

COSuser interactive TKB

The Interactive TKB (*i*TKB) for COSuser is employed during the early stages of project implementation to bypass delays in building automatic TKBs that will form the final configuration, and to work in place of automatic TKBs where they are either too expensive or impractical to construct.

Software for User Provisioning, an activity which is a subset of Identity Management, is now generally accepted as being a proven technology. It provides a significant return on investment (RoI), improves service levels, increases security, assists auditing and contributes greatly towards legislative compliance.

Implementation is, however, a non-trivial undertaking, with typical timescales ranging from 12 to 18 months to completion. When the main business driver is to meet an urgent requirement for an audit, or to achieve legislative compliance, this may be unattractive. The *i*TKB provides user organizations with a solution to the problem of how to quickly establish, in an audited and controlled manner, a record of where all employees and contractors have user accounts.

In the implementation of a user provisioning solution, the installation of Target Knowledge Bases (TKBs, or Connectors in industry jargon – modules that concentrate the knowledge of how to automatically provision users on an operating system or application) is a major factor in the length of time taken. The TKB has to be installed, if available, or developed if not (most large organisations have a number of applications which are home grown or which are not catered for by the vendor),

policies need to be defined and agreed, and existing user information has to be imported, cleaned and linked with the authoritative data source, all before the benefits may be experienced. For an enterprise with hundreds of applications it can be a time-consuming, although eventually worthwhile, task.

Recent legislation, such as Sarbanes-Oxley and the similar European directives, establishes deadlines for enterprises who must

prove due diligence in restricting access to critical data to be fully compliant. The problem is therefore how to obtain the audit and control benefits of user provisioning in a timely manner, without having to wait for full automation in order to be productive.

The *i*TKB is one answer to this problem. In the absence of user provisioning software, the task of registering and de-registering users will often fall to the experts on each element of the computing infrastructure.

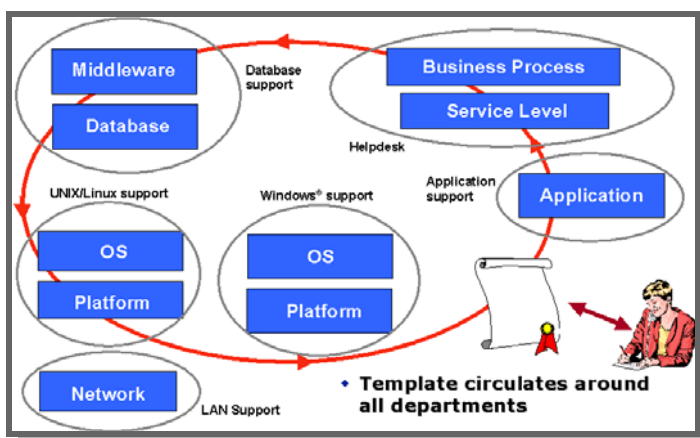


Figure 1 – Illustration of the complexity of adding a single new user to an enterprise IT service

For example, DBAs perform user administration tasks for databases, UNIX administrators for UNIX, Windows Administrators for MS Windows etc. A request to add a new user needs to pass through all such departments and each expert or system administrator must do their bit to register the user on the software for which they are responsible.

The job of *automatic* TKBs or Connectors is to render this process automatic through centralized administration but, as we learned above, it takes time to implement them. In contrast, the *ITKB* can provide a means to quickly establish control by leveraging the existing set-up for manual provisioning while the automation elements are being commissioned. In doing so, the *ITKB* provides a single database specifying where all employees and contractors have their user accounts, a fundamental requirement for auditors and compliance. It does so with full auditing of how those accounts were established.

Once the initial authoritative source of users has been established within the *COSuser* repository (perhaps by the importing of data from the HR system, a directory or metadirectory), the *ITKB* can be set up – in a matter of days rather than months – for every element of the infrastructure that needs to be provisioned with user information.

Information regarding users is input into *COSuser* in the same way as if the infrastructure elements were being provisioned automatically *i.e.* a user's information is input centrally and the roles relating to their access rights are assigned. When the roles are expanded by the *COSuser* Transaction Engine they are split into those that can be carried out by the automatic TKBs/Connectors already installed, and those for which there is no installed TKB/Connector. In the former case the user is registered/deregistered/changed automatically and, in the latter case, the *ITKB* is called.

Where the transactions are routed to the *ITKB*, the group of administration staff who are responsible for the registration of users on that target application are informed by email of the requirement to perform a user registration task, and are provided with a URL to obtain the relevant information. The information is presented as shown below, although the look and feel of the web browser interface is normally modified to reflect the organization's Intranet standards.

