# How Cisco Enterprise Policy Manager Complements User Provisioning Products

## Introduction

In the past few years, many organizations have completed or initiated projects to deploy Identity and Access Management (IAM) technologies. The main focus has been on managing user identities – the creation and deletion, synchronization, provisioning, authentication, federation, and auditing of user accounts, attributes, and credentials.

These capabilities enable organizations to address the question of who is trying to access an application, data object, or network service. A critical gap, however, has been left unaddressed by IAM products – answering and enforcing whether a particular access request is entitled and therefore should be permitted. This second question is equally as important, if not more, than the first.

User-provisioning products, such as those offered by IBM, Oracle, Sun, and others, are used to manage the lifecycle of user identities, including adding and deleting users and user attributes (such as users' group memberships, locations, phone numbers, etc.). Administrators deploy provisioning products to synchronize or otherwise propagate user-related attributes that various applications require. Unlike provisioning products, enterprise-policy management products provide application-centric permissions (defined using role- and rule-based policies) which are evaluated based on off provisioned user attributes to enforce authorization policies at run time. Table 1 compares the capabilities of Cisco® Enterprise Policy Manager with provisioning products

**Table 1.** Comparison of Cisco Enterprise Policy Manager and User Provisioning Products

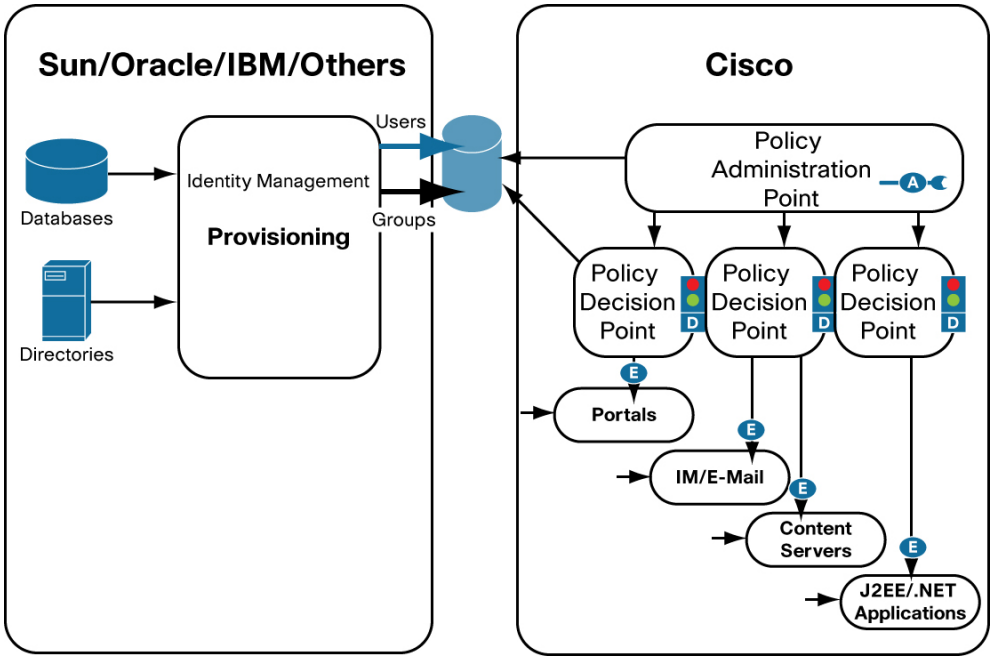
| | Cisco Policy Manager | User Provisioning Products |
|---|---|---|
| **Provision user accounts and attributes** | No | Yes |
| **Administer coarse-grained access policies** | Yes | No |
| **Enforce coarse-grained access policies** | Yes | No |
| **Administer fine-grained access policies** | Yes | No |
| **Enforce fine-grained access policies** | Yes | No |
| **Administer user (role, group, and attribute)-based policies** | Yes | No |
| **Administer resource-based policies** | Yes | No |
| **Provide workflow-based administration** | No | Yes |
| **Facilitate role-based policy expressions** | Yes | Yes |
| **Facilitate complex rule-based policy expressions** | Yes | No |
| **Audit access activity** | Yes | No |

Policy administration and enforcement associates users with resources by policy. Therefore, it is critically important to identify the optimal approach to integrate the user-provisioning solution with the enterprise-policy solution. This solution guide discusses the three most common approaches enterprises use to integrate Cisco Enterprise Policy Manager into their provisioning projects.

