August 2005

SAP User and Access Management with Microsoft Identity Integration Server

Authors

Rüdiger Berndt, IdM Lead Architect, Oxford Computer Group Ltd.,
Ruediger.Berndt@oxfordcomputergroup.com
James Cowling, IdM Lead Architect, Oxford Computer Group Ltd.,
James.Cowling@oxfordcomputergroup.com

Co-Editors

Tilo Böttcher, SAP Program Managers CTSC, Global SAP Alliance, Microsoft
Jürgen Daiberl, SAP Program Managers CTSC, Global SAP Alliance, Microsoft
André Fischer, Project Manager CTSC, SAP AG

Summary

This paper provides information about how to centralize user identity and access management for SAP systems using the Microsoft Identity Integration Server and Active Directory products.

Microsoft

OXFORD COMPUTER GROUP

SAP

Applies to

- Microsoft Identity Integration Server (MIIS)
- Microsoft Visual Studio .NET 2003
- Microsoft .NET Framework 1.1
- NetWeaver 04 Stack 4
- SAP R/3 (4.X)
- SAP HR & EP
- Oxford MIIS Management Agent for SAP

Keywords

Identity Management, MIIS, ADAM, Central User Management, SAP Integration

Level of difficulty

Technical consultants, Solution Architects, Developers

Contact

This document is provided to you by the Oxford Computer Group Ltd. and the Collaboration Technology Support Center Microsoft, a joint team from SAP and Microsoft that drives interoperability.
For feedback or questions you can contact the Oxford Computer Group Ltd. at info@oxfordcomputergroup.com the CTSC at ctsc@sap.com or ctsc@microsoft.com. Please check the .NET interoperability area in the SAP Developer Network (http://sdn.sap.com) and at the Microsoft-SAP Alliance web site (http://www.microsoft-sap.com) for any updates or further information.

Microsoft

OXFORD COMPUTER GROUP

SAP

This document is a common publication by SAP and Microsoft ("Co-Editors") who have both contributed to its content and retain respective rights therein.

The information contained in this document represents the current view of the Co-Editors on the issues discussed as of the date of publication. Because the Co-Editors must respond to changing market conditions, it should not be interpreted to be a commitment on the part of the Co-Editors, and the Co-Editors cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. NEITHER OF THE CO-EDITORS MAKES ANY WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of the Co-Editors.

Either Co-Editor may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from the respective Co-Editor(s), the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

Unless otherwise noted, any example companies, organizations, products, domain names, e-mail addresses, logos, people, places and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, email address, logo, person, place or event is intended or should be inferred.

Contents

Microsoft

OXFORD COMPUTER GROUP

SAP

Introduction

Many organizations are increasingly considering consolidating and integrating their user management systems into one central system, helping reduce operational and helpdesk costs, while addressing overall security concerns of managing identities and access rights.

Microsoft Identity Integration Server (MIIS) 2003 is a centralized service that stores and integrates identity information for organizations with multiple directories. MIIS provides organizations with the capability to manage these directories automatically, based on an authoritative source – the typical authoritative source being an HR system such as mySAP ERP Human Capital Management (HCM).

In addition to the employee data held in an SAP HCM System, SAP Web Application Server (WAS)-based systems (i.e. R/3, BW, etc.) also contain separate user information that is often, but not always, consolidated through the SAP Central User Administration (CUA). While the HR data is commonly useful as a source for user objects managed centrally by MIIS, the SAP R/3 systems are more typically a "target" for provisioning of user identity data – i.e. the SAP R/3 users should be automatically created and removed based on the presence or absence of an "employee" in the HR system.

This paper provides a description of the two scenarios described above, plus an approach for password synchronization. The diagram below summarizes the relationships between the systems in an ideal identity management solution.

