

TECHNOLOGY BRIEF

Connector Xpress and Policy Xpress | May 2010

CA Identity Manager: customization without coding

Accelerating time-to-value and lowering
total cost of ownership with Connector Xpress
and Policy Xpress

Bob Burgess
CA Security Management

we can



table of contents

executive summary

SECTION 1
Challenge **04**

The flexibility requirement **04**

SECTION 2
Solution **05**

Customization without coding **05**

SECTION 3
Conclusions **11**

Flexibility and lower cost **11**

SECTION 4
About the author **12**

executive summary

Challenge

An effective identity management solution should conform to the business' needs and not drive the business to support the solution. When well integrated with the business, these solutions are often complex, because of the business policies and processes they must support. Each organization has its own unique requirements. Implementing identity management requires nimble and flexible methods to interoperate between various systems and cooperate within current business processes. Flexibility has traditionally meant developers coding customized solutions or extensions to a commercial package, increasing the length and complexity of initial and ongoing deployments, as well as costs.

Solution

In addition to the traditional features expected in an “enterprise-class” provisioning solution, CA Identity Manager provides unique tools, Policy Xpress and Connector Xpress, that significantly reduce the time it takes to realize value from an identity management project, both early in the implementation and longer term for a lower total cost of ownership (TCO). These tools make it easy to create connectivity and integrate business logic without requiring coding, in essence delivering “customization without coding.”

Benefits

Customization without coding, delivered through Policy Xpress and Connector Xpress, can provide customers with significant and quantifiable savings. Savings increase as the number of applications or business policies being integrated increases. In one instance, a customer calculated that by using this functionality the organization could save 6,300 hours of development time to integrate the solution, compared to what they otherwise would have required with traditional code development. The projected savings amounted to over one million dollars and significantly accelerated project implementation.

Section 1: Challenge

The flexibility requirement

Business processes are complex and often require communication between the various systems and environments. Organizations need to be adaptable and nimble as they are constantly changing. These needs require organizational flexibility and with regard to computer systems mean custom code development is usually a part of the solution. There are two general categories that drive the need for customization as a part of identity management systems:

- Communicating with managed systems
- Implementing the organization's unique business logic or policies

Connections to managed systems

To provision and deprovision accounts within an organization, connections are needed to communicate with each endpoint, managed system, or application. CA Identity Manager provides a number of out-of-the-box (OOTB) connectors for managing endpoint systems like RACF, SAP, Salesforce.com, UNIX/LINUX, and SQL databases, just to name a few. These connectors provide bidirectional communication between CA Identity Manager and various third-party systems. However, these connectors deal with a finite set of endpoints and most organizations have not only these commercial solutions, but many "homegrown" or internally developed solutions as well. Connecting to internally developed systems is almost always a part of an identity management project. So connection options for these internal applications need to be available. In fact, organizations usually have many more custom applications than commercial applications which use OOTB connectors. Creating custom connectors is the first area where organizations find they need greater flexibility in implementing a functioning and manageable identity management solution.

Business logic implementation

The second area of needed flexibility occurs when an organization attempts to implement the business requirements into logic that a computer system can use. For example, when an operational manual states that "a manager must first approve an employee's access request and the change must be recorded for auditing," this must also happen within the provisioning system. To dynamically direct that business process properly, there must be computational or operational logic implemented somewhere. This requires more than just defining a workflow component within an identity management solution. It requires the ability to define business logic that extends beyond just a simple approval process. Business requirements come in all flavors and sizes, and to successfully implement that logic, an identity management solution must have great flexibility and adaptability.

High price of customization

This sort of flexibility usually drives the need for highly skilled developers who can code in JavaScript and Java to leverage an identity management solution's APIs. Without question, such manual coding provides complete flexibility; however, it also comes with a high total cost of ownership (TCO) and slow deployment or time-to-value. The coding option is expensive not only during the solution's implementation, but will continue to cause a negative impact to the solution cost for years into the future as business needs and product upgrades drive changes to the code.