## Attribute-Level Integration Model

Provisioning products can manage user attributes stored in databases or directories. Attributes include information such as user groups or custom attributes identifying user location, contact information, etc. Typically, user attributes are created when a user joins, or otherwise forms a relationship with, the organization. Over time, user attributes change to reflect evolving responsibilities, and updated attributes are captured in the database or directory. Finally, when a user is terminated, attribute entries are deleted or marked as invalid in the directories and databases as summarized in Figure 1.

**Figure 1.** Attribute-Level Integration Model




From a policy-management perspective, all attributes managed by provisioning products act as authoritative sources of data referenced during policy resolution at run time. The provisioning product in this model is responsible for updating attributes to reflect user status, whereas the enterprise policy-management system is responsible for consuming this data for policy resolution. All enterprise policy-management policies are attribute-based. At run time, when a user accesses a protected resource, a policy that references one or more user attributes is evaluated.

Table 2 summarizes the responsibilities of various components in the overall solution.

**Table 2.** Responsibilities of Components in Attribute-Level Integration Model

| Function | Product or Component Satisfying Need |
|---|---|
| **User attributes** | Provisioning product |
| **Enterprise groups and roles** | Provisioning product |
| **User-group membership review** | Provisioning product |
| **Application resources** | Cisco Enterprise Policy Manager |
| **Application groups and roles** | Cisco Enterprise Policy Manager |
| **Run-time policy resolution** | Cisco Enterprise Policy Manager or natively by application |
| **Run-time policy enforcement** | Cisco Enterprise Policy Manager or natively by application (does not need to directly read provisioned attributes) |
| **Fine-grained policy entitlement review** | Cisco Enterprise Policy Manager |

### Benefits

Benefits of the Cisco Enterprise Policy Manager follow:

- Clear demarcation of responsibilities between Cisco Enterprise Policy Manager and provisioning products: Provisioning products simply manage user attributes, whereas Cisco Enterprise Policy Manager consumes these attributes during policy resolution.
- Loosely coupled solution that requires no custom adapters to specific provisioning products: Provisioning products simply write into directories or databases and Cisco Enterprise Policy Manager reads from these sources.
- User de-provisioning: User de-provisioning results in automatically revoked fine-grained entitlements because no user information or user ID is maintained in Cisco Enterprise Policy Manager.
- Policies: Cisco policies are rule-based and reference-provisioned attributes.

### Limitations

Limitations of the Attribute Level Integration Model follow:

- There is no visibility into user lifecycle events (such as adding or deleting a user) within Cisco Enterprise Policy Manager: Prefetching user policy decisions (or smarter caching) is more difficult.
- Changes in attribute values need to be reflected in the Cisco Enterprise Policy Manager attribute cache: Cisco Enterprise Policy Manager automatically registers callback handlers for tracking changed user attributes in the LDAP server but not from other sources (such as databases).

### Use Case

A large financial services institution decided to deploy IBM Tivoli Identity Manager (TIM) to provision users into Microsoft Exchange, Active Directory, SunOne LDAP, and several application user repositories. Application-level entitlements, however, required the definition of application-specific roles and policies that further required a resource model and fine-grained policies that were embedded into each application. For improved auditing and remediation, this customer externalized these entitlements from the application using Cisco Enterprise Policy Manager.

The security architecture required use of the provisioned attribute sources in policy resolution. Because enterprise groups and roles were defined and provisioned into a SunOne LDAP server, Cisco Enterprise Policy Manager was configured to use this repository as the attribute authority for user information needed for policy resolution. All role- and rule-based policies in Cisco Enterprise Policy Manager reference one or more user attributes managed in the SunOne LDAP. Cisco Enterprise Policy Manager stores no user ID or user-related information.