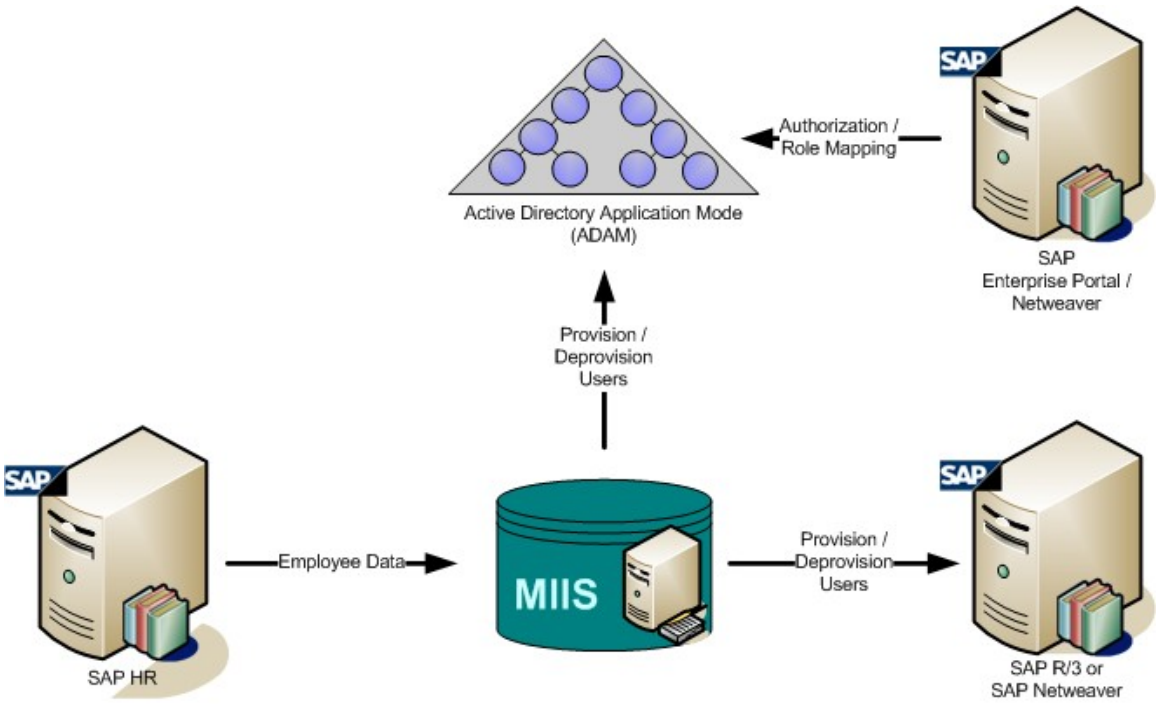


Figure 1 - Interconnection of SAP systems with MIIS

Architecture

Interface Architecture

There are several methods for connecting or integrating with SAP back-end systems. At the time of writing, the following connection methods were considered useful in the context of identity management solutions:

- via Business Application Programming Interfaces (BAPI) and Remote Function Calls (RFC)
- via SAP WAS (CUA) LDAP integration to/from Active Directory or Active Directory Application Mode (ADAM)

This paper will describe the approaches for using both of the connection methods above.

BAPI and RFC Integration

Oxford Computer Group (Oxford), an MIIS integration specialist, developed a .NET-based MIIS Management Agent for SAP using BAPIs and RFC, which has been deployed in production at various large customer sites. In this solution, MIIS reads and writes user, employee and organizational information through BAPIs and RFC, communicating with both SAP HR and SAP R/3 systems.

Microsoft has also planned to release a native MIIS Management Agent for SAP. This management agent was not available at the time this document was written, so it is not covered further in this document. Since the methods of integrating with SAP systems are similar, the functionality is also expected to be similar as what is outlined in this paper.

SAP WAS LDAP Integration with Active Directory/ADAM

While the Oxford approach is rich in functionality; it is also worth mentioning a solution using “out of the box” components from SAP and Microsoft, which represents a cost-effective solution in simple or more homogeneous environments. In this solution, the SAP CUA reads user information from ADAM or Active Directory using SAP WAS (CUA) replication and updates SAP users in multiple target SAP R/3 systems. In the classical MIIS context, the information in ADAM is provided by MIIS from an authoritative HR source.

In cases where only Active Directory or ADAM is used for integration (i.e. no direct BAPI integration with SAP), the Identity Integration Feature Pack from Microsoft can be used instead of the MIIS Enterprise Edition, potentially helping save some licensing costs.

