



Purpose of this Document:

Prior to Active Directory, only one domain controller (DC) was allowed to process changes to the directory database. This master DC was called the Primary Domain Controller (PDC).

Active Directory extends this single-master model to include multiple roles, and the ability to transfer these roles to any DC in the enterprise.

Active Directory has five of these roles, which are named Flexible Single Master Operations (FSMO) roles:

- Domain Naming Master
- Infrastructure Master
- PDC Emulator
- RID Master
- Schema Master

This document explains: the function of each FSMO role; how to determine which DC owns a particular role; and how to transfer a role to another DC.

Domain Naming Master:

The Domain Naming Master role holder is the DC responsible for making changes to the forest-wide domain name space of the directory. This DC is the only one that can add or remove a domain from Active Directory.

The Domain Naming Master role is unique in an enterprise.

Infrastructure Master:

When an object in one domain is referenced by another object in a different domain, Active Directory represents the reference by the GUID, the SID (for references to security principals), and the DN of the Active Directory object being referenced.

The Infrastructure Master role holder is the DC responsible for updating an object's SID and distinguished name in a cross-domain object reference.

The Infrastructure Master role is unique per domain.

PDC Emulator:

The PDC Emulator role holder performs the following functions:

- Synchronisation of time
- Password changes performed by other DCs in the domain are replicated preferentially to the PDC emulator
- Authentication failures that occur at a given DC in a domain because of an incorrect password are forwarded to the PDC emulator before a bad password failure message is reported to the user
- Account lockouts

The PDC Emulator role is unique per domain.

RID Master:

The RID Master is responsible for assigning pools of RIDs to other DCs on the domain. Each DC on a domain is allowed to create new security principal objects.

The RID Master issues each DC with a pool of RIDs to assign to these newly created objects. Once the pool falls below a threshold, the DC issues a request to the RID Master for an additional pool of RIDs.

The RID Master role is unique per domain.



Schema Master:

The Schema Master is responsible for processing updates to the AD schema. Once the Schema Master updates the AD schema, these changes are replicated to other DCs on the domain.

The Schema Master role is unique in an enterprise.

Checking and transferring the FSMO roles assigned to DCs:

This section illustrates how to check and change the FSMO roles assigned to DCs using Windows' GUI interface. The screenshots provided are from a Windows 2003 DC.

1. RID Master, PDC Emulator and Infrastructure Master Roles

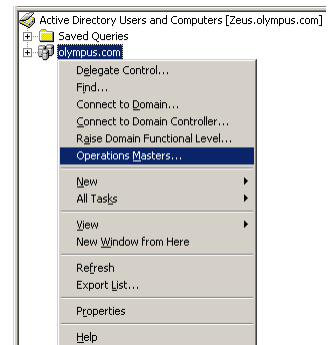
Use the *Active Directory Users and Computers* interface to determine which DCs hold the RID Master, PDC Emulator and Infrastructure Master roles in a domain.

Click on the domain (e.g. *olympus.com*), select *Operations Masters*.

To assign the role to another DC, you must connect to the domain via that DC.

Right-click on the domain and select *Connect to Domain Controller*.

Use the *Operations Masters* interface to pass on the relevant role.



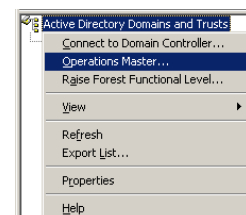
2. Domain Naming Master Role

Use the *Active Directory Domains and Trusts* interface to determine which DC in the forest has the Domain Naming Master role.

Click *Active Directory Domains and Trusts*, select *Operations Master*.

To assign the role to a different DC, you must connect to the target DC.

Right-click on *Active Directory Domains and Trusts* and select *Connect to Domain Controller*.



3. Schema Master Role

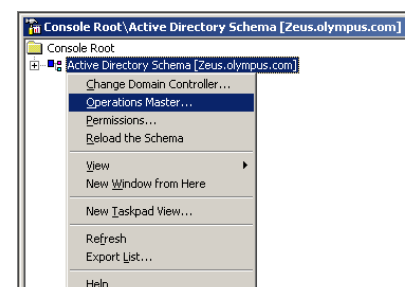
You can use the Schema Master tool to transfer the Schema Master role. Note that the *Schmmgmt.dll* dynamic-link library must be registered in order to make the Schema Master tool available as an MMC snap-in.

Registering the Schema Tool:

1. Go to the Command Prompt: Click *Start*, select *Run*.
2. Type **regsvr32 schmmgmt.dll**, click OK. A message should be displayed stating that the registration was successful.

Transferring the Schema Master Role:

1. Click *Start*, click *Run*, type **mmc**, click OK
2. Click *File* -> *Add/Remove Snap-in*
3. Add *Active Directory Schema*
4. Right-click *Active Directory Schema*, select *Change Domain Controller*
5. Click *Specify Domain Controller*, type the name of the domain controller that will be the new role holder, click OK
6. Right-click *Active Directory Schema*, select *Operation Master*





Glossary of terms used in this document:

FSMO: Flexible Single Master Operations

GUID: Globally Unique Identifier

PDC: Primary Domain Controller

RID: Relative Identifier

SID: Security Identifier

Additional Resources:

Microsoft Knowledge-Base articles:

- Windows 2000 Active Directory FSMO roles. <http://support.microsoft.com/kb/197132>
- Using Ntdsutil.exe to transfer or seize FSMO roles to a domain controller. <http://support.microsoft.com/kb/255504>

This paper was written by Sanjay Pather, an Operations Manager at SekChek Information Protection Services.

Sanjay is responsible for the quality of SekChek reports and research and testing of security controls on the various platforms supported by SekChek.