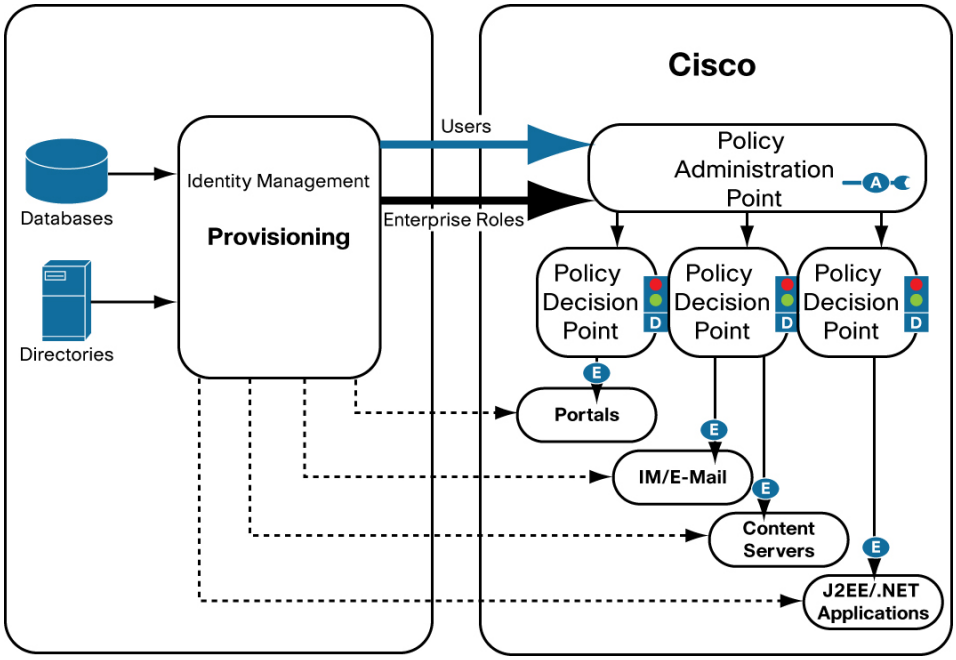
In this model, all 100,000 users are managed externally from Cisco Enterprise Policy Manager by IBM TIM. More than six attributes associated with users provisioned into SunOne LDAP are used for policy resolution. Attributes are configured to be cached in Cisco Enterprise Policy Manager with appropriate Time To Live values. All resources and application-specific policies (role- and rule-based) are managed within Cisco Enterprise Policy Manager by delegated administration.

### User-Level Integration Model

The drawback of the previous approach centers primarily around the lack of visibility of user identities within Cisco Enterprise Policy Manager. Awareness of users and their attributes is critical in certain scenarios where user IDs may need to be explicitly entered into the Cisco Enterprise Policy Manager repository. The following are a few scenarios where Cisco Enterprise Policy Manager requires real-time visibility of user accounts and attributes:

- Users are explicitly assigned application-specific roles or resources (rather than by rules).
- Users need additional application-specific attributes that are not suitable for storing in enterprisewide directories.
- There is a requirement to pre-fetch and cache user decisions when a user is added or if user attributes change.

**Figure 2.** User-Level Integration Model




To accommodate these requirements, organizations must provision user accounts (and optionally attributes, groups, roles, etc.) into the Cisco Enterprise Policy Manager repository. You can do this by using a provisioning database adapter to populate the appropriate tables, or by using a Services Provisioning Markup Language (SPML) interface to Cisco Enterprise Policy Manager. In addition, you need to develop workflow tasks (for example, adding, modifying, and deleting) within the provisioning system to help ensure that changes to users, attributes, and roles in the authoritative data sources are propagated to the Cisco Enterprise Policy Manager repository.

Table 3 summarizes the responsibilities of components involved in the user-level integration model.

**Table 3.** Responsibilities of Components in User-Level Integration Model

| Function | Product or Component Satisfying Need |
|---|---|
| **User attributes** | Cisco Enterprise Policy Manager or provisioning product |
| **Enterprise groups and roles** | Cisco Enterprise Policy Manager or provisioning product |
| **User-group membership review** | Cisco Enterprise Policy Manager |

| | |
|---|---|
| **Application resources** | Cisco Enterprise Policy Manager |
| **Application groups and roles** | Cisco Enterprise Policy Manager |
| **Run-time policy resolution** | Cisco Enterprise Policy Manager or natively by application |
| **Run-time policy enforcement** | Cisco Enterprise Policy Manager or natively by application (does not need to directly read provisioned attributes) |
| **Fine-grained entitlement review** | Cisco Enterprise Policy Manager |

### Benefits

Benefits of this model follow:

- Integration between Cisco Enterprise Policy Manager and the provisioning solution is direct, ensuring user accounts, attributes, and role mappings are automatically provisioned into the Cisco Enterprise Policy Manager repository. The workflow engine of the provisioning-system detects any changes to authoritative user data and subsequently updates the Cisco Enterprise Policy Manager repository.
- Enterprises can include optional approval and notification processes in the provisioning workflow to help ensure that changes are properly vetted before they are provisioned to the Cisco Enterprise Policy Manager repository.
- Because administrators provision users, attributes, and roles, no run-time user lookups or dynamic rules are required to evaluate policies. This scenario allows for optimal use of the caching and prefetch capabilities of Cisco Enterprise Policy Manager that enhance performance and scalability.
- User management and policy management within Cisco Enterprise Policy Manager is simplified. The provisioning integration removes the need for an administrator to manage (for example, create, update, or delete) user accounts or handle user-to-role mappings.

