (www.cgi.com) released a whitepaper last fall entitled, *"Governance-Based Access Control: Enabling improved information sharing that meets compliance requirements."* Governance-Based Access Control (GBAC), as described in the paper, is focused on the classification of information assets for the purpose of information sharing in an environment where:

- Many organizations may require access to information
- Information may be accessed by, or shared with, external users
- Everyone may be subject to compliance with multiple authorities and jurisdictions

2AB subsequently released two whitepapers which describe how the access management standards supported by our iLock Security Services products (jLock's JCP JAAS and orbLock's OMG Resource Access Decision Facility) can be utilized to support the GBAC access control model. The papers outline the steps necessary to apply the GBAC model using these standards in a scalable manner.

Those steps include:

- Classify Information
- Classify People
- Define Access Rules

In this article, we summarize the information available in the JAAS whitepaper and show some of the tools we're providing in jLock Power Edition to fully support the GBAC model.

Figure 1 shows how the classification of information described in the CGI whitepaper can be represented as JAAS resources.

In Figure 2 and Figure 3 we explore how Groups (an organizational view) and Roles (a functional view) may be defined for use in classification of people. Figure 4 shows the assignment of groups and roles to people (roles may also be defined directly to a group).

Access control rules are defined in GBAC based upon the roles of individuals and context information related to the information. The rules we show in this example are

(Preview continued on page 5)