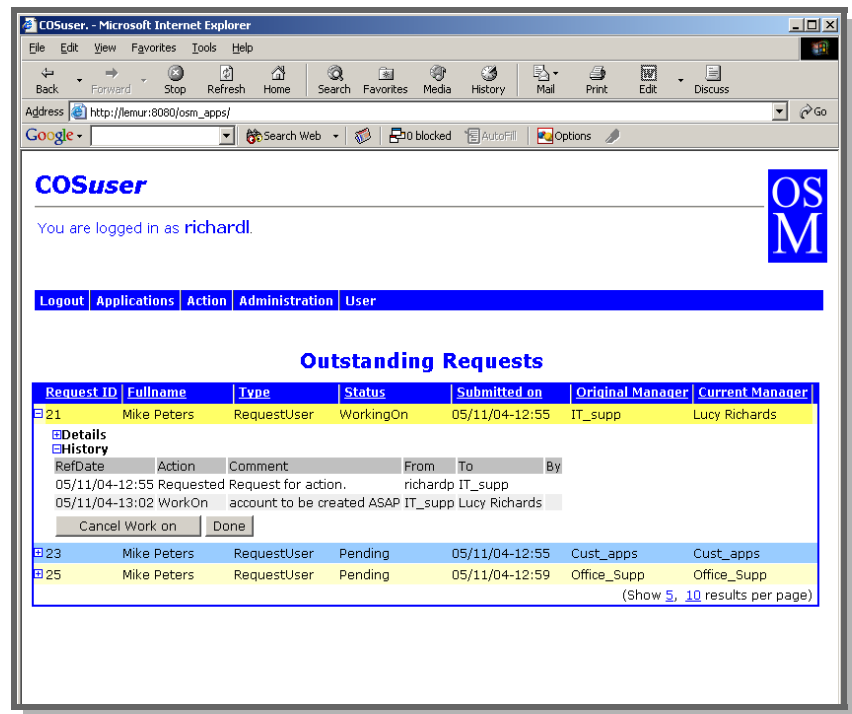


Figure 2 – a list of outstanding requests as viewed by an administrator

The information provided enables the administration group to provision the user or to reject the request, along with a reason for doing so.

As a task is normally assigned to a group of administrators rather than an individual for purposes of workload balancing and resilience, individual members of a group can take ownership of a transaction to prevent duplication of effort. Once completed the administrator confirms via the URL that they have performed the requested task. The administrator may also enter any additional information that they consider relevant, such information being logged in the audit trail for the transaction.

As a result of the executed task, the central *COSuser* repository of user information is updated to show that the account exists in the same way as if it had been provisioned automatically. The account's

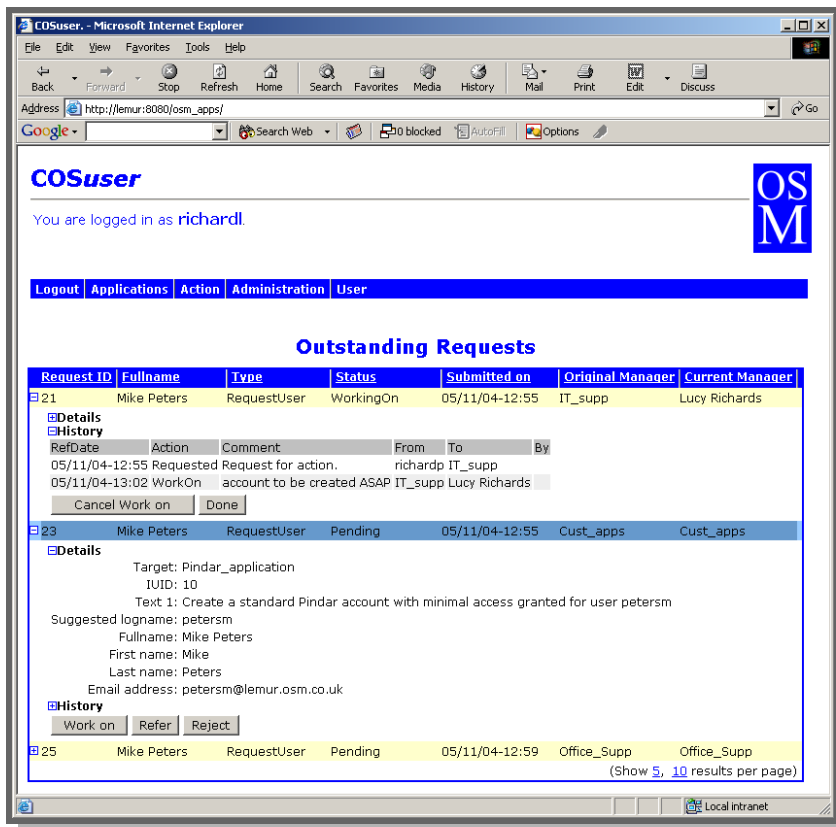


Figure 3 – details of a request as seen by an administrator

existence is noted under the heading of Interactive User Provisioning Accounts to distinguish those that have been provisioned manually. An example of a report generated

