



Microsoft Identity and Integration Server Step by Step Guide

The Microsoft Integration and Identity Server 2003 (MIIS 2003) Feature Pack 1a is used to synchronize GAL information between one or more forests. In brief the MIIS application synchronizes the two GALs by creating contacts. The product has the functionality to define destination OU within the two forests that will be synchronized as well as limit the synchronization to specific container that have user objects.

The MIIS requires a full synchronization the first time the management agents are configured. Then it can be scheduled to run in set times and perform delta changes. In that way only limited traffic is generated between the two forests.

For this guide, the MIIS application will be constantly utilized during a period of migration of the forest1.com to the forest2.com.

During this period of migration the following activities take place:

1. Users are copied from the forest1.com to the forest2.com using ADMT.
2. The users' mailbox is migrated to the new Exchange server using Exchange migration wizard.
3. The user account and mailbox in the forest1.com get deleted or disabled.
4. The user disappears from the forest1.com GAL.
5. The user is now created in the forest2.com and the mailbox exists in the new exchange organization. The user accounts appear now in the new GAL.
6. When MIIS runs it will create new contact object in the forest1.com for the users that were migrated in the forest2.com.

System Sense
Level 3, 1 James Place
North Sydney, NSW 2060



Phone: 99226136
Fax: 99224257
E-mail: info@systemsense.com.au
Web: www.systemsense.com.au



Architecture

The MIIS solution requires the following components:

1. The MIIS server.

The MIIS_SERVER is a member server in the forest1.com domain. The server could also have been a standalone server. The MIIS can be only installed in a windows 2003 enterprise server. The application is storing all data in a SQL server 2000 SP3 that can be local or remote. The security framework of the application is based in the utilization of several local groups that are created in the server. The local groups define several roles that allow specific actions to be performed from the management console of the server.

2. The source forest.

The MIIS server will have to connect to the source forest and perform LDAP searches to the forest1.com. The server will connect at port 389 and it will execute LDAP search, look up user object attributes and create contacts. There is a requirement that the management agent of the MIIS will use an administrator account of the forest1.com domain. Finally the MIIS server must have connectivity with at least one domain controller from any other domains within the forest (if it required that they also get synchronised).

3. The target forest

The MIIS server will have to connect to the source forest and perform LDAP searches to the forest2.com. The server will connect at port 389 and it will execute LDAP search, look up user object attributes and create contacts. There is a requirement that the management agent of the MIIS will use an administrator account of the forest2.com domain. Finally the MIIS server must have connectivity with at least one domain controller from the forest2.com domain.

System Sense
Level 3, 1 James Place
North Sydney, NSW 2060



Phone: 99226136
Fax: 99224257
E-mail: info@systemsense.com.au
Web: www.systemsense.com.au



Configuration

Management Agent for forest1.com

1. Create a new management agent by the name "forest1.com management agent".
2. Select "Active Directory Global Address List (GAL)". Select "Next".
3. Connect to the forest1.com domain.
4. Enter the authentication details of the forest1.com. Select "Next".
5. In the select directory partitions, check "dc=forest1,dc=com".
6. Uncheck sign and encrypt LDAP traffic.
7. Select containers and select the required OU. Click Next.
8. Select target and select partition "dc=forest1,dc=com". Select container "OU=Contacts,OU=forest2,OU=GALMA,DC=forest1,DC=com,"
9. Select Source and select partition "dc=forest1,dc=com". Select container "OU=Contacts,OU=forest1,OU=GALMA,DC=forest1,DC=com,"
10. Edit the SMTP suffix and add "@forest1.com".
11. Select next for the following options: Object types, attributes, connector filter, join and projection rules, attribute flow, de-provisioning and extensions.
12. Finish the Management Agent.