The Oxford MIIS Management Agent for SAP

Supported Scenarios

The Oxford MIIS Management Agent for SAP can be used in the following situations:

- Reading employee data from the HCM System
- Reading organizational structure from various SAP modules
- Synchronizing users into SAP R/3 systems
- Resetting and changing passwords in SAP R/3 systems

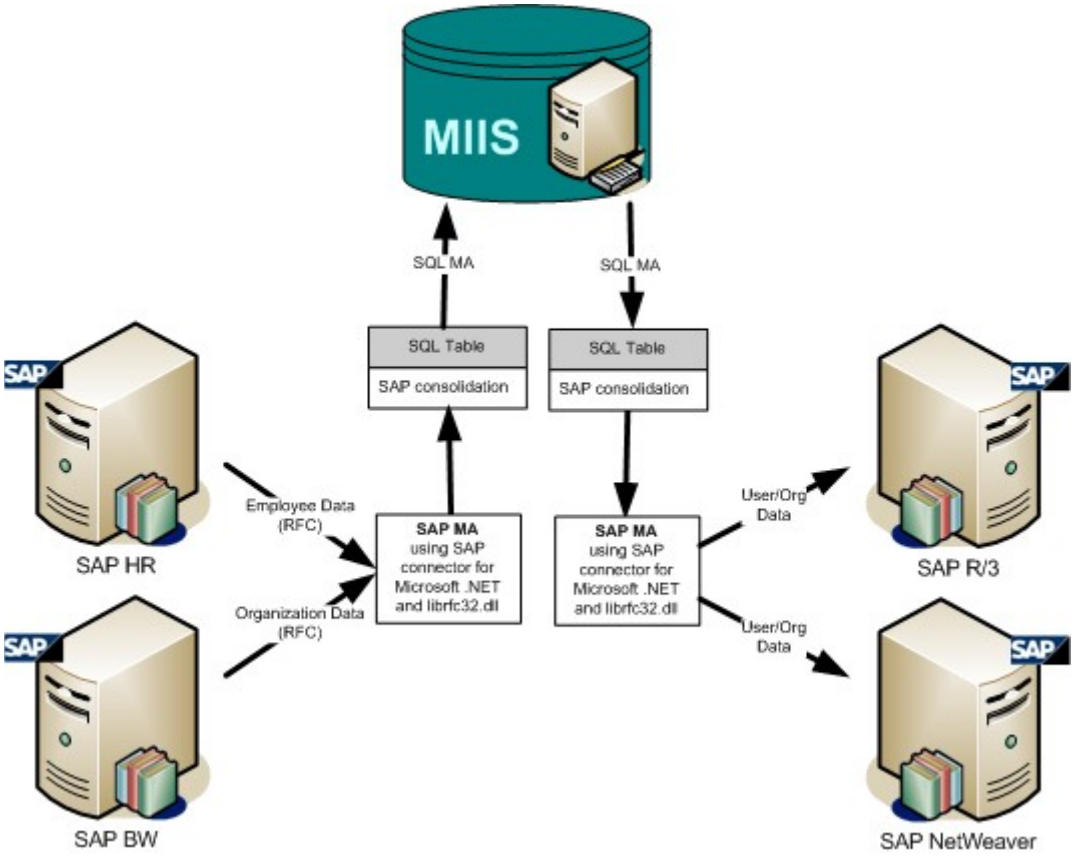


Figure 2: Architectural overview SAP Business Systems Access via OCG MA for SAP

The management agent supports access via BAPIs or Intermediate Documents (IDoc) and uses the SAP connector for Microsoft .NET 2.0. The BAPIs can be either standard or custom, and depending on the BAPI being used, delta imports are possible – i.e. only the changes made in SAP HR since the last import are read and processed by MIIS.

The management agent (MA) supports consolidation of data in multiple clients, modules, systems and languages. The consolidation of data from multiple clients is particularly significant when references are made between identities in different clients – for example, if an individual, stored in one SAP client, has a manager in a different SAP client. To maintain the reference attribute for use in a target directory (e.g. AD's *manager* attribute), the reference must be read by the same Management Agent from both of the SAP clients in the same MA synchronization run.

The data consolidation is performed with one or more Microsoft SQL Server database tables as the target. For performance reasons, it can be advantageous to use multiple tables, allowing the separation of static data from more dynamic data, so that updates can be accelerated. This is not required, however – multiple management agents for SAP can update a single table.

