Accessing the ManageSoft Administration Server and Reports across domains

ManageSoft knowledge base article 100662

Overview

The ManageSoft administration server and reports server are installed on computers in one Active Directory domain, and are configured for access only by users who are members of that domain. Special configuration steps are necessary for users who are not members of the same domain. At the 7.5 release, this configuration process is manual, following the process documented here.

Prerequisites

This article assumes familiarity with the following topics:

- Active directory domains and groups
- Rights configuration in ManageSoft
- General ManageSoft functionality.

Contents

This document covers the following subjects:

- Domains and trusts in Active Directory
- Groups in Microsoft Windows, Active Directory, and SQL Server
- Groups created when ManageSoft is installed
- Preparing the administration server for access across domains
- How to grant access to ManageSoft reports to users from another domain
- How to install the remote console in another domain

Domains and trusts in Active Directory

Each Active Directory domain exists in a *domain tree* consisting of a *root domain* and zero or more *child domains*, which each may have further child domains. Multiple domain trees may exist, and if they do, they are referred to as a *forest*. Each domain is responsible for authenticating its users and applying its own policies.

Where access rights for a service must be granted to a user from outside the domain which owns that service, the domain must trust the user's domain (the foreign domain) to authenticate that user and to ensure that adequate security policies are in force. This is done by configuring *domain trusts*. Normally, all domains in a domain tree have trusts in both directions (parent and child), but trusts must be manually configured for domains in different forests.

Please consult your Microsoft documentation to find out how to configure trusts for the domains between which you require access to ManageSoft.

Groups in Microsoft Windows, Active Directory, and SQL Server

Access rights in ManageSoft are granted only to groups, never to individual users. ManageSoft makes use of the standard group mechanism available from the operating system, so it's important to understand the capabilities and limitations of the different types of groups in Microsoft products.

Firstly, it's important to note that each Active Directory domain is configured in one of two modes (native or mixed-mode), which affects the behavior of the different types of groups. Mixed mode supports inter-operation with Windows NT 4 domains, and is more restrictive. Because most ManageSoft customers have some Windows NT 4 computers, their domains are generally configured in mixed mode. This document describes an approach that works in mixed mode. Customers who are familiar with the different modes will observe that some elements of the configuration can be simplified for native-mode domains. These simplifications are not detailed here, though will be noted where possible.

The types of groups (and group-like objects) are:

- **Computer Local groups**
  These groups may only be used for controlling access rights for services on one computer. They may contain, as members, computer and user accounts and Domain Global groups, all from any trusted domain. Computer Local groups cannot be created on Domain Controllers – for use from a Domain Controller, Domain Local groups are used instead.

- **Domain Local groups**
  These groups belong to an Active Directory domain, and may only be used for controlling access rights for services on computers belonging to the domain. They may contain, from any trusted domain, computer and user accounts and Domain Global groups. Although it is not obvious from the Microsoft SQL Server documentation, Domain Local groups are **not** effective in controlling access to SQL Server unless the SQL Server instance is installed on a Domain Controller.

- **Domain Global groups**
  These groups belong to the domain, and may contain members only from this domain. Unless in native mode, other global groups are not allowed. Global groups may be used to control access rights in any domain, and this is often done by making them members of a local group in the foreign domain.

- **Universal Groups**
  Universal groups belong to the domain, and may contain any kind of members from any domain, and may be put into other groups and used to assign rights in any domain. However they cannot be created in mixed-mode domains, and so will be ignored for the remainder of this document.

- **SQL Server roles**
  SQL Server has a group structure which is purely internal to itself, known as roles to distinguish them from other types of groups. They offer an alternative to some of the configurations suggested here, but no special advantages, so will be ignored for the remainder of this document.

For more information on Groups in Microsoft Windows and Active Directory, see the Microsoft support article http://support.microsoft.com/?kbid=318862. For advice about how to configure Groups and Roles for use in Microsoft SQL Server see http://www.microsoft.com/technet/prodtechnol/sql/2000/maintain/sp3sec01.mspx.

Groups created when ManageSoft is installed

The ManageSoft administration server may be installed across one or more computers. The services that must be available from these computers are the **core server**, the **web server**, and the **database server**. These computers must normally belong to the same domain, and so the Domain Controller for the domain is also relevant.

ManageSoft creates the following Domain Global groups relevant for cross-domain access control in the domain of which these servers are a member:

- **MGS Administrators**
- **MGS Report Users**

These groups, being Domain Global groups, cannot have members from outside their domain. Thus if access rights to core services and SQL Server were to be granted through these groups, configuring additional domains would require each right to be granted to other global groups in each such domain. However, since the SQL database has upwards of a thousand rights, this is clearly not an acceptable design. Instead, ManageSoft creates two *local* groups for the SQL Server. These are:

- **MGS Data Readers**
- **MGS Data Modifiers**

These groups are created as Computer Local groups (unless the SQL Server instance is installed on a Domain Controller, in which case Domain Local groups are added). All rights granted in SQL are assigned to one of these groups, depending on whether the right allows modification of data in the ManageSoft database or merely read access.