Configuration

Management Agent for forest2.com

1. Create a new management agent by the name "forest2.com management agent".
2. Select "Active Directory Global Address List (GAL)". Select "Next".
3. Connect to the forest2.com domain.
4. Enter the authentication details of the forest2.com. Select "Next".
5. In the select directory partitions, check "dc=forest2,dc=com".
6. Uncheck sign and encrypt LDAP traffic.
7. Select containers and click on the ou GALMA. Click Next.
8. Select target and select partition "dc=forest2,dc=com". Select container "OU=Contacts,OU=forest1,OU=GALMA,DC=forest2,DC=com,"
9. 22. Select Source and select partition "dc=forest2,dc=com". Select container "OU=Contacts,OU=forest2,OU=GALMA,DC=forest2,DC=com,"
10. 23. Edit the SMTP suffix and add "@forest2.com".
11. 24. Select next for the following options: Object types, attributes, connector filter, join and projection rules, attribute flow, de-provisioning and extensions.



Running the Management Agents for the first time

1. Enable Provisioning rules extension under Tools > Options.
2. Select the "forest1.com management agent" and under run profiles select "Full import (Stage Only)".
3. Select the "forest2.com management agent" and under run profiles select "Full import (Stage Only)".
4. Select the "forest1.com management agent" and under run profiles select "Full Synchronization".
5. Select the "forest2.com management agent" and under run profiles select "Full Synchronization".
6. Select the "forest1.com management agent" and under run profiles select "Export".
7. Select the "forest2.com management agent" and under run profiles select "Export".
8. Select the "forest1.com management agent" and under run profiles select "Delta Import".
9. Select the "forest2.com management agent" and under run profiles select "Delta Import".
10. The GAL Sync setup is now complete.

For all subsequent management agent operations, use the previous run profiles with the following changes:

1. Delta Import (Staging Only) to the connector space instead of Full import. This step imports all updated Active Directory data into the connector space.
2. Delta Synchronization instead of Full Synchronization. This synchronizes updated connector space data with the metaverse.
3. Export. This exports connector space data to the Active Directory forests.
4. Delta Import. This confirms that the export was successful.

System Sense
Level 3, 1 James Place
North Sydney, NSW 2060



Phone: 99226136
Fax: 99224257
E-mail: info@systemsense.com.au
Web: www.systemsense.com.au

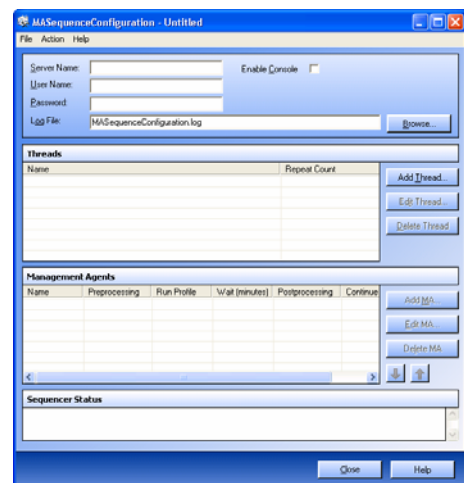


Scheduling

Once the first synchronization is finalized, all contacts are created. With the migration project under way, there is the requirement that the Management agents are constantly activated so as all incremental changes flow to the GAL. The primary way to schedule MIIS to run the Management Agents is with the use of an XML script and the MASEquencer tool.

The XML file is created using the Management Agent Run Sequence Configuration Tool. In this tool the running threads are defined as well as the run profiles, their order, the pre and post behavior and all relevant delays and timeouts.

The MASEquencer tool can be scheduled using windows scheduler and configured to run in set times. The schedule must be configured to run with the local administrator account that is member of the MIIS Admins local group. The tool will create a log file with all error or success information.



MIIS Backup

The MIIS Server comprises of several components that have to be properly backed up. The main requirements are:

1. All SQL server folders get backed up.
2. The SQL Server "MicrosoftIdentityIntegrationServer" database gets backed up.
3. The SQL Server System Databases get backed up.
4. The MIIS application folders, scheduling and encryption key folders get backed up.

System Sense
Level 3, 1 James Place
North Sydney, NSW 2060



Phone: 99226136
Fax: 99224257
E-mail: info@systemsense.com.au
Web: www.systemsense.com.au