Each time a change is needed a developer will need to find the source code, identify the needed code changes, and then implement those changes. Often the implementation of this coding change requires a complete system halt. System users must then wait for the identity management system to restart. Scheduling a change thus becomes an additional consideration. Hopefully, the developer will remember to update the source control repository with the code changes for future use. Many organizations have at least one “special” application that provides a mission-critical business function, where somewhere along the way the source code was lost or misplaced. The system continues to work, but nobody can change it, and all hope that it will continue to work is lost since there is no acceptable method to fix it except to rebuild the application. It is a very expensive and risky situation and occurs more often than many organizations are willing to admit.

Section 2: Solution

Customization without coding

Business requirements will continue to evolve; they are pushed by mergers, outsourcing, organizational realignments, and government mandates, just to list a few examples. An identity management solution has to provide enough flexibility to meet these ever-evolving requirements while doing so in a cost-effective manner. What if you could have both, flexibility with a lower TCO (compared to the added cost of manual development of connector and policy integration) and a solution that provided an accelerated time-to-value?

CA Identity Manager provides unique flexibility and functionality at a lower TCO compared with manual development by including two utilities:

- **Connector Xpress** Creates connections to manage target endpoint systems via SQL databases and LDAP directories
- **Policy Xpress** Creates complex business logic or policies without the need to develop custom code

Connector Xpress

Connector Xpress enables an organization to generate a fully functioning connector for custom applications using a series of simple wizard-based screens rather than by writing code. It enables connections between CA Identity Manager and SQL databases, and LDAP directories. Homegrown or internal applications, just like commercial packages, store user account credentials in a variety of repositories and the most common types are SQL databases and LDAP directories. As cloud computing expands, user credentials may be stored anywhere across the Internet, so web services is another important method for communicating with custom applications and accessing the appropriate user account repository.

Connector Xpress includes support for the following directories:

- CA Directory
- Sun One Directory
- Novell Directory

Connector Xpress includes support for the following databases:

- Oracle
- Microsoft SQL Server
- Ingres
- DB2
- DB2 for z/OS
- Sybase
- MySQL
- Informix

Figure A

Connector Xpress: mapping attributes

Connector Xpress provides a series of screens that an administrator uses to define the user account profile attributes to the custom application user repository (see images below). The attributes are “mapped” between CA Identity Manager and the managed system. Once defined, the connector is added to the available CA Identity Manager connectors.