The **MGS Report Users** global group is a member of the **MGS Data Readers** group, and the **MGS Administrators** global group is a member of both local groups. This allows members of these global groups to connect to the ManageSoft database and to read (or modify, respectively) any data in it.

Preparing the administration server for access across domains

The **MGS Administrators** and **MGS Report Users** groups (and other groups we might create) are subject to access controls within ManageSoft itself, requiring rights that are granted using the Assign Rights wizard. The user who installs ManageSoft is made a member of **MGS Administrators**, but you can use **Active Directory Users and Computers** to add any domain user to these groups.

In order for ManageSoft to evaluate access rights, it must be configured to merge policies in all domains containing user accounts that are (ultimately) members of **MGS Administrators** and **MGS Report Users**. The domain in which the core administration server is installed is automatically configured in this way, but other domains must be configured manually. To do this, use the **Setup for multiple domains** tool available from the ManageSoft console.

After configuring other domains to merge policy, use the **Merge ManageSoft Policies** scheduled task to populate the Active Directory information for all configured domains.

For further details of the **Setup for multiple domains** tool, see **Chapter 3: Configuring environments with multiple domains** in the **ManageSoft Configuration Guide**.

How to grant access to ManageSoft reports to users from another domain

If you have understood the foregoing, the following process is quite simple. Here are the steps:

- Create a Domain Global group called **MGS Report Users** in the domain of which your reporting users are members. Add those users to this group.

- Find the **MGS Data Readers** group used by your SQL Server computer, and add the new **MGS Report Users** group from your foreign domain as a member. This will allow the users in this group to access the ManageSoft database for reporting.

    - If your SQL Server is a Domain Controller, the **MGS Data Readers** group will be a group in the SQL Server computer's domain. Use **Active Directory Users and Computers** to find and edit this group's members.

    - If your SQL Server is not a Domain Controller, the **MGS Data Readers** group will be a local group on the computer. Use the **Computer Management** console to find and edit this group's members.

  Note that if any users were logged in during these changes, they will need to log out and log in again once you have set up the group memberships described so far.

- Ensure that the user's domain has been configured for policy merging in ManageSoft. By default, the only domains ManageSoft knows about are those in the same domain tree as the core administration server, and any other domains that have been created as a result of processing inventories. Use the **Setup for multiple domains** wizard to configure domains for policy merging.

- On the ManageSoft core administration server, merge ManageSoft policies for the foreign domain. This will load the new **MGS Report Users** group and its memberships into the ManageSoft database.

- Check that the **FlatName** field of the Domain record in the ManageSoft database has been populated with the NT4-compatible Domain name. The absence of this field will prevent the **Assign Rights** wizard from functioning correctly. You must use SQL (Query Analyser, Enterprise Manager, or the **osql** command line) to check and fix these.

- Use the **Assign Rights** wizard to grant appropriate access to reports for the new group. This wizard is available by right-clicking on the top-level node on the administrative console, and selecting **Manage access rights…** from the context menu.

Users on the foreign domain who are in the **MGS Report Users** group will now be able to log in to the ManageSoft reports using the ManageSoftRP virtual directory on your web server.

How to install the remote console in another domain

This is a lengthy process. Please ensure that you first read all steps carefully, and only proceed after you're satisfied that you understand it fully. *Write down each change that you make*. Since the process involves replacing some of the default installation configurations of the ManageSoft product, it's important that you can revert each change if you run into problems.

The process is as follows:

- If your ManageSoft data server (SQL Server instance) is not on a Domain Controller, then a number of configuration changes must be made on the core server:

    - Create **MGS Data Modifiers** and **MGS Data Readers** groups on your core server. If the core server is a Domain Controller, these groups must be Domain Local groups; otherwise the groups should be created as Computer Local groups.

    - Add the **MGS Administrators** global group as a member of the **MGS Data Modifiers** group, and the **MGS Report Users** as a member of the **MGS Data Readers** group.

  If your Data Server is on a Domain Controller, these groups and memberships will already have been created by the installation of ManageSoft on the data server as Domain Local groups, and so the above steps are not required.

- On the ManageSoft core server, change the Access Control Lists (security settings) wherever rights have been granted to the **MGS Administrators** group to grant those rights instead to the **MGS Data Modifiers** group, and wherever rights have been granted to the **MGS Report Users** group to grant

those rights instead to the **MGS Data Readers** group, as follows.