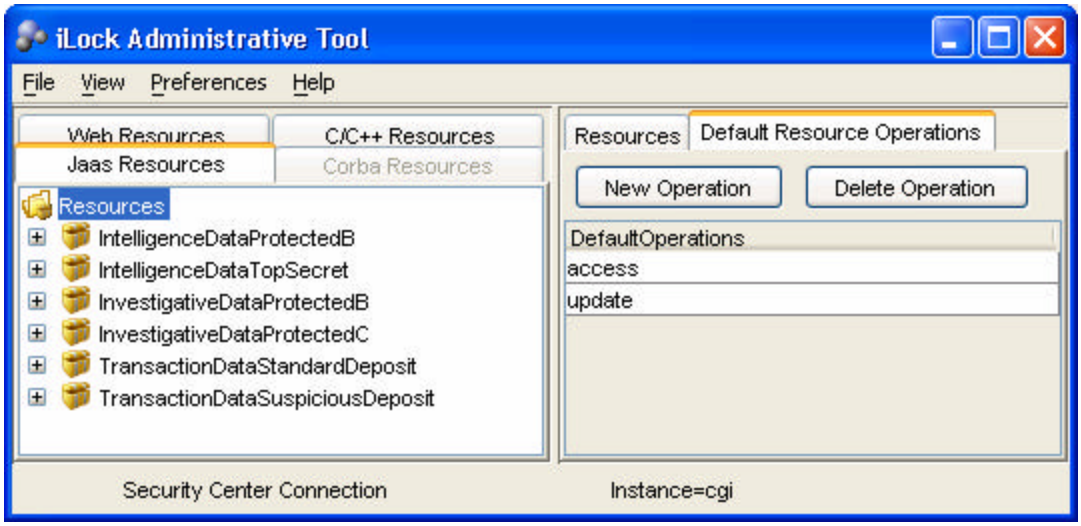


Figure 1: Viewing the GBAC Information Classifications as JAAS Resources

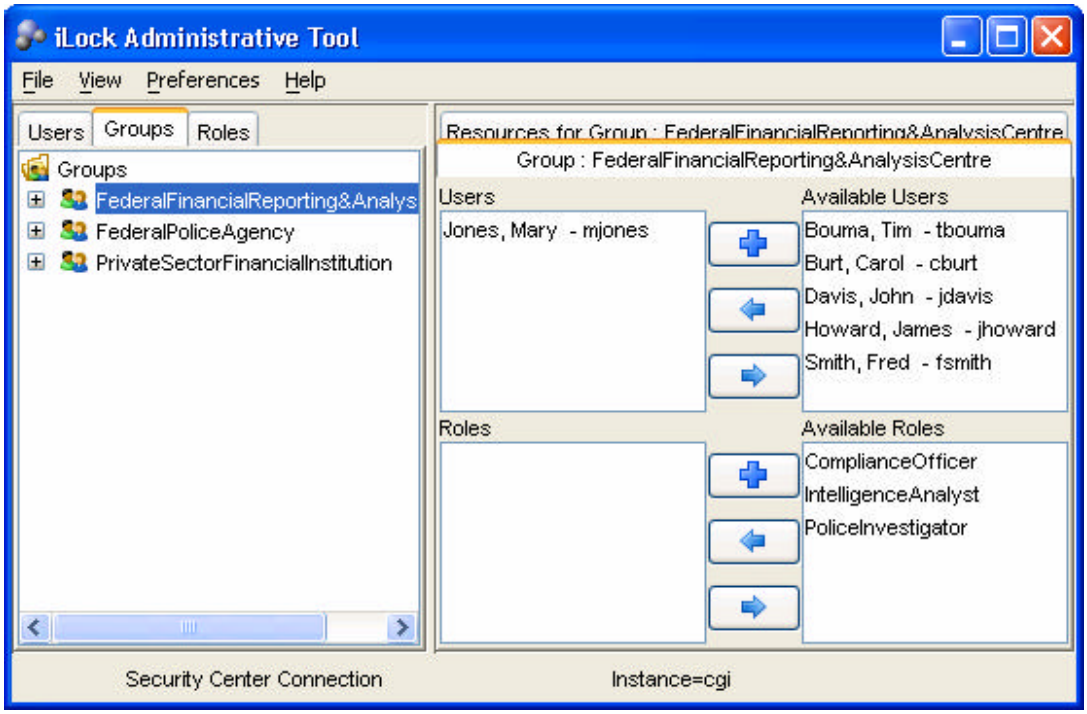


Figure 2: Defining the GBAC Groups that will be used to classify people

"IT Governance provides the business foundation for establishing Access Policy based on classification of People, Information and Services"

Figure 3: Defining GBAC roles that will be used to classify people

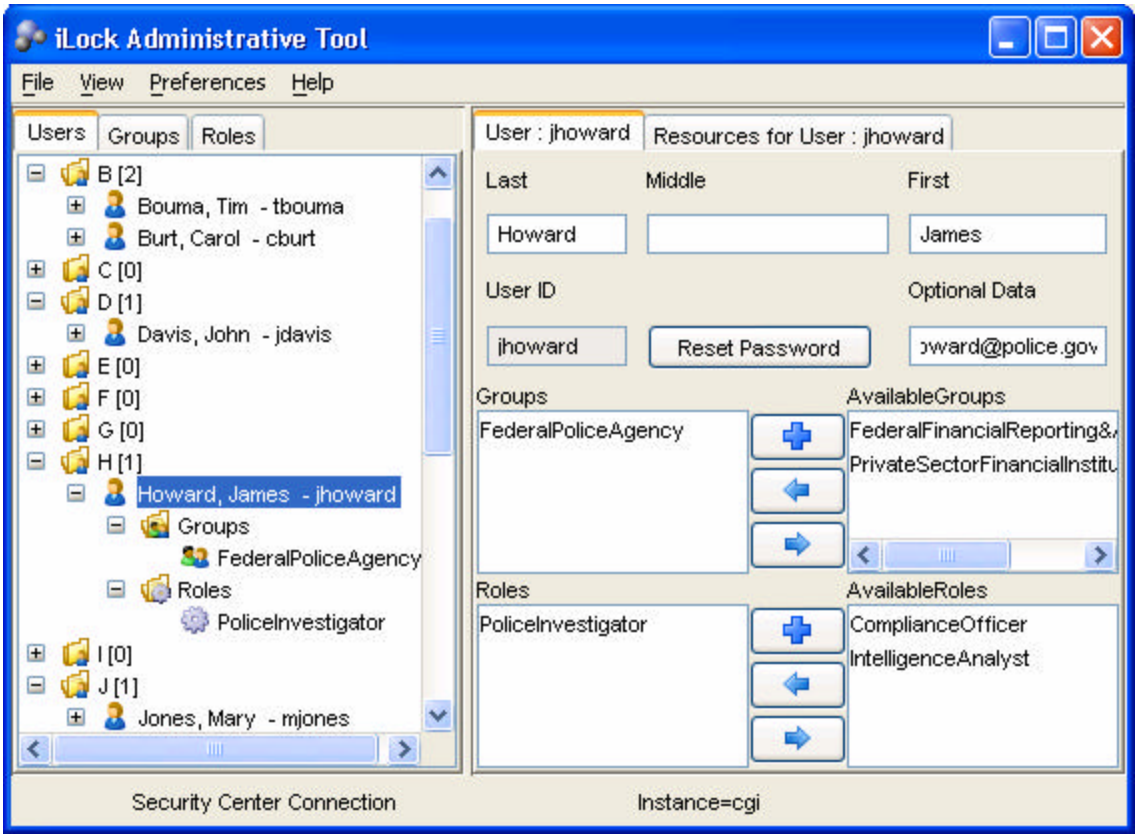


Figure 4: James Howard is in the Group FederalPoliceAgency and has the Role PoliceInvestigator