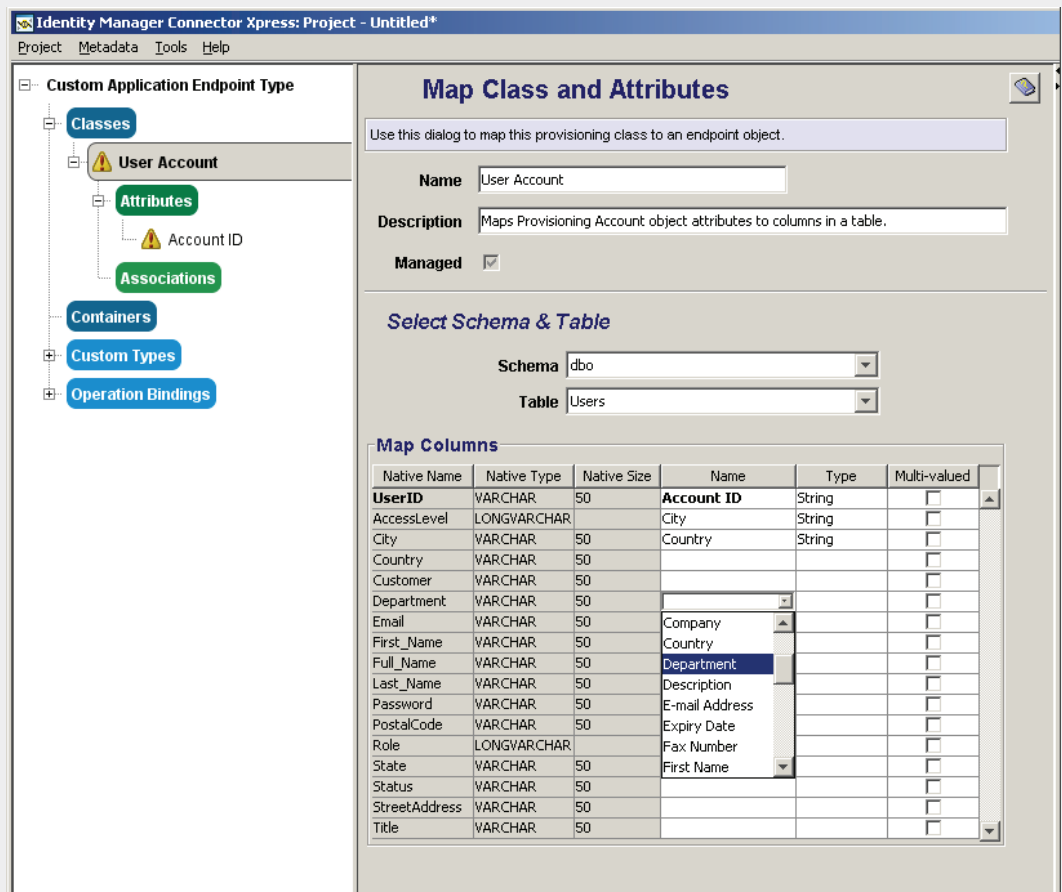


Figure B

Connector Xpress: mapping table columns

Experience with a number of customers has found that the time typically required to build a traditional custom connector (without Connector Xpress) can range from 4 to 6 or even as high as 8 weeks per application or endpoint system. Alternatively, experience with Connector Xpress finds that configuring a connector with this wizard-based tool can range from 1 to 2 weeks, saving between 3 to 6 weeks per connector. Whether organizations only want to integrate 2 or 3 homegrown applications, or as many as 10 to 20, the savings becomes substantial—both in costs in not requiring development processes and people as well as in time to get up and running and yield the value of increased reach and automation.

Connector Xpress requires no development of code, no maintenance of source code, and modifications can be easily performed in the future. It can integrate with multi-table database structures and stored procedures for a richer set of options. By design, Connector Xpress can keep versions of the connectors, and these definitions can be easily stored for quick recovery if needed. This may not replace the need for the occasional development of a custom connection to some archaic system that does use industry-standard storage mechanisms, but experience has shown Connector Xpress will address the majority of internally developed applications.

Map Columns

Native Name	Native Type	Native Size	Name	Type	Multi-valued
UserID	VARCHAR	50	Account ID	String	<input type="checkbox"/>
AccessLevel	LONGVARCHAR		City	String	<input type="checkbox"/>
City	VARCHAR	50	Country	String	<input type="checkbox"/>
Country	VARCHAR	50	Country	String	<input type="checkbox"/>
Customer	VARCHAR	50	User Name	String	<input type="checkbox"/>
Department	VARCHAR	50	Department	String	<input type="checkbox"/>
Email	VARCHAR	50			<input type="checkbox"/>
First_Name	VARCHAR	50	Custom Attribute...		<input type="checkbox"/>
Full_Name	VARCHAR	50	Multi Attribute...		<input type="checkbox"/>
Last_Name	VARCHAR	50	Account ID		<input type="checkbox"/>
Password	VARCHAR	50	City		<input type="checkbox"/>
PostalCode	VARCHAR	50	Company		<input type="checkbox"/>
Role	LONGVARCHAR		Country		<input type="checkbox"/>
State	VARCHAR	50	Department		<input type="checkbox"/>
Status	VARCHAR	50			<input type="checkbox"/>
StreetAddress	VARCHAR	50			<input type="checkbox"/>
Title	VARCHAR	50			<input type="checkbox"/>

Saving over one million dollars in development costs

In one example, a manufacturer of digital copying machines uses CA Identity Manager for its provisioning solution that includes 17 endpoint systems. Of these systems, 13 are custom applications. The identity management project manager determined that by using Connector Xpress he saved 6,300 hours that would have been required to create these custom connectors through “heads-down” code development. The bottom-line potential savings amounted to over one million dollars and significantly accelerated project implementation. Savings obviously vary depending on what number of applications are targeted; however, the more applications that are integrated and automated through CA Identity Manager, the greater overall value is realized by the organization.

Example 1: Provisioning to homegrown system

There are a myriad of custom or homegrown systems maintained by organizations. Often they support critical business processes and need to be incorporated into an automated provisioning solution.

As an example, Connector Xpress can create a connection to a homegrown storage resource management (SRM) system. The SRM system could have multiple user, group, and role tables hosted on an Oracle DBMS platform. These tables would contain the user account credentials and associate specific privileges for each user account. In order for an identity management solution to manage this system, at a minimum it must have read/rewrite access to these tables.