To make changes to the file system, use Windows Explorer to browse to the places listed below, and right-click to select **Properties**. In the **Properties** page, select the **Security** tab. It is essential to apply the listed changes recursively, so they affect all files and folders below the target folders. To do this, press the **Advanced…** button and check the box labeled **Reset permissions on all child objects and enable propagation of inheritable permissions** before selecting **OK** or **Apply**. A confirmation dialog will appear, since any customizations you have made to security settings on the files and directories will be destroyed in the process.

- The ManageSoft folder (by default **C:\ManageSoft**)
  MGS Data Modifiers should have **Full Control**, and **MGS Administrators** may be deleted.

- The ManageSoft Program Files directory (by default **C:\Program Files\ManageSoft**). **MGS Data Modifiers** should have **Full Control**, and **MGS Administrators** may be deleted.

- The ManageSoft Application Data directory for all users (by default **C:\Documents and Settings\All Users\Application Data\ManageSoft Corp**).
  Note that the Application Data directory is normally hidden – type its name into Explorer or use **Tools > Folder Options** to see it. **MGS Data Modifiers** should have **Full Control,** and **MGS Data Readers** should have write-only access (in the Advanced pane this encompasses four settings – Create Files/Write Data, Create Folders/Append Data, Write Attributes, Write Extended Attributes). **MGS Administrators** and **MGS Report Users** may be deleted.

To modify the Windows Registry, select **Start** >**Run**, type **regedt32** and press **Enter**. Then:

- Open **HKEY_LOCAL_MACHINE** > **SOFTWARE > ManageSoft Corp > ManageSoft**. Details of the next step depend on the operating system:

  - On Windows 2003, right-click **Properties**

  - On Windows 2000, select **Security > Permissions** from the menu bar.

  MGS Data Modifiers should have **Full Control**, and **MGS Administrators** may be deleted.

- Open **HKEY_LOCAL_MACHINE** > **SYSTEM > CurrentControlSet > Control > SecurePipeServers**
  Select **winreg** and open the Security dialog as before. **MGS Data Modifiers** should have **Read** permission (in the Advanced pane this encompasses four settings – Query Value, Enumerate Subkeys,

Notify and Read Control), and **MGS Administrators** may be deleted. This allows remote registry access so that the remote console can read configuration settings.

- Prepare the remote domain. Repeat these steps for each domain where you need a ManageSoft Remote console:

  - Use **Active Directory Users and Computers** to create two domain global groups, called **MGS Administrators** and **MGS Report Users**.

  - Add these two new groups as members of the **MGS Data Modifiers** and **MGS Data Readers** groups respectively on both the core server *and* the data server (if you have a separate data server). Depending on whether these servers are Domain Controllers, you may need to use either the **Computer Management** tool (for Computer Local groups) or **Active Directory Users and Computers** (for Domain Local groups).

  - Add each user who will run a console as a member of the new **MGS Administrators** group. If you are one of the users added, ensure that you log out and log in again to pick up this new membership.

- For each remote domain, assign rights to these groups on the **core administration server**:

  - Perform a policy merge for the remote domain, in order to gather the new group information into the ManageSoft database.

  - Grant rights to the remote **MGS Administrators** and **MGS Report Users** groups using the **Assign Rights** wizard. Normally the **MGS Administrators** have all rights over all resources, and **MGS Report Users** have read-only rights over reporting areas.

- Install the ManageSoft remote console on each computer in the domain where you require remote access. This step must be performed as a local or domain administrator, and this user must also be a member of the domain's **MGS Administrators** group. Afterwards, other members of this group will be able to use the ManageSoft console without being local or domain administrators.

  - Load the ManageSoft install CD-ROM on your remote console computer. Browse on the CD-ROM to the directory **ManageSoft\Administration server** where you'll find the Microsoft installer file **ManageSoft for administration servers.msi**.

  - The installer file must be run with options, because the installer tries to add the local user to the **MGS Administrators** group in the remote domain. This fails and causes the install to roll back. You need to start a Windows command prompt window, and run the following command:

    msiexec /I "ManageSoft for administration servers.msi" /l*v

install.log **IGNORE_ADD_USER_ERRORS="TRUE "**

Note that this should be all on one command line. The installer will run through – select all required options for a remote console install.

- You should now be able to open the remote console and perform any actions for which you have granted rights using the **Assign Rights** wizard.

- For **Software Allocation** actions which require rights to make changes in Active Directory, those rights must be independently granted in Active Directory. They cannot be granted through the ManageSoft **Assign Rights** wizard. If the user is a Domain Administrator, these rights will already be available.

- You can also use **Active Directory Users and Computers** in each domain to add or remove users from either the **MGS Administrators** or **MGS Report Users**. Added users will gain access immediately after logging in again.