The architecture allows scaling of the solution: the SAP connector for Microsoft .NET components do not need to run on the MIIS server, and multiple SAP connector for Microsoft .NET components can be running simultaneously. This means that a large number of SAP systems can be connected, with no need for additional MIIS servers or

agents. MIIS sees a single, consolidated HR source, and reads this data using a standard SQL Management Agent.

Connecting MIIS via CUA Replication

Supported Scenarios

The CUA replication solution can be used in the following situation:

- Synchronizing User Accounts into SAP R/3 systems with CUA

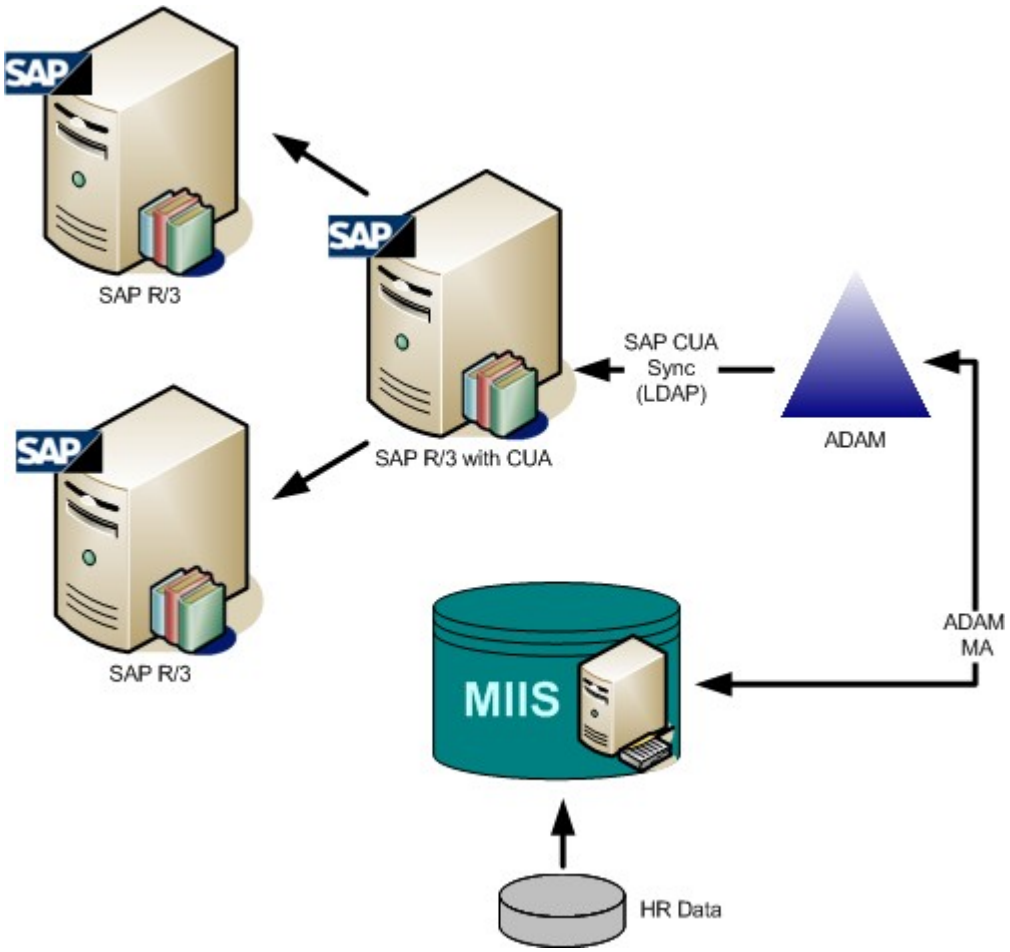


Figure 3: Overview SAP back-end systems Access via AD Agent and SAP CUA LDAP replication

SAP CUA Replication offers support for many directories including Active Directory (Windows Server 2000 or 2003) and ADAM. One of these directories can be used to exchange standard user attributes such as name, e-mail, telephone number, roles, etc. from MIIS into the SAP back-end systems. Because ADAM is a lightweight directory (LDAPv3) with a cost-effective licensing requirement of the standard Windows Server client access license, which many organizations already have, it is a common intermediate directory used with MIIS. For brevity, we will discuss the implementation of an ADAM-based solution - integration with Active Directory is almost identical.