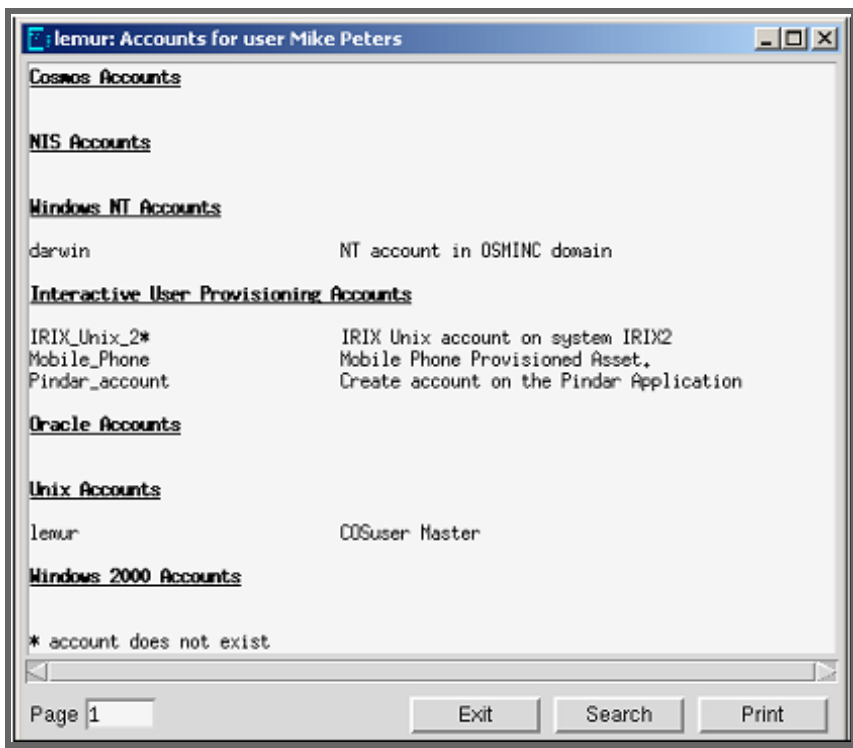


Figure 4 – report of accounts for a specified user

from COSuser for a particular user is shown below.

As can be seen on the report, this user (Mike Peters) has a Windows NT account on *darwin*, and a UNIX account on *lemur*, both of which have been provisioned automatically. He also has an account on an application called *Pindar* and a mobile phone, both of which have been provisioned interactively and confirmed. An account on a Silicon Graphics Irix system has been requested but not yet confirmed (indicated by the '*' next to the name of the account).

In addition to the database update, all other activity is audited so that, for example, a record is kept that a particular administrator manually registered Mike Peters on the *Pindar* application at a particular time and date. The audit trails are kept with all the other COSuser audit trails and follow the same format.

One main benefit of using the *iTKB*, therefore, is that a central repository of all users, and the accounts they have, can be established without having to wait for automatic TKBs/Connectors to be designed, developed and rolled-out. It is this central updating of the user repository which differentiates the *iTKB* from just a web based workflow tool.

The *iTKB* can be replaced over time as automatic TKBs/Connectors take its place, but it is likely to remain in place to provision a number of applications that do not lend themselves to automation. This group includes those that have neither a Command Line Interface nor API for user administration, and those where the transaction volumes (in terms of users), cost of development or concerns about lack of security make it unjustifiable to provision automatically.

The *iTKB* is also used where physical

and other assets may need to be provisioned. When a user joins the organization, he/she needs access not only to applications but to other tools to do his/her jobs – physical assets such as PCs or mobile phones, and non-physical assets such as telecoms links or access passwords to the office security system. The allocation of these assets may all be controlled by the ITKB as can their reclamation when an individual leaves the organization. At least one major financial institution believes that it has already recovered its investment in user provisioning by the recovery of physical assets from its leavers.

Summary

The ITKB may be used in a number of different ways:

- to quickly establish a central repository of user

information to meet audit and legislative compliance requirements prior to automation

- to provision users on applications where there is no way of automating user registration or passwords e.g. where the only means of applying user information is interactive
- to provision users on applications where the return on investment (RoI) for automating user registration is poor
- to provision users with material and non-material assets such as mobile phones, laptops, desks or a home telephone account

For more information please visit:

www.cosuser.com



www.cosuser.com

www.osmcorp.com

OPEN SYSTEMS MANAGEMENT, INC.

1511 Third Avenue, Suite 905
Seattle WA 98101
USA

Tel: (866) 601 8011 (toll-free, USA)
Fax: (206) 583 8374
info@osminc.com

OPEN SYSTEMS MANAGEMENT LTD

Kings Ride Court
Kings Ride
Ascot, Berkshire SL5 7JR
UK

Tel: +44 (0)1344 638000
Fax: +44 (0)1344 638011
info@osm.co.uk