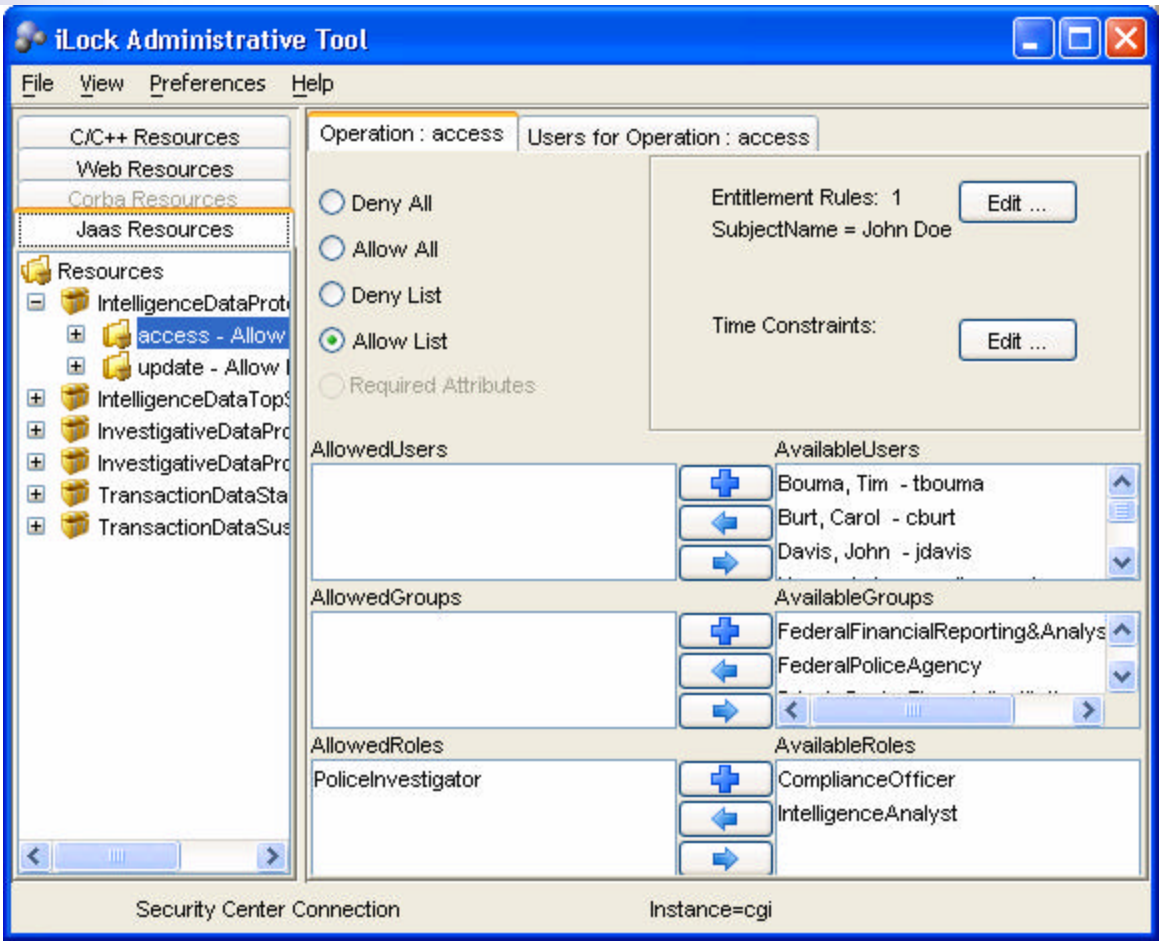


Figure 5: Using GBAC Classifications to define Access Policy Entitlements and Timed-Based Rules can also be defined

outlined in Table 2 of the CGI GBAC whitepaper.

By selecting a Resource (GBAC information classification) as shown in Figure 4, you can view and/or modify the access policy. Note that jLock allows you to specify rules for different operations on Resources (the GBAC information classification). For example, you see that there are access and update rules which may be defined differently.

