Microsoft Exchange 2003 – GAL Sync with the Identity Integration Feature Pack (IIFP)

Written by Marc Grote
mailto:grotem@it-training-grote.de

Abstract

The Windows 2003 Forest is the logical boundary of Exchange 2003. Microsoft recommends deploying only one Active Directory Forest when ever it is possible.

There are many reasons for are single forest deployment beginning by the administrative overhead through the need to synchronize the global Address Lists of Exchange 2003 between two forest to provide a central GAL.

But what if you have more than one forest with Exchange 2003 (through a merger or acquisition)? In this article I will explain in high level steps how to synchronize the GALs (Global Access Lists) of two Exchange 2003 organizations with the help of IIFP. Because of the complexity of this project, I can't take a screenshot of every configuration step. This article should give you an overview about this complex process.

IIFP (Identity Integration Feature Pack) for Microsoft Windows Server Active Directory helps you synchronize identity information and easily provision and deprovision accounts and identity information.

Reference: MIIS Online documentation and the "Technical Overview Whitepaper of MIIS 2003"

Overview

IIFP manages identities and coordinates user details across the following:

- Microsoft Active Directory
- Active Directory Application Mode (ADAM)
- Microsoft Exchange 2000 Server
- Microsoft Exchange Server 2003

Using IIFP you can combine identity information for a given user or resource into a single, logical view. IIFP also automates the provisioning of new and updated identity data, eliminating time-consuming, repetitive administration and the need to manually add, delete, or update identity information, groups, and user accounts.

IIFP has been designed to integrate identity information between multiple Active Directory forests or between AD and ADAM. IIFP enables us to:

- Automatically synchronize users, and their associated information, in one Active Directory forest as contacts in other Active Directory forests
- Selectively synchronize only the user or organizational units that you need to
- Synchronize identity information between Active Directory and ADAM instances
- Synchronizes domain local, global or universal groups across forests
- Synchronize Exchange 2000 and Exchange 2003 global address lists across forests
- Provision users across forests

The Identity Integration Feature Pack is the small Brother of the well know Microsoft product MIIS 2003. MIIS is short for Microsoft Identity Integration Server.

The full MIIS product has the ability to synchronize the following directory services:

- Active Directory
- Active Directory Application Mode
- Attribute value pair text files
- Delimited text files
- Directory Services Markup Language
- Fixed width text files
- Global Address Lists (Exchange)
- LDAP Directory Interchange Format
- Lotus Notes/Domino 4.6 & 5.0
- Microsoft NT 4 Domains
- Microsoft Exchange 5.5 Bridgeheads
- Microsoft Exchange 5.5, 2000 & 2003
- Microsoft SQL 7 & 2000 databases
- Novell eDirectory v8.6.2 & v8.7
- Oracle 8i & 9i databases
- SunONE/iPlanet/Netscape Directory
- IBM Informix, DB2, dBase, Access, Excel, OLE DB via SQL DTS

For more information about MIIS visit: http://www.microsoft.com/miis

Requirements

IIFP requires Microsoft SQL Server 2000 Standard Edition or Enterprise Edition as its back-end store and must be installed on a Microsoft Windows Server 2003, Enterprise Edition, server.

Required Hardware

- Server with a Pentium III 500 MHz or faster processor (Pentium 4 recommended)
- 512 megabytes (MB) of RAM; 1 gigabyte (GB) or more recommended
- Hard disk space required:
  20 MB for typical installation of Identity Integration Feature Pack and rules extensions
  8 GB of available hard disk space on the partition that contains the database files
- Super VGA or higher resolution monitor
- CD-ROM or DVD-ROM drive
- Microsoft Mouse or compatible pointing device

Required Software

Microsoft Windows Server 2003, Enterprise Edition
Microsoft SQL Server 2000, Enterprise Edition, Service Pack 3 (SP3), or Standard Edition, Service Pack 3 (SP3)
Microsoft SQL Server 2000, Developer Edition, Service Pack 3 (SP3) may be used for testing purposes only

IIFP Basics

Connected Data Sources

A connected data source is a directory, database, or other data repository that contains identity data to be integrated with the metadirectory. I will explain what the metabase is later in this article. Connected data sources can be enterprise directories, e-mail directories, directories from other Operating Systems, HR (Human Resource) databases, or data in flat files, such as LDIF, XML, or delimited text.