In this case, Connect Xpress, through a series of screens, can provide direct access by using the JDBC protocol to the needed table structure for this SRM system. Connector Xpress would then display, to the administrator defining the connector, the tables’ column attributes. It will provide easy mapping of the table columns to attributes used by CA Identity Manager for automated provisioning.

The administrator could optionally specify specific formatting or error checking of the data as well. Then, when the connection has been defined, the administrator adds this to the available connector list of the CA Identity Manager environment. This completed connector can then be used to automate the provisioning or deprovisioning of users to this SRM system. All of this can be done without writing development code or calling a programmer.

Connector Xpress enables your administrators to connect, without developing code, to most of your organization’s custom applications. As described above, it provides the ability to define and implement a custom connection within 1 to 2 weeks that typically could require 4 to 6 or even 8 weeks (hundreds of hours) of a developer’s time. That is flexibility and accelerated connectivity without coding.

Policy Xpress

Policy Xpress provides the ability to implement unique, complex business logic and policies without the need to develop custom code. An administrator using CA Identity Manager’s portal screens can configure a policy within Policy Xpress to implement even the most sophisticated business logic required.

What does this mean to the business? As business policies change, an administrator can modify the logic and policies using configuration screens within CA Identity Manager without requiring a developer to make underlying code changes, or more importantly—with proper change management procedures—without restarting the CA Identity Manager services. Policy Xpress is an integral component of CA Identity Manager.

Figure C

Policy Xpress: data element definition process

Policy Xpress provides a new paradigm for implementing business logic without developing code. A policy within Policy Xpress can be broken down to the following actions or steps:

1. **Gather and transform data** Define the variables that will be changed or viewed
2. **Create and execute rules** Determine when to execute the policy
3. **Perform actions at specified times** Execute the business logic or defined task at any point within the task

CA Identity Manager
Logged in as: *superadmin* (Logout) [Help](#)

Home Users Groups Roles and Tasks Endpoints Policies Reports System

Tasks

Create Policy Xpress Policy: *Base user name*

Profile Events **Data** Entry Rules Action Rules Advanced

Add Data Element

• = Required

- Name
- Category
- Type
- Function

Function Description
Sets a constant to be used for other data elements. Note: If you need to use values across policies, use a data element with a category of Variables.

Constant

The types of data that can be accessed in a policy include:

- Accounts
- Attributes
- Data sources
- System events
- Groups
- System roles
- System info
- Defined variables

The rules can be defined to match data based upon the following conditions:

- Equals
- Not equals
- Starts with
- Not start with
- Contains
- Not contains
- Ends with
- Not ends with

Policy Xpress gives you the ability to execute a policy at the following times relative to events (example, CreateUserEvent) within the system:

- Before
- Approved
- Rejected
- After
- Failed

Let's consider a couple of examples of how Policy Xpress helps with business logic within an identity management implementation. This is by no means an exhaustive list of possible uses for Policy Xpress, as there are many dozens of additional use cases that could be addressed.

Example 1: Write to an external store

During account provisioning, the new user ID or additional user metadata is often used by the application to authorize transactions that may also need to be written to an additional system or external store. This may be done to maintain legacy business policies or processes. Even though CA Identity Manager will create a user account on the managed system, there may also be an added step to record the authorization information for that user into another repository.

The traditional approach would involve using Java or JavaScript programming to implement this logic. The developer would have to figure out how to access the needed attributes which are available through native application APIs or the target application's framework. Once the details have been understood, development can commence with a cycle of code, test, debug, and finally deployment of the code. The developer ideally will also store the source code in a source code control system for future reference. This process stretches the timeline of the identity management system implementation process and adds an unknown risk factor to the effort that is easily misjudged and can drive up costs significantly.

Using Policy Xpress, an administrator can simply define a policy that is a part of the CA Identity Manager portal environment. This policy can gather the user's required account attributes from the policy screens, and then the administrator defines when the action should occur, such as during a "user create" event. Finally, the business logic of writing this user's ID or attributes to the appropriate database table is defined through a specified JDBC connection. Again, all of this is accomplished through the Policy Xpress configuration screens contained within CA Identity Manager, via point-and-click selection of items from drop-down lists and menus—not custom coding.