In addition to the standard SAP configuration steps required to configure ADAM synchronization with SAP back-end systems, the following steps are required on the MIIS side:

- Identify and, where necessary, create appropriate attributes in the MIIS Metaverse to store SAP-specific attributes
- Create a Management Agent for the ADAM system
- Define attribute flows to the ADAM SAP specific attributes from the MIIS Metaverse, so that the required values can be retrieved by the SAP CUA from ADAM

Summary of Functionality

The following table summarizes the functionality available within the two connectivity solutions mentioned above:

Feature	Oxford BAPI-based MA for SAP	CUA Replication via AD/ADAM
Read Employee Identities into MIIS from SAP HR	✓	✓ (*)
Write back to SAP HR (e.g. email addresses)	✓	
Write Users into SAP R/3	✓	✓
Manage SAP R/3 user roles	✓	✓
Read Organizational Structure	✓	
Consolidate data from multiple SAP Clients to MIIS	✓	
Synchronize Passwords into SAP R/3	✓	

(*) AD/ADAM can be provisioned and updated using the SAP HR LDAP interface as described in the collaboration brief *Creating Users in Active Directory from Employee Data Stored in SAP HR*.

Administration of Role-Based Authorization

SAP systems use Roles extensively for authorization purposes. The challenge in an Identity Management solution is to assign these Roles automatically, rather than relying on potentially error-prone (and costly) manual administration. This role assignment is usually based on information (such as job title) extracted from an HR system – the solution discussed previously described this type of HR data extraction.

In order to automate the assignment of roles in target SAP R/3 systems, the MIIS integration requires a means of identifying which roles in the R/3 system are related to which job titles from the HR system. This mapping is carried out by means of a mapping table in the SQL server of the MA for SAP, and results in a value for each target system with the format “Subsystem:Rolename”.

The final element of the solution is to deliver these values to the target systems. Here, we discuss the process when a SAP CUA is involved, which automates the distribution of the role information on the SAP side.

It is also possible to perform this distribution directly to each target systems using a BAPI-based management agent, such as the Oxford solution described above.

The architecture of the CUA-based solution is shown below:

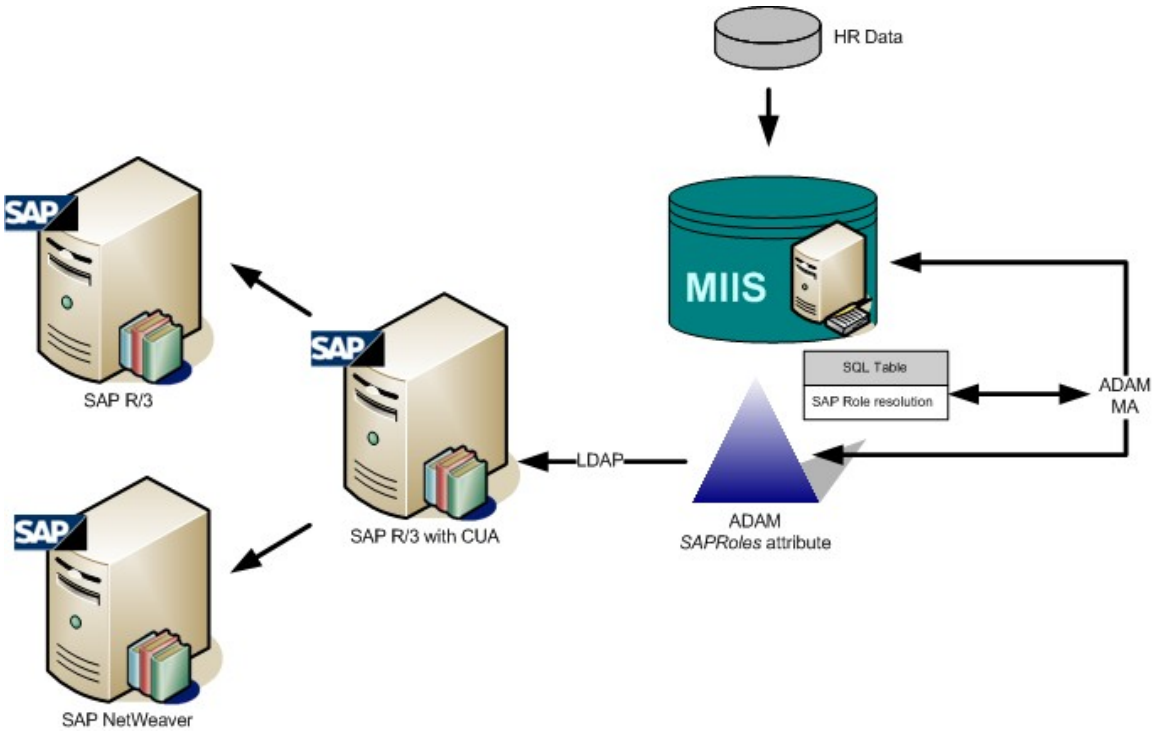


Figure 4: Enterprise role resolution

The process is as follows:

- HR data is read into MIIS, including the job title (or other source attribute for role mapping)
- The job title is used by the ADAM Management Agent to identify the appropriate Roles in target systems, with a query against the appropriate SQL table
- The multi-value SAPRoles attribute is set in ADAM by the ADAM Management Agent, using the values retrieved by the query
- The CUA retrieves the SAPRoles attribute and distributes it to the appropriate target systems

For example – if the Job Title “Purchasing Agent” is read from the HR system, and this should result in this user having the role “Buyer” in the SAP system, the ADAM Management Agent looks up the value “Purchasing Agent” in the role resolution table, and finds the value “Buyer”, which is then written to the SAPRoles attribute.

Thus, the relationship between job titles in HR and required roles in SAP are automatically implemented, with no need for manual intervention. Once SAP Roles are exported and managed centrally by an MIIS-based identity management solution, they can be combined as Enterprise Roles with roles from other non-SAP “target” systems, enabling a centralized role-based provisioning solution. This forms the foundation of a more complete enterprise wide access management solution.

Transfer of Password changes to the SAP Backend-System

Deploying a password management solution is an important aspect for reducing Helpdesk costs. In an SAP and Microsoft environment, two methods of password management can be considered.

1) Kerberos Integration

Native integration between SAP and Microsoft Active Directory using Kerberos-based authentication services is possible. This removes the need for storing passwords in the SAP systems and AD becomes the central authentication service. MIIS is used to manage all other identity information, including the SAP roles. Further discussion of this approach is beyond the scope of this paper.

2) Password Synchronization

When native AD integration is not available, a password synchronization approach is needed to set passwords in the various "target" SAP systems. The management agents delivered with MIIS generally support password management: they can take a password from some source (either from a user password change from the Windows interface or from a self-service web-based password reset interface) and can set the same password in the various connected systems. The Management Agent developed by Oxford is no exception. To change a password in an SAP R/3 System the SUSR_USER_CHANGE_PASSWORD_RFC function can be used, but this is only possible if the old password is known and the SAP system allows the password change for this user. In cases where the old password is not known (for example the setting of an initial password) the password can be reset using the BAPI_User_change function.

Example code to perform such a password reset can be found in the Appendix.

This code will generally run on the MIIS server, which should already have access to the appropriate RFC interfaces, although this is not technically a requirement. The code can be called from any password management system, in particular, of course, MIIS's password management.