### Limitations

Limitations of this model follow:

- Custom development is required to build provisioning adapters and workflow tasks.

### Use Case

A large manufacturer deployed Sun Identity Manager and decided to directly integrate the provisioning system with the Cisco Enterprise Policy Manager in order to streamline user and policy management as well as optimize performance.

As users are added to the authoritative data source (for example, the human resources system) in the enterprise, Sun Identity Manager automatically creates accounts in Cisco Enterprise Policy Manager and maps those accounts to default roles based on attributes such as location, department, and job function. When a user’s attribute changes (for example, job title or department) in the authoritative data source, the provisioning system initiates workflow tasks that update the user’s role mappings within the Cisco Enterprise Policy Manager repository. The provisioning system obtains the appropriate approvals before role changes are provisioned to Cisco Enterprise Policy Manager. When users are terminated in the authoritative data source, the provisioning system de-provisions the accounts in Cisco Enterprise Policy Manager.

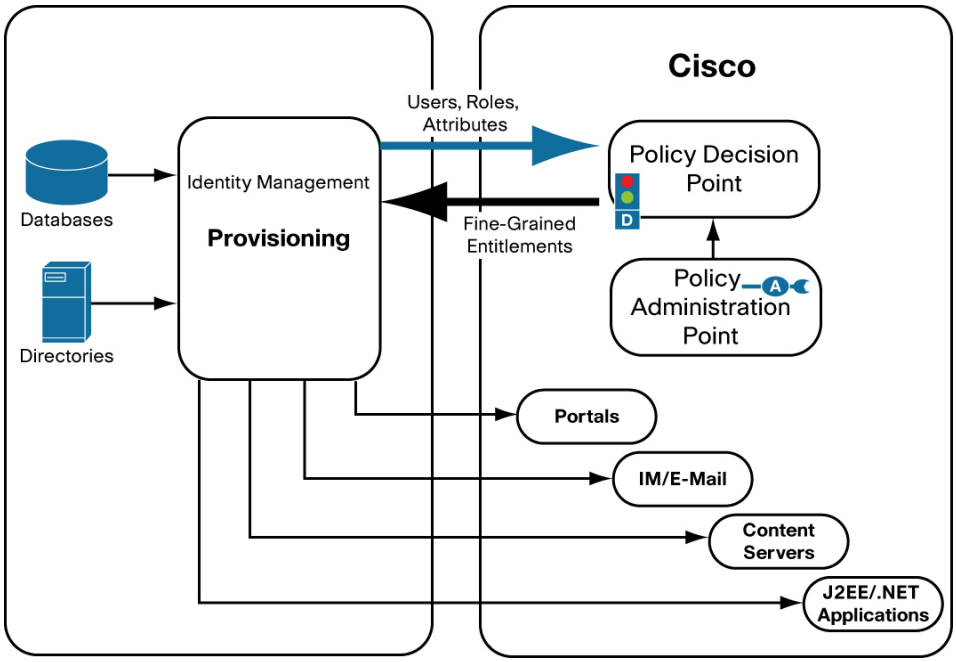
Provisioning of users, attributes, and role mappings allows for optimal use of the caching and prefetch capabilities of Cisco Enterprise Policy Manager. Unlike the attribute-level integration, Cisco Enterprise Policy Manager does not need to perform dynamic LDAP lookups at run time to collect user attributes or determine group membership in order to evaluate policies. The user-level model provides simple, drag-and-drop assignment of role-based policies.

### Policy-Level Integration Model

The user-level integration model described in the previous section provides centralized visibility and control over policies with distributed enforcement. This approach works in most scenarios, but in the following cases a third model might be preferable:

- There is a lack of easy integration points for Cisco Enterprise Policy Manager to protect legacy applications.
- Provisioning adapters have been developed for many repositories that need to be provisioned and the development of Cisco Policy Enforcement Points for the same resources is not feasible or desirable.
- Enterprises want to take full advantage of its investment in a provisioning product with its capability for rollback, attestation, and workflow processes.

**Figure 3.** Policy-Level Integration Model




In this integration scenario, entitlement policies are administered, resolved, and monitored in the Cisco Enterprise Policy Manager platform, whereas the provisioning solution distributes the entitlement decisions to the applications for enforcement through native mechanisms that exist within those resources (for example, access control lists [ACLs]). Unlike the user-level integration model described previously, there is a two-step process for integration between the provisioning product and Cisco Enterprise Policy Manager:

1. The provisioning system sends user-role, attribute, and group information to Cisco Enterprise Policy Manager through a provisioning adapter (as in the user-level integration model).