A slight variation of this example would be the need to perform an information look-up as part of provisioning a user account to a managed system. Perhaps the newly created account requires a department name attribute to be defined. If, as in this example, the department code lives on a tertiary system, this is easily obtained through a Policy Xpress policy which makes the request to the external system where the department code attribute is contained. This connection could be web services—based or even as simple as an LDAP (via JNDI) or SQL (via JDBC) query—once again, all done through point-and-click configuration—not custom coding.

Example 2: Business process chaining

In many organizations today IT as a service, or more specifically, Help Desk as a service is a key component of servicing change requests for users or consumers of IT and business services. Communication with a service desk application is often needed to generate a service ticket as a discrete step within the business logic of the provisioning process. With Policy Xpress, an administrator can define the attributes to be passed to the service desk application by selecting the items from a menu-driven portal screen. Then, the administrator needs to decide when this action should be executed, and, finally, configure the web service and appropriate methods to call and pass the relevant attributes. Without a capability like Policy Xpress, a developer would need to be involved in this process, adding additional risk, time, and cost to the implementation of the identity management solution

Both examples show that the required business logic can be integrated without writing code, without maintaining code and without the ongoing cost of code changes and longer-term impacts to upgradeability. This is a significant departure from most identity management solutions in the marketplace today.

Section 3: Conclusions

Flexibility and lower cost

Identity management solutions require the flexibility and adaptability to implement business logic and ensure connectivity to many different heterogeneous enterprise systems. In today's environments, nothing stays the same for long because of the dynamic and competitive nature of business environments and shifting government regulatory requirements. The end result: business systems must be changed, and the identity management solutions supporting these systems must ebb and flow to meet the demands of the business. This begs the question: "How can this be done quickly and in a cost effective manner?" Traditionally, hiring a team of local or offshore developers to write custom code was the default solution. However, this is costly in terms of both money and time and results in an inconsistent approach to supporting the business.

CA Identity Manager delivers significant, unique capabilities which mitigate these risks and costs. Connector Xpress and Policy Xpress provide connectivity and business logic without coding. This provides organizations a number of tangible benefits because there is no coding, no developers, and no ongoing code maintenance. These benefits include:

- **Expanding connectivity options** Connect to most/many of your internal or homegrown applications easily and quickly without development or custom code.
- **Removing the need for special development skills** An administrator can leverage the CA Identity Manager portal interface and configure clean, easily reconfigurable, upgradeable policies using a simple menu-driven point-and-click interface, enabling a faster time-to-value, or time-to-successful-implementation.
- **Eliminating code maintenance** No code maintenance is required, as the logic is implemented as a set of policies and behaves as a core part of the product's native functionality. Change is facilitated via configuration screens and stored in the native policy store to streamline the process and maintain consistent business logic during system upgrades.
- **Lowering initial and ongoing costs** An overall lower TCO for the organization is enabled by expediting the time it takes to implement the solution, expediting the time it takes to manage change to the solution, and expediting the time it takes to upgrade the solution as the vendor evolves the product over time.

These factors combine to enable organizations to remain highly flexible and adaptable to ever-changing business needs, and at a lower cost than without CA Identity Manager's Xpress tools.

Section 4

About the author

Bob Burgess is a Senior Principal Consultant and a member of CA's Security Center of Excellence team. His industry experience spans more than 20 years as a developer, technical evangelist, manager of a development team, and stints in product marketing and sales. Prior to this experience, Bob served 11 years (active and reserve duty) in the in US Air Force involved with future weapons systems at Strategic Air Command Headquarters and served, among other positions, as a Squadron Command. Bob has a Bachelor of Science in Computer Science in addition to a Bachelor of Science in Engineering Technology, both from Texas A&M University.

To learn more about the CA Identity Manager architecture and technical approach, visit www.ca.com/us/user-provisioning.aspx.

CA Technologies is an IT management software and solutions company with expertise across all IT environments—from mainframe and physical to virtual and cloud. CA Technologies manages and secures IT environments and enables customers to deliver more flexible IT services. CA Technologies' innovative products and services provide the insight and control essential for IT organizations to power business agility. The majority of the Global Fortune 500 rely on CA Technologies to manage their evolving IT ecosystems. For additional information, visit CA Technologies at ca.com.