Management Agents

A management agent links a specific Connected Data Source to the metadirectory. The management agent moves data from the connected data source and the metadirectory. When data in the metadirectory is modified, the management agent exports the data out to the connected data source to keep the connected data source synchronized with the metadirectory. There is at least one management agent for each connected directory.

Connector Space

The connector space is a staging / storage area, where the management agents can move data into and out of a connected data source. Each connected data source has its own logical area in the connector space, which is managed by its corresponding management agent. The connector space is essentially a mirror of the related connected data source, with each object in the connected data source having a corresponding entry in the connector space.

The Metaverse

The Metaverse is a set of tables within MIIS / IIFP that contain the joined identity information from multiple connected sources. All identity information about specific objects, which are stored in multiple connected sources, are synchronized into a single entry in the metaverse.
When you run a management agent, changes that you made to objects in the connected sources are written to the connector space, rules are then applied, and the resulting data is then written to the metaverse if import flow rules detect that this data should be written to the metaverse. The metaverse then sends those changes to the connector space of other connected directories that the object is synchronized with, and their respective management agents then propagate the changes to those connected directories based on the rules defined in the management agents for those connector spaces

Let's begin

Our test environment:

2 Windows 2003 Enterprise DC with Exchange 2003
- One Server named London
- One Server named Rom

2 Forests – One Forest called nwtraders.msft
- One Forest called roma.italien

One of the Servers installed with MS SQL 2000 Developer Edition (Setup creates a SQL database named MicrosoftIdentityIntegrationServer) and IIFP.

In every Forest create some sample user accounts with associated mailboxes and some contacts. This objects will be used for the GAL synchronization process.

Now we can download IIFP under www.microsoft.com/downloads (search for MIIS or IIFP). After the download of IIFP (ca. 7 MB in size) simply install the IIFP package.

The installation is not part of this article but I write a few of lines about the installation:

- Select the installation form (Complete / Custom)
- Select the components to install (on 1 Server we install IIFP with all options)
- Choose the SQL Server instance for IIFP
- Specify the path for the IIFP database
- Choose a Service Account for IIFP
- Specify group names for IIFP management
- Installation begins
- Specify the path to save the previously created encryption keys
- You must Logoff and Logon after setup has finished

After installation has finished install the latest update for IIFP. The latest update when I was writing this article was version 3.0.1023.0.

Network Connectivity

To synchronize the GAL of two different forest we need to establish a naming resolution through DNS. You can use Conditional Forwarders or Secondary DNS zones.

Create a Management Agent

The next step is to create a Management Agent for every forest. To this click Start – All Programs – Identity Integration Feature Pack – Identity Manager

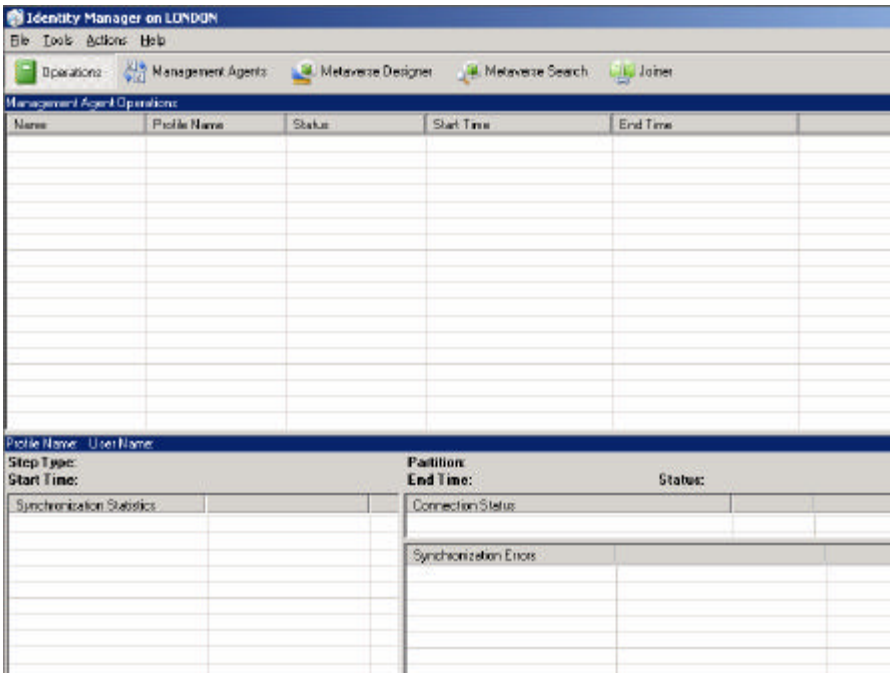

Figure 1: The Identity Manager

Specify a Management Agent for – Active Directory Global Address List (GAL)

- Specify a name for the Management Agent
- Connect to the Active Directory Forest with an account that has the right to read the Directory- and Schema-Partitions
- Select the Directory Partition and Containers (deactivate all objects and then select the OU or OUs to synchronize)
- Deactivate “Sign and encrypt LDAP traffic”
- GAL Container configuration
  - TARGET = Specify destination container (an empty container for the synchronized objects from the foreign forest)
  - SOURCE = Specify the local Domain distinguished name and a container (OU) to export the contacts and users to the foreign forest.
  - Specify SMTP Suffix (the local SMTP Suffix - for both contacts and users/groups)
- Select Object Types (in this default configuration – change nothing)
- Select attributes (in this default configuration – change nothing)
- Configure connector filter (in this default configuration – change nothing)
- Configure Join and Projection Rules (in this default configuration – change nothing)
- Configure Attribute flow (in this default configuration – change nothing)
- Configure Deprovisioning (in this default configuration – change nothing)
- Configure Extensions (in this default configuration – change nothing)

Perform these steps for every forest.

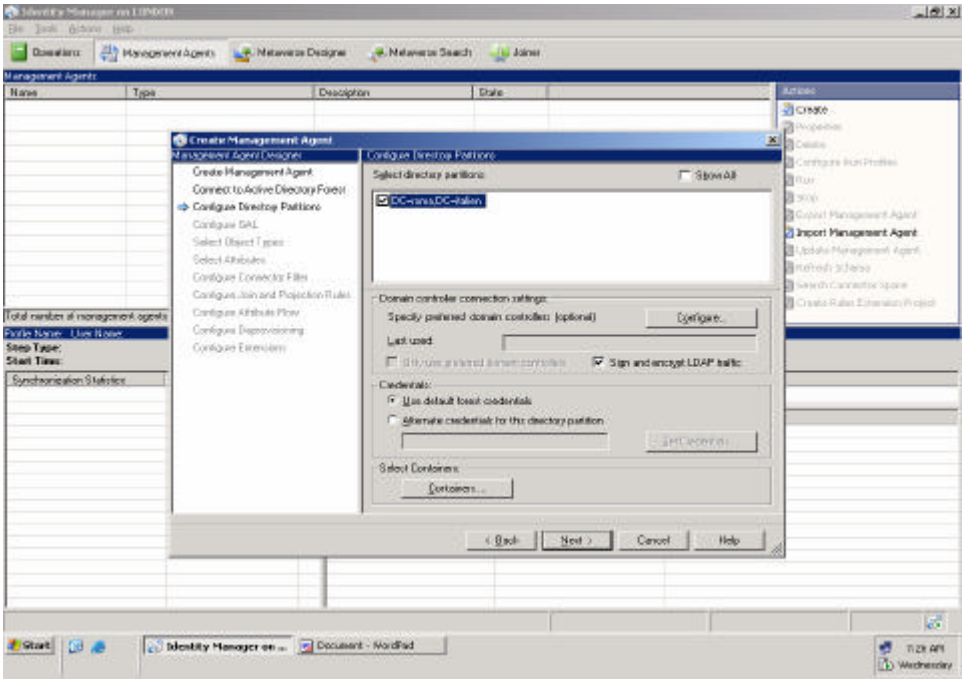

Figure 2: One step in the Management Agent Designer Process – Specify the DS partition

Click TOOLS – CONFIGURE EXTENSIONS – Ensure that “Enable Metaverse Rules Extensions” is selected

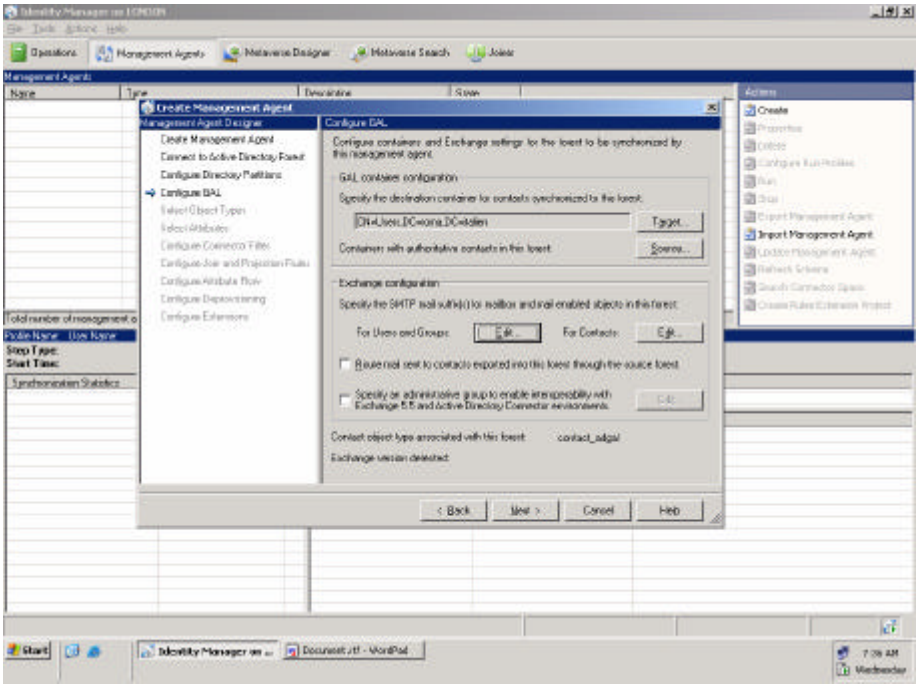

Figure 3: One step in the Management Agent Designer Process – GAL configuration

Synchronization / Import / Export

After the configuration of the management Agent has finished we have to complete the following steps for every Management Agent:

- Run the Management Agent – Specify a FULL IMPORT (Stage Only) for both Management Agents
- Run the Management Agent – Specify “Delta Synchronization” for both Management Agents
- Run the Management Agent - Specifiy “Export” for both Management Agents
- Perform a Delta Import for both Management Agents

It takes a while depending on the size of the objects to synchronize. After the Management Agent has done his work you can view details of this operation.

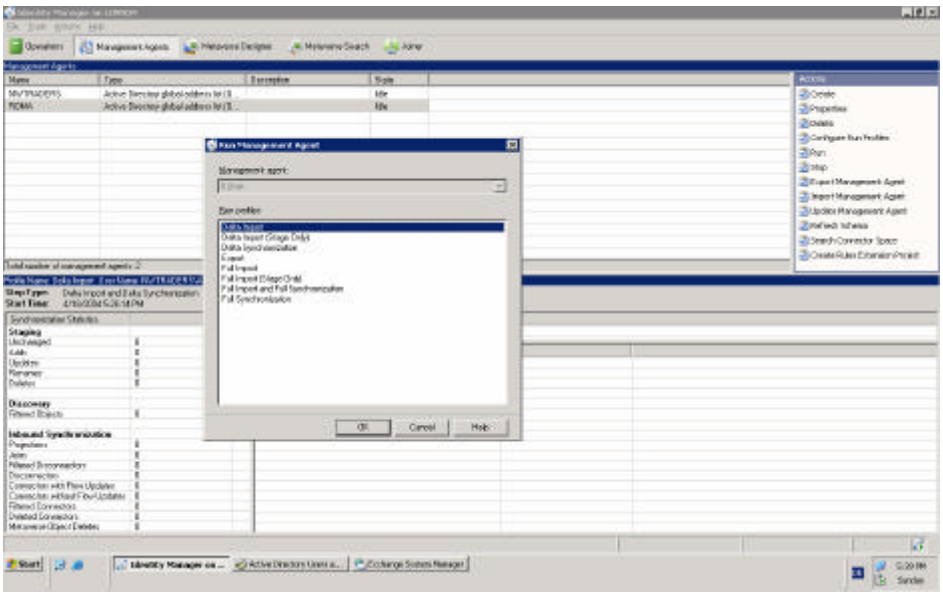

Figure 4: One step of the possible Run-profiles

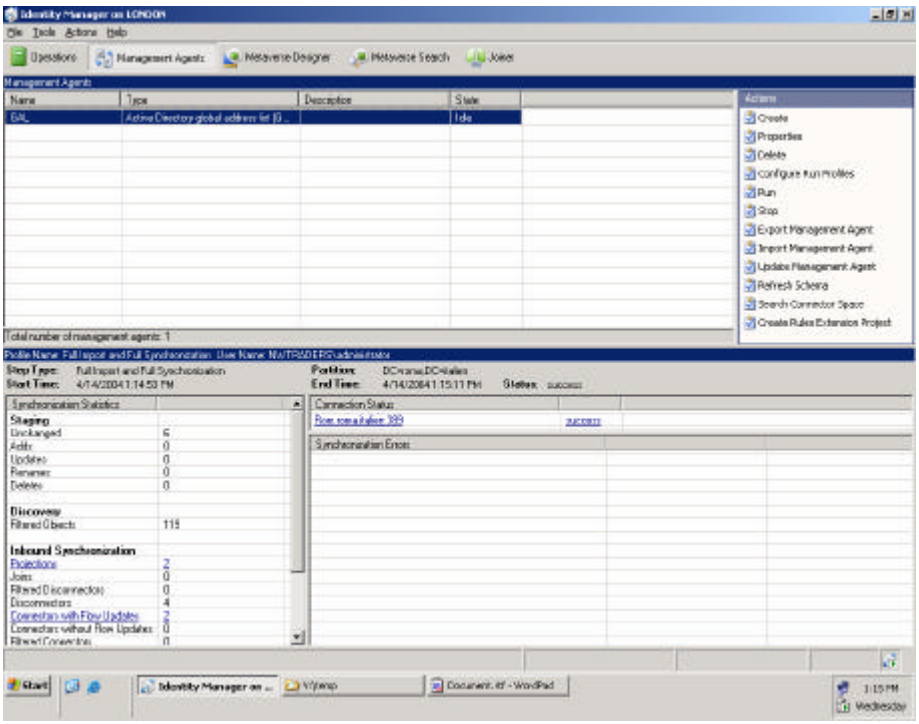

Figure 5: The Management Agent after a Full Import and Full Synchronization

Under “Operations” in Identity Manager you can see the Management Agent Operations. Every listed operation displays a single instance of IIFP

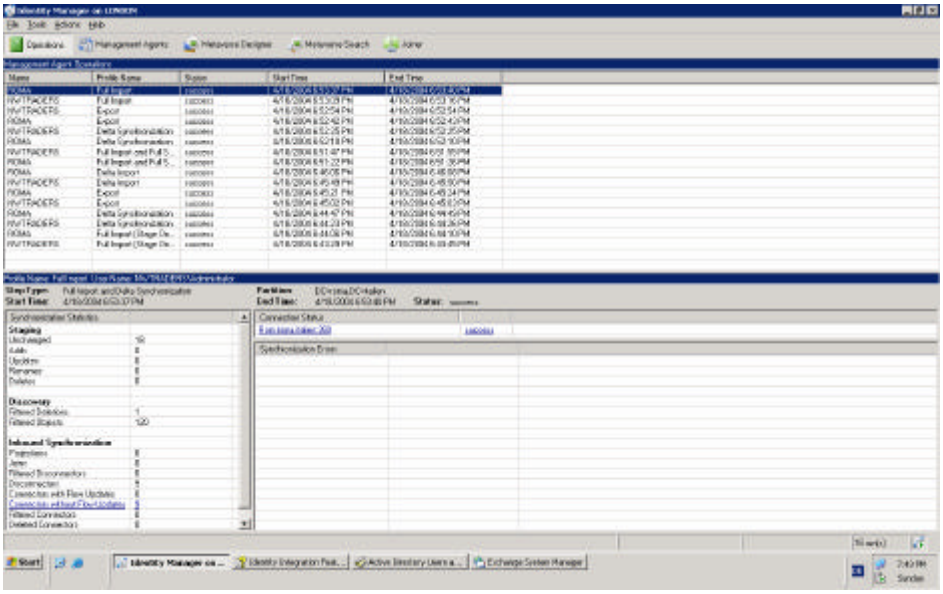

Figure 6: Detailed information about the Management Agent Operations

Metaverse results

You can view the details of the synchronization process in Identity Manager under “Metaverse Search”.
Select the Scope by Object Type and then click “Search”.

IIFP creates an Object Type for every Management Agent. It is called CONTACT_MANAGEMENT AGENT NAME. You can view the results of IIFP when you select this object.
Every Active Directory User Object is mapped through the Object Type “Person”.

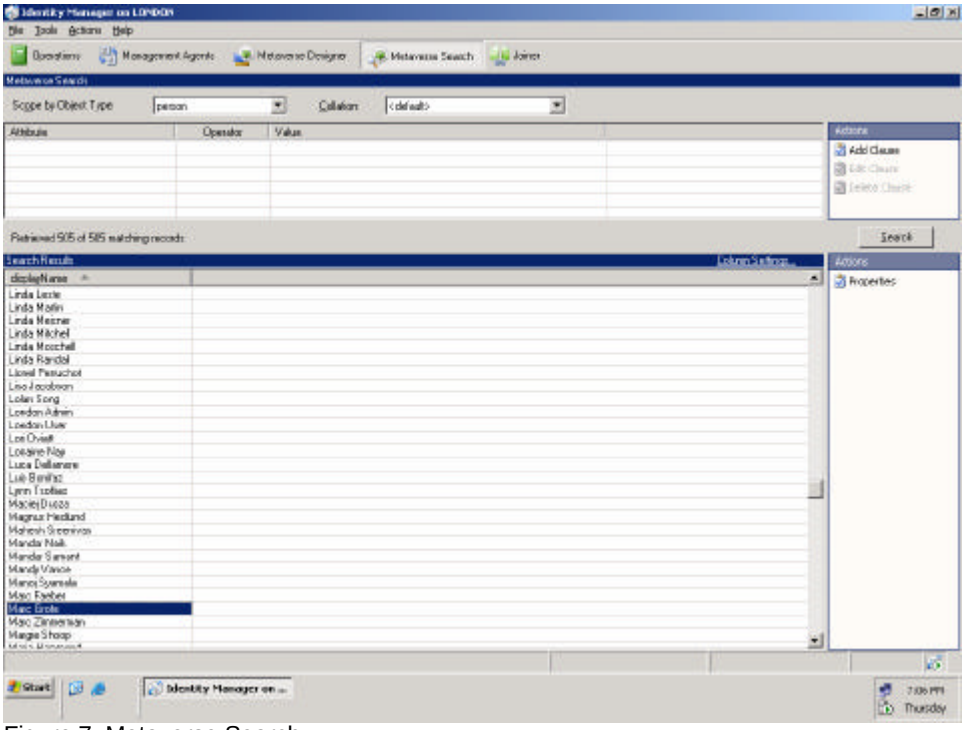

Figure 7: Metaverse Search

The result

After the synchronization process has successfully finished you can see the synchonized objects in the selected OU in ADUC (Active Directory Users and Computers).
IIFP creates an Object Type „Contact“ in the Destination Forest for every Active Directory User Object in the Source Forest and via Verse.

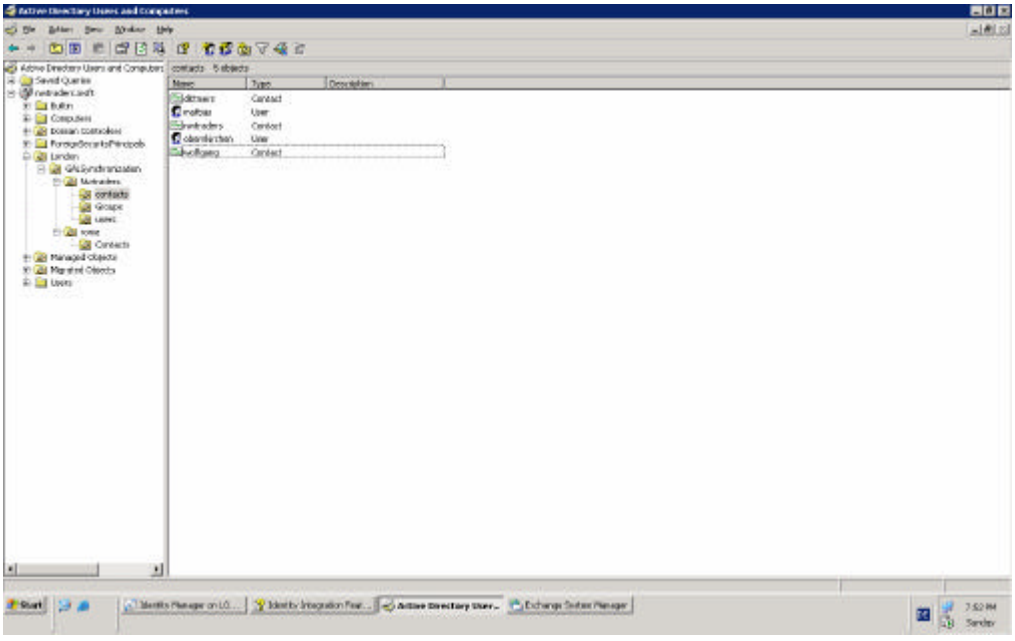

Figure 8: From IIFP created Contacts

You can see all contacts and objects (foreign and own) in the Exchange Global Address List. It is now possible to send E-Mails to objects in every forest with the help of the IIFP GAL synchronization process.

Conclusion

IIFP provides some basic functionality to synchronize data between two different forests and GAL synchronization management for Exchange 2003.

This article looks not beyond the secrets and myths of MIIS / IIFP. It is a very complex product and you will need much time for planning and deploying MIIS / IIFP.

I'm not the Metadirectory Service expert. This was my first try how to synchronize different GALs and I would like to share my experience with you.

To synchronize with other directories or to have more flexibility and administrative control select MIIS as the product of your choice.

Related Links

http://www.microsoft.com/windowsserver2003/techinfo/overview/galsynchstep.mspx
http://www.microsoft.com/windowsserver2003/techinfo/overview/miisgalarch.mspx
www.microsoft.com/miis