Installing the Oxford Computer Group Management Agent for SAP

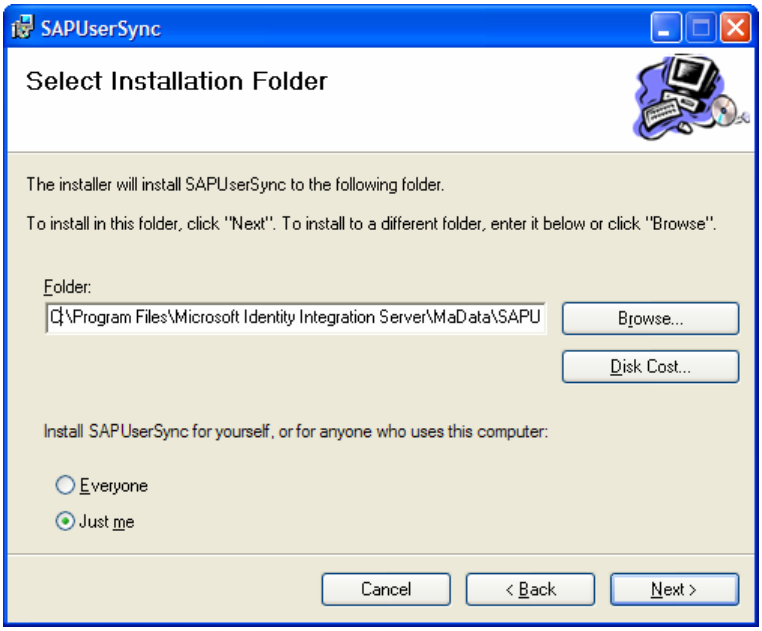
Prerequisites

The Server must at least have the following software already installed:

- Windows 2003 Server
- Microsoft SQL Server 2000
- .NET Runtime 1.1
- SAP connector for Microsoft .NET 2.0 Runtime

Installation

- Run the Setup Program and Install the program under the MADATA Folder of MIIS. (Other locations are supported, but this location keeps all MA-related components together)



- Ensure that the SQL-Server is running
- Use the SQL Query Analyzer to execute the script SQL_Createtables.sql. This script creates the appropriate SQL tables, views and indexes
- Adjust the configuration in the file SAPUserSync.exe.config (as described in section 2.b of the included readme.txt)
  This defines the BAPI calls and describes the target SAP structure which will be used by the Management Agent for the specific SAP environment concerned.
- Run the SAPUserSync program, and check that the SQL table is populated with data
- After this first run, recreate indexes by running “SQL_RecreateIndex.sql” script. This should be repeated occasionally – as a rule of thumb whenever more than 10% of the users have been changed. This is for optimization only: functionality is not affected by this step.
- Create and configure the MIIS SQL Management Agent from the provided template to read the consolidated HR data into MIIS

SUMMARY

This paper has focused on two approaches for integrating SAP user identity information using Microsoft’s Identity Integration Server and Active Directory products, using SAP as both the source of identity information, as well as the target of provisioning and role-management activity. In particular the integration approach involving Microsoft Identity Integration Server is of interest to organizations that have more than just Microsoft and SAP systems in their IT infrastructure, enabling the building of a centralized user identity and access management system.

Appendix: Sample source code for password reset

```
Private Sub ChangeR3Password(ByRef Proxy As SAPProxyDll.SAPProxyDll, ByVal Username As
String, ByVal Encrpassword As String, ByVal Encroldpassword As String)
        Dim Password, OldPassword As String

        If Encrpassword.Length > 0 Then
            Try
        ' Old and new password should be decrypted with MIIS decryption Functionality
                Password = decryptPassword(Encrpassword)
                OldPassword = decryptPassword(Encroldpassword)
                If Password.Length > 0 Then
                    If Not (sappassreq(Password)) Then
                       Debug.writeline("Warning while changing password of User " &
                       Username &
                       ". Password does not comply with SAP password rules.", 1, 1102)
                    End If
                    If SpecialChars(Password) Then
                      Debug.writeline("Warning while changing password of User " &
                      Username &
                      ". Password contains special characters.", 1, 1103)
                    End If
                    Debug.writeline("Trying to call Susr_User_Change_Password_Rfc", 3)
                      Proxy.Susr_User_Change_Password_Rfc(Username.ToUpper, Password,
                      OldPassword)
                    Debug.writeline("Successful password change.")
                Else
                      Debug.writeline("Error while changing password of User " & Username
                      & ". Error Message: Decrypted password is EMTPY.")
                End If
            Catch ex As SAP.Connector.RfcAbapException
                If ex.AbapException.ToLower = "change_not_allowed" Then
                      Errordescription = "Error while changing password of User " &
                      Username & ". Abap Error Message: " & ex.AbapException & ".
                      Possibly wrong old password, no permissions, wrong client or more
                      than 1 change / day"
                Else
                      Errordescription = "Error while changing password of User " &
                      Username & ". Abap Error Message: " & ex.AbapException & "."
                End If
                Debug.writeline(Errordescription, 1, 1104)
            Catch ex As Exception
               Errordescription = "Error while changing password of User " & Username & ".
               Error Message: " & ex.ToString
            End Try
        End If
End Sub
```