The GBAC model requires that context information be provided at the time of the access request. This information is evaluated as part of the policy. For example, the scenario in the GBAC whitepaper has two different examples. Some of the rules are scoped to information regarding someone with the Subject Name of "John Doe" as shown above. In another GBAC rule, the transaction amount of a deposit must be greater than $10,000. This type of policy is an example of what jLock implements using entitlement rules. Since the JAAS model of authorization has no mechanism for supporting this type of rule, jLock Power Edition has extended JAAS to enable complex, context-sensitive and entitlement-based policies. jLock also supports time sensitive rules. For example, an access policy may only be valid Monday through Friday from 8:00am to 5:00pm.

This article provides an overview of the support that iLock products provide for Goverance-Based Access Control. In addition to whitepapers, 2AB has two demonstration CDs available. The GBAC CDs include an evaluation of jLock Power Edition and a demonstration application. For your copy, e-mail info@2ab.com.

(OpenSource from page 1)

support of highly complex access control policies. The commercial version of jLock will be value add and compatible with the freely available version, providing an upgrade path and a fully-supported binary solution for end-users and/or ISVs. Support for users of the open source standard version will also be available.

Current licensees of jLock will be provided access to the source immediately. General availability of the open source version is planned before the end of 1st quarter.

Standards Update: The Future of CORBA®

CORBA/i and CORBA/e

The next generation of CORBA focuses on simplification and re-packaging for key market segments. The key elements aren't "new" so the maturity of implementations can be depended upon and leveraged, but these specifications represent a new, user-friendly and user-focused direction for CORBA standards. It is clear that middleware technology must be easier to understand, simpler to use and more manageable than is feasible with the current specification.

The specifications (currently in draft format) focus on maintaining the strength and maturity of business-critical features of CORBA technology while streamlining the specification to enable more sophisticated tooling and management capabilities.

This update acknowledges and directly addresses the increasing criticism by the analyst and user communities that CORBA has become "too complex." Like any mature technical solution, some of the features that "seemed like a good idea at the time," were never widely used. Other features, added for a niche market segment, bloated the entire specification making it difficult to understand.

Fortunately, the tremendous success of CORBA, as evidenced from the list of companies that have leveraged CORBA technology for business critical solutions, provides excellent "real-business" case studies for determining the features that can be culled from the core specification to simplify it without threatening its viability.

The new standards, code-named **CORBA/i** (for *Integration*) and **CORBA/e** (for *Embedded*), are the first in a series of profiles. They focus on the requirements of the integration and embedded CORBA markets respectively. The key features of the CORBA specification are retained in all profiles (e.g. IIOP).

A key goal of this profiling effort was to ensure that interoperability is not compromised between the profiles. For this reason, all the vendors met on several occasions to discuss the core features that all profiles must support. The draft specifications are the result of collaboration between 2AB, Borland, IONA, Fujitsu, HP, Prism Technologies and Objective Interface Systems.

This approach acknowledges the unique requirements of each market segment (vs. trying to continue a "one size fits all" brand for CORBA middleware).

The specifications (in pre-release format) are available via download to OMG members as the following document numbers. **CORBA/i** includes a single conformance point for *CORBA for Integration* and is document: **smsc/05-11-09. CORBA/e** includes the following two profiles: *A CORBA/e Minimal Profile Specification*: **realtime/05-11-03** and a *CORBA/e Reduced Profile Specification*: **realtime/05-11-02 smsc/05-11-05.**

2AB will deliver CORBA/i compliant releases of orb2 with tools that enhance the manageability and security of the runtime environment with easy-to-use development tools for building robust CORBA applications.

1700 Highway 31
Calera, AL 35040

Phone: 205-621-7455
Fax: 205-621-7455
E-mail: info@2ab.com
Support: support@2ab.com

2AB is a provider of Trusted Solutions for Distributed Business. 2AB offers the middleware, identity and access management tools needed by application developers to integrate systems and protect sensitive information from unauthorized access. 2AB is a business partner of IBM, Intel, HP, Sun, Microsoft and Stratus. The orb2 and iLock product suites are available for Java, Eiffel, C and C++ on AIX, HP-UX (PA-RISC and ia64), OpenVMS (ALPHA and ia64), Linux, Solaris, VOS, Windows and z/OS. Founded in 1997, 2AB is privately held.
For more information, please see http://www.2ab.com.