2. Cisco Enterprise Policy Manager resolves the policies and sends the decisions in the form of a user-, group-, or role-based ACLs to the provisioning solution, which then takes this list of fine-grained entitlements and provisions it to the protected applications using the same adapters that provision users into those applications.

In this model, Cisco Enterprise Policy Manager does not enforce the entitlement policies at run time. Companies can take full advantage of their investments in provisioning adapters while still getting centralized visibility and control over fine-grained entitlement policies.

Table 4 summarizes the responsibilities of components involved in the policy-level integration model.

**Table 4.** Responsibilities of Components in Policy-Level Integration Model

| Function | Product or Component Satisfying Need |
|---|---|
| **User attributes** | Cisco Enterprise Policy Manager or provisioning product |
| **Enterprise groups and roles** | Cisco Enterprise Policy Manager or provisioning product |
| **User-group membership review** | Cisco Enterprise Policy Manager or provisioning product |
| **Application resources** | Cisco Enterprise Policy Manager |
| **Application groups and roles** | Cisco Enterprise Policy Manager |
| **Run-time policy resolution** | Natively by application |
| **Run-time policy enforcement** | Natively by application |
| **Fine-grained policy entitlement review** | Cisco Enterprise Policy Manager |

## Benefits

Benefits of this model include all of the benefits of the user-level integration model plus the following:

- This model takes advantage of the synergistic strengths of user management and adapters in provisioning products, and the enterprise policy and fine-grain policy visibility provided by Cisco Enterprise Policy Manager.
- This model takes advantage of the approval, workflow, attestation, and rollback capabilities built into provisioning systems. Although Cisco Enterprise Policy Manager has many of these capabilities, being able to use a common workflow and attestation process for user elements as well as entitlements can lead to improved consistency and accuracy in policy resolution.
- Enterprises gain the benefits of Cisco centralized policy management across a broad set of legacy applications that provisioning products are already integrated with, without requiring a great deal of incremental effort.

### Limitations

Limitations of this model follow:

- Run-time policy enforcement occurs natively within the application, and applying contextual policies requires writing code into each application, leading to duplication of code and complicating audit and remediation.
- This model does not address the need to eliminate or externalize custom code that uses this entitlement data for run-time resolution and enforcement.

- This model has no consolidated activity logs. Because each application natively enforces the entitlement policies, there is no centralized visibility of the access attempts, failures, and successes across multiple resources.

**Use Case**

A large pharmaceutical manufacturer has deployed Oracle Identity Manager and integrated it with all of its applications and resources, including older systems. The company then decided to purchase Cisco Enterprise Policy Manager and wants to rapidly deploy the solution for centralized policy management and resolution in order to meet a pending compliance deadline.

As users are added to the authoritative data source (for example, the human resources system) in the enterprise, the provisioning system automatically creates accounts in the Cisco Enterprise Policy Manager and maps those accounts to default roles based on attributes such as location, department, and job function. When a user's attributes change (for example, a change in job title or department) in the authoritative data source, the provisioning system initiates workflow tasks that update the user's role mappings within the Cisco Enterprise Policy Manager repository. Before role changes are provisioned to the Cisco Enterprise Policy Manager, the provisioning system obtains the appropriate approvals. When users are terminated in the authoritative data source, the provisioning system de-provisions the accounts in Cisco Enterprise Policy Manager.

Administrators model the resources and policies in Cisco Enterprise Policy Manager and the system then resolves those policies based on the user accounts and attributes that Oracle Identity Manager provisioned into the Cisco Enterprise Policy Manager repository. The resulting entitlements are then sent back to Oracle Identity Manager for propagation to the target applications. For highly sensitive resources, Oracle Identity Manager can apply additional workflows or approvals on the entitlements prior to distributing them. When users make requests for a resource, the entitlement policies are enforced natively by the application.

## Conclusion

User-provisioning systems are a critical component in any IAM infrastructure, but they do not provide all of the capabilities required for managing fine-grained entitlements to enterprise applications and data. Cisco Enterprise Policy Manager complements and enhances provisioning deployments by adding a layer of centralized policy management that delivers complete control and visibility over users' access to sensitive resources. Cisco Enterprise Policy Manager has been integrated with leading provisioning products from IBM, Oracle, Sun, and others to deliver three deployment models, which are optimized to meet different enterprise requirements. For more information about Cisco Enterprise Policy Manager and how it complements provisioning systems, contact your Cisco account executive or visit http://www.cisco.com/policy

**Americas Headquarters**
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

**Asia Pacific Headquarters**
Cisco Systems (USA) Pte. Ltd.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

**Europe Headquarters**
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.



Printed in USA C22-449